

**PWRI**

INAUGURAL DEFENSE AND SECURITY  
RESEARCH SYMPOSIUM OF THE  
**PURDUE MILITARY RESEARCH INSTITUTE**

JUNE 26–27, 2023 • PURDUE UNIVERSITY

WEST LAFAYETTE, INDIANA, USA

*“ACADEMIA AS A STRATEGIC NATIONAL ASSET”*



EDITED BY DR. CHAD LAUX, DR. J. ERIC DIETZ,  
DR. JOHN SPRINGER, DR. RANDY RAPP, AND DR. LEON ROBERT

# Table of Contents

<b>Conference Foreword</b> .....	iii
Chad Laux, John Springer, Randy Rapp, Leon Robert, Jr., and J. Eric Dietz	
<b>Developing Training Materials to Supplement the Indiana Cybersecurity Scorecard</b> .....	1
Madison Thomas and J. Eric Dietz	
<b>An Empirical Comparison of Continuous and Periodic Cybersecurity Monitoring Toward Securing the Defense Industrial Base Supply Chain</b> .....	17
Vijay Sundararajan, Arman Ghodousi, and J. Eric Dietz	
<b>A Natural Approach for Synthetic Short-form Text Analysis</b> .....	24
Ruiting Shao, Ryan Schwarz, Christopher Clifton, and Edward J. Delp	
<b>A Data-Driven Approach to Digital Literacy</b> .....	30
Alexis Bradstreet and Nicolas Starck	
<b>An Ocean Apart: Island Disaster Response Logistics</b> .....	35
Paul L. Knudsen and Mary Johnson	
<b>Adaptive Detection and Policy Transformation for Insider Threats</b> .....	47
Nicholas B. Harrell, Alexander Master, and J. Eric Dietz	
<b>Information Communication Technology Support to Remote Work in Higher Education Institutes</b> .....	56
Craig Keith and Chad Laux	
<b>Hypersonics: A Case History of the Dynamic Soarer Project, and Questions to Consider with the Adoption of Exotic Technologies</b> .....	63
Nicholas Michael Sambaluk	
<b>Outlining the Development of Instructional Resources for Cyberphysical Security Mitigation and Preparedness</b> .....	70
Rylee Lane, Shawn Ehlers, Glaris Lancia Raja Arul, and J. Eric Dietz	
<b>Evacuation Situational Manual Guidance for Long-Term Care Facilities</b> .....	77
Rylee Lane, Brock Warner, Dylan John, and William Field	
<b>Performance Analysis of HiFive Unmatched RISC-V Processor Versus x86 Processor Running Microsoft SEAL Homomorphic Encryption Library</b> .....	85
Zachary Legg, James Dean, and Leleia Hsia	
<b>The Need for Higher Fidelity Active Shooter Simulation</b> .....	91
K. Tzvetanov and J. Eric Dietz	
<b>Optimizing Hemorrhage Control Kit Placement</b> .....	99
K. Tzvetanov and J. Eric Dietz	
<b>A Brief History and Critique of Cybersecurity Attack Frameworks</b> .....	108
Sayako Quinlan and Cory-Khoi Quang Nguyen	
<b>Quantum Circuit Reduction Using Three-Layer Transposition</b> .....	116
Christian L. Grauberger, Laurence D. Merkle, and Leleia Hsia	
<b>Analysis of the Relative Risks Associated with Firearms as an Active Shooter Mitigation Technique on School Campuses</b> .....	122
Richard Weston and J. Eric Dietz	

<b>Equivariant Decoders for Quantum LDPC Codes</b> .....	<b>132</b>
Jim Z. Wang, Laurence D. Merkle, and Leleia A. Hsia	
<b>Exploring the Use of UAV-Based Traffic Monitoring for Real-Time Routes Optimization for Military Vehicles</b> .....	<b>137</b>
Claudio Martani	
<b>Using Just-in-Time Training to Evaluate Retention</b> .....	<b>143</b>
Mason Lane, Madison Thomas, J. Eric Dietz, and Rylee Lane	
<b>Active Shooter Prevention Methods in Schools</b> .....	<b>156</b>
Katherine Reichart, Madison Thomas, and J. Eric Dietz	
<b>Conference Appendix</b> .....	<b>186</b>
Purdue Military Research Institute	

## PMRI Conference Foreword

Chad Laux, John Springer, Randy R. Rapp, Leon L. Robert, Jr., and J. Eric Dietz

Purdue has made many recent contributions in responding to and supporting Department of Defense research requirements. Purdue Military Research Institute (PMRI) was created almost 10 years ago to offer an example of this combining learning, discovery, and engagement work on campus. The PMRI program was designed to complement the competitively awarded Purdue Sponsored Research Program that typically has a large fraction sourced from military defense applications and requirements.

As of the Fall Semester of 2022, PMRI has recruited over 170 military officers since beginning this effort in 2014.

The program, with full support of President Mug Chiang, is poised to grow and focus on synergistic collaboration with our military partners by offering access to some 2,400 Purdue faculty conducting world-class research in numerous research areas of significant interest

to the Department of Defense (DoD). The PMRI partners with the Army, Navy and Marines, Air Force, and Space Force in three focus areas:

- Merit-based fellowships for active-duty military members that cover all costs for graduate degree programs (except for books and incidental costs around graduation).
- Summer intern program for undergraduates from the military academies, Purdue ROTC, and select student veterans from other US universities/colleges.
- Faculty exchange program.

In a world of rapidly increasing technology and surges in threat, PMRI seeks to develop defense and security leaders who, beyond excellence in military leadership,



Spring Purdue Military Research Institute (PMRI) Group with President Chiang

are highly capable as innovative next generation problem solvers. We expect the relationship built between officers and faculty members to reach well into the future as many military operational problems arise needing solutions. Our focus is on STEM majors with application to DoD research or potential application to DoD research. We work with students to identify a faculty advisor in their area of study that is either doing DoD research today, is expecting to conduct DoD research in the future, or is conducting research in areas that have DoD potential interest. Most importantly, the program provides a win/win for the nation, for Purdue, and for the military officer.

PMRI began as an innovation experiment that was encouraged by former President Daniels early in his Purdue leadership. At the core, this program is about the relationships that may be called on throughout the careers of the Purdue and military participants. With the military requirements, officers have less than 24 months to earn a MS Degree and 36 months to earn a PhD beyond the MS. Part of our initial challenge was to convince faculty that this was possible. Initially, our goal was to recruit ten officers per year, which was achieved beginning in 2014, our first year of the program.

PMRI has enjoyed great support from campus administration and faculty. For the last three years and with the leadership support from the College of Engineering, we have admitted over 30 officers each year. With additional recruiting, we will reach over 200 officers beginning graduate studies as of Fall 2023 and in that number, we have only had 2 officers to date that have not finished on time. This is a significant asset to the officer and military service as many other universities have absent without degree rates over 20%.

PMRI officers as students continue to impress faculty with their sense of duty, commitment to quality and innovation. The US military must be ready to deter and win conflicts with the military we have and PMRI is designed to make officers an asset like any other weapon system capable of rapid problem solving and solution implementation. Reacting to new risks and threat surprises is an increasing challenge in today's rapid development of data and technology. PMRI fellowships have resulted in the following positive examples promoting research growth:

- New research areas and patents
- Technical papers providing answers to heretofore unexplored research areas
- Enhanced ability to better match student background and interest with faculty
- Create a stronger research team with more diversity based on the military experience

A couple specific student examples include this comment from an Air Force Lieutenant Colonel working at a research lab:

"..We have a substantial number of Purdue alumni working here and they are consistently among our top performers. Keep doing what you are doing because you are doing something right!"

and these from Exit surveys:

"Furthermore, the faculty and staff at Purdue made my experience much more than I anticipated. Purdue offers an extremely diverse environment while encouraging group interaction. Although the curriculum is highly demanding, the support and network Purdue provides helped me transition and ensure I was set up for success. This academic challenge will pay dividends in my career in the military and provide opportunities in the civilian sector upon retiring from the Army."

"PMRI was the easiest part of this whole experience. From the application process, to funding, to ancillary support. . .there is not a single aspect of this program I can offer advice on. I'm not one to hold back on critiques, but this entire program has been impressive."

We plan to sustain the PMRI program by adding a nior advisory board to guide and support future program initiatives to improve our program impact, target selective further officer growth and set the finest military officers in the world on a path that makes military confrontation with the United States unlikely. Next year we want to build research joint focus areas where officers from multiple services work together to solve general solutions to military defense and security problems making the delivery of defense solutions faster and less costly to the taxpayer. We also want to work more closely with the military services to help guide future officer assignments into the most valuable military posting after graduation. Finally, we want to continue to see security and defense solutions that bridge government from the local to national levels.

With this conference on June 26 & 27, at Purdue University's West Lafayette Campus, we are hosting the Inaugural Defense & Security Research Symposium titled "*Academia as a Strategic National Asset*". Our Conference Theme: *Innovation through Teamwork*: We aim to maximize a US strategic national defense advantage by

expanding the partnership between the defense, academic, and innovation ecosystems. This conference will bring together defense and security program faculty, students, and external stakeholders to convene an annual event highlighting PMRI research, engagement, and impact.

### CONFERENCE OBJECTIVES

- Build a network of stakeholders willing to take a leading role in promoting PMRI-related goals.
- Share and highlight research of our PMRI students and faculty, and stakeholders.
- Share PMRI experiences of collaboration with partner institutions.

**Conference Topics.** With an exciting theme for the upcoming conference, we invited and accepted over 20 papers on defense relevant topics, including:

- **Topic Area 1: Emerging Defense Research.** Topics include biotechnology, quantum science, future generation wireless technology, microelectronics, autonomous systems, sensing, advanced materials or other defense and security areas of emerging research.
- **Topic Area 2: Defense and Security Area of Application and Adoption.** Topics include AI and autonomy, cyber, systems-of-systems,

microelectronics, space technology, space domain access and awareness, defense energy systems, and computing, software and human-machine interfaces, and other related area.

- **Topic Area 3: Defense-Specific Areas.** Topics include directed energy, hypersonics, advanced sensors, advanced energetic materials, directed energy, advanced materials, advanced manufacturing, and other related areas.
- **Topic Area 4: Teamwork and Mission Focused Research.** Topics include selection of advanced degree priorities, building defense-university partnerships, disaster response & recovery, building a solutions-oriented workforce, human performance, augmented cognition, built environment, and other human performance-related areas.

This conference was designed to provide an opportunity to present technical research by PMRI Officers that did not require travel. We have many other participants presenting from the Air Force Institute of Technology, Naval Postgraduate School, Air War College and the Nation's Military Academies. We hope you find this conference and effort to be an asset for your research and mission success. Many of the presenters are military officers within the PMRI program. Also, we look forward to advice on how we might continue this effort for the success of the PMRI mission.



# Developing Training Materials to Supplement the Indiana Cybersecurity Scorecard

Madison Thomas and J. Eric Dietz, PhD, PE

## INTRODUCTION

The rise of society’s dependence on technology as well as the desire to be constantly connected raises cybersecurity challenges for both public and private organizations alike. Cybercrime is estimated to have cost businesses \$6 trillion in 2021 with costs only increasing and estimated to hit \$10.5 trillion by 2025 (Morgan, 2020). This challenges organizations to thoroughly understand their cybersecurity risks, investing and maintaining their systems thoroughly in order to not contribute to the increasing cost of cybercrime. Organizations have begun developing scorecards, self-assessments that can be used as a tool to understand where the organization may be lacking in cybersecurity policies. Dr. Jim Lerums, alongside the Indiana Executive Council on Cybersecurity, created a scorecard that incorporates National Institute of Standards and Technology (NIST) cybersecurity framework standards for use by organizations within the state (Lerums, 2019). The scorecard allows businesses to self-evaluate their current cybersecurity practices and self-awareness on a Likert scale. The scorecard has been so successful that it has been adopted by NIST as well. While the current cybersecurity scorecard plays an important role in helping businesses and counties in the state of Indiana evaluate their cybersecurity readiness, this approach does not provide these organizations with the resources necessary to understand and improve their scores. This paper argues that a supplemental guide to the scorecard that includes definitions, instructions, and resources on how to improve cybersecurity scorecard scores will improve overall cybersecurity awareness and protection for residents of Indiana.

The purpose of this research is to determine whether a supplemental guide would give organizations with different levels of cybersecurity expertise the ability to understand where they are lacking within the cybersecurity scorecard and how to improve. Along with an after-action survey, the cybersecurity scorecard and the supplemental guide may lead to insight into where organizations are struggling the most with their cybersecurity. These insights can help in either providing government-funded projects or giving these organizations the resources to seek out education and improve cybersecurity infrastructure on their own.

The research questions central to this research were as follows:

1. Do Indiana counties that use the state-provided cybersecurity scorecard to improve their cybersecurity practices and incident response plans find it useful?
2. What biases or misunderstandings are in the current cybersecurity scorecard that can be addressed in the new implementation guide?

## LITERATURE REVIEW

### *Cyber Hygiene*

Previous research suggested that computer hackers and physical penetration testers exploit a lack of user training and cyber hygiene practices to breach networks and buildings (Kävrestad & Nohlberg, 2021). Vishwanath et al. (2020) define cyber hygiene as “the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet-enabled devices from being compromised in a cyber-attack.” While employees are valuable to an organization, if they participate in poor cyber hygiene practices, they may be more of a security liability than an asset. Poor cyber hygiene practices have been more apparent during the COVID-19 pandemic as more workers are working from home, which gives cybercriminals a greater opportunity to prey on vulnerabilities (Eboibi, 2020). Implementing policies related to cyber hygiene such as requiring two-factor authentication or disabling single sign-on from other websites such as Facebook or LinkedIn could decrease the number of opportunities for gaining access to a business system.

### *Cybersecurity Awareness Training*

Along with cyber hygiene, effectively training employees on best practices within cybersecurity is imperative. Beuran et al. (2017) developed CyTrONE, an automated training environment that creates tasks and generates content based on a users’ needs. Cybersecurity training environments like CyTrONE are often nicknamed cyber ranges for their resemblance to gun shooting ranges that have different targets and obstacles (Beuran et al.,



2017; Taylor, 2021). Environments such as CyTrONE increase training setup accuracy, decrease setup time and cost, and make training reproducible for many participants (Beuran et al., 2017). CyTrOne uses a wizard-like setup that lets training organizers customize the lessons created by topic as well as by difficulty and then upload the lessons to a learning management software or export them (Beuran et al., 2017). Automating and scaling the training process are imperative as consumers of the Indiana cybersecurity scorecard and the resource guide are organizations and Indiana counties of various sizes. If an organization chooses to not automate training or provide consistent training to users, a training manual showing how to implement security measures for an information system, proper cyber hygiene practices, and cybersecurity training that is readily accessible to employees could be another option. Examples of security

measures include firewalls, malware detection systems, intrusion detection and prevention systems, data loss prevention tools, and benchmarking assessments (Manworren et al., 2016). However, for security measures to be effective they must be both accurately implemented and activated. During the Target 2013 data breach, Target turned off a number of these security functions as they interfered with day-to-day data transmission (Manworren et al., 2016). With these security features turned off, the attackers were able to do reconnaissance, weaponize, and begin exploiting Target without its knowledge. This attack is known as a Cyber Kill Chain attack. Figure 1 describes the steps of a Cyber Kill Chain attack, developed by Lockheed Martin (2020). Implementing security measures can prevent data breaches and give cybersecurity analysts time to evaluate what is happening within the network and to put up additional defenses.

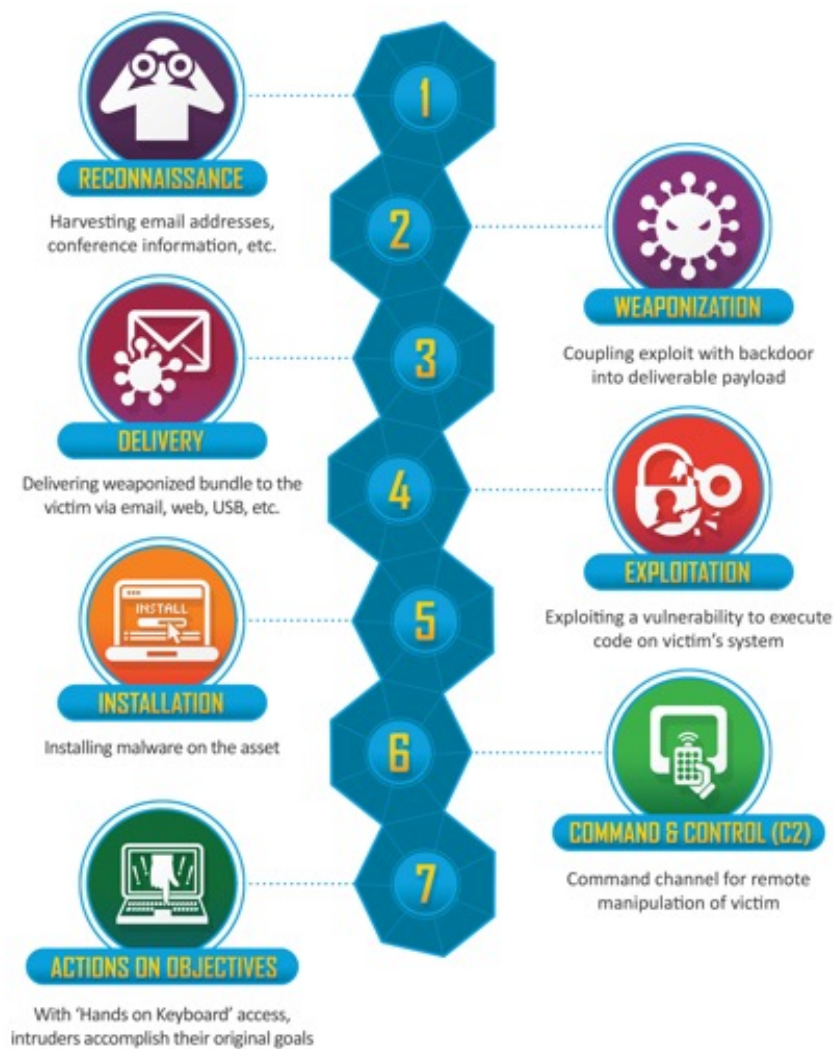


Figure 1. Steps of a Cyber Kill Chain attack

### ***Cybersecurity Training Evaluation Methods***

Within automated user training, different types of evaluation methods can be used. Kävrestad and Nohlberg (2021) found that there are four main evaluation types for testing a user's understanding of computer security and awareness training, also known as SAT. The goal of SAT is to improve a user's computer security behavior in order to maintain good cybersecurity practices at the business level. The four main evaluation types of SAT are perception, knowledge, simulation, and experiment (Kävrestad & Nohlberg, 2021). Perception training measures not a user's retention of training material but their viewpoint and experience of the training itself. Researchers argue that perception training is often more enjoyable for users. However, it does not actually address the user's behavior (Kävrestad & Nohlberg 2021). Kävrestad and Nohlberg also note that knowledge-based SAT is problematic as users can know that reusing passwords is a bad habit, for example, yet continue to do it. The latter types of SAT, simulation and experiment, give a more valid understanding of a user's behavior and knowledge as they are put into situations and made to react. Employee cybersecurity awareness and training methods are included in the cybersecurity scorecard. Understanding different evaluation method strategies allows for a better understanding of how to develop a training manual to accompany the cybersecurity scorecard.

### ***Common Cybersecurity Attacks***

Along with training, a way to effectively protect against cybersecurity attacks in the public sector is to understand the current attack landscape and what kinds of attacks are common.

Harknett and Stever (2009) shed light on how local governments are key actors in cybersecurity threat management. This comes as no surprise as on February 5, 2021, a water treatment plant in Oldsmar, Florida, reported a breach of the supervisory control and data acquisition system, where the attacker increased sodium hydroxide levels to 100 times higher than normal (Pew Charitable Trust, n.d.; Computer and Infrastructure Security Agency [CISA], n.d.). CISA stated that vulnerabilities leading to this breach included using older operating systems on control machines as well as remote desktop sharing software like TeamViewer (CISA, n.d.). Local governments must be fast actors in understanding and implementing patches for flawed computer programs to prevent critical infrastructure cybersecurity events. Rodin (2015) defines critical infrastructure as "physical or virtual systems and assets that are vital enough to a government that if they are destroyed or temporarily unavailable there could be extensive impacts to national security, economy, and public safety and health."

Examples of critical infrastructure include bridges, water systems such as basins and dams, electrical grids, and commercial water systems. These systems have interdependent information technology systems and therefore are at risk for cybersecurity breaches (Rodin, 2015). As mentioned above, attacks on critical infrastructure are not uncommon.

Another impactful critical infrastructure attack happened in May 2021 when the Colonial Pipeline, one of the largest fuel pipelines in the United States, was shut down due to a ransomware attack (Peñaloza, 2021). Ransomware is a type of malicious software designed to harm a programmable device or network by encrypting the files on the device or network, leaving them useless, and then requiring ransom be paid to receive a decryption key (CISA, n.d., "Stop Ransomware"; McAfee, 2019). The Colonial Pipeline attack was a specific type of ransomware attack, called ransomware as a service (RaaS), whereby an entity pays another entity to launch the ransomware on its behalf (2022). Capgemini, an information technology consulting company, predicts that the pandemic has led the public sector to utilize cloud-based products more (Capgemini, 2022). Doing so opens up an opportunity for a new attack landscape. If local governments use cloud services, they should be aware of what cybersecurity frameworks the services use. The federal government is required to use the NIST cybersecurity framework, and since security is only as secure as its weakest link, it is imperative that local governments use this framework as well (Gordon et al., 2020). The Indiana cybersecurity scorecard implementation guide would bridge the gap by aligning the priorities of both the public and private sectors as the implementation guide is based on scorecard scores.

### ***Partnerships with Local Businesses***

A way to effectively protect against critical infrastructure attacks would be to create partnerships between local governments and private businesses in the community to improve security of the local county infrastructure and to bridge the cybersecurity knowledge gap (Harknett & Stever, 2009). By incorporating private sector industry and government, there is a wider knowledge base as well as collaboration on how to protect against common cyberattacks that are emerging or currently popular (Atkins & Lawson, 2021).

As well as working with the private sector, contracting with local businesses helps minimize challenges related to cost and lack of technical experience (Nussbaum & Park, 2018). Nussbaum and Park (2018) recognize that if there is more competition among contractors, it is more likely that a local government will contract for those services. However, there may be issues with value alignment

as local governments and private businesses have different bottom lines. Providing options within the Indiana cybersecurity scorecard implementation guide on ways to improve cybersecurity with and without private industry partnerships is critical to avoid undue stress on both parties.

### **Cybersecurity Implementation**

Another option that the Indiana cybersecurity scorecard implementation guide will provide is addressing cybersecurity at the county level as a public good. Asllani et al. (2013) argue that cybersecurity should be seen as a public good because cybersecurity is both nonrival and nonexcludable: nonrival in that having strong cybersecurity standards does not reduce the availability for others to be cyber secure as well, and nonexcludable in that individuals cannot be easily limited in the benefit of proper cybersecurity practices and therefore protection (Asllani et al., 2013). Other public goods such as safety, law enforcement, and public education are financed through taxpayer dollars. Publicly funded government-level cybersecurity could cause a county's taxes to rise and affect how much benefit is given at a certain cost.

One of the largest factors when discussing implementing a cybersecurity program is cost. Radziwill and Benton used the NIST cybersecurity framework and quality cost models to thoroughly understand all facets of cybersecurity costs. They suggested that cost models in cybersecurity should address all aspects of costs such as operating and implementing tools and systems, cost of consulting and labor, and cost of risk and uncertainty (Radziwill & Benton, 2017). Anderson et al. (2013) categorize costs into direct and indirect costs. Direct costs include recuperating and redistributing money withdrawn from accounts as well as the cost of labor to reset account credentials for county or municipality employees. Indirect costs include loss of trust for the county or municipality, missed opportunities as employees are not able to focus on their work but instead are mending current breach issues, and effort put into removing malware from computers and reimaging the machine (Anderson et al., 2013). Radziwill and Benton include relevant formulas to determine cost such as return on security investment, as well as cost of quality, cost of conformance, and cost of nonconformance. These formulas are listed in Appendix A. A metric not included by Atkins and Lawson is the idea of the depreciation of equipment and upgrades within a system (Krutilla et al., 2021). Regarding other metrics, Atkins and Lawson understood that different public and private sectors do not face the same threats, and therefore equitable spending should not be a valued metric (2021). As such, this emphasizes the point the research team makes that the Indiana cybersecurity scorecard

implementation guide should be open access. The Indiana cybersecurity scorecard implementation guide will include resources related to costs that are inclusive to both ends of a county budget to provide as much guidance as possible.

### **Cybersecurity Insurance**

One way an organization or county could confront the idea of protection and cost is through cyber insurance. Cyber insurance (CI) is an evolving market for protecting organizations against cybersecurity incidents. Based on prior incidents, it is apparent though that insurers and the insured have different definitions of what is a cybersecurity incident and what is not. In 2017, Mondelez International's servers and laptops were infected with the ransomware NotPetya (Kshetri, 2020). Their insurer, Zurich American Insurance Company, denied the \$100 million claim because they classified NotPetya as an act of "cyberwar" (Kshetri, 2020). Another key component in the insurance industry is risk modeling. Risk modeling states that insuring the energy sector and information technology sector are similar in risk assessments (Acharya et al., 2022). Acharya et al. found that insurance design, which includes liability, losses, and premium charges, depends on the likelihood of attack. With some organizations choosing to get CI and others not, this can affect the industry's outlook on cyber incidents. Haislip and Kolev (2019) investigated how cybersecurity breaches affect nonbreached counterparts through insurance and audit prices. Nonbreached peers experience an increase in audit fees and negative equity returns for insurance companies (Haislip & Kolev, 2019). This as well could create a difference in values alignment among private-sector competitors as well as between the public and private sectors. Breaches also impact insurance companies as they may see a positive increase in demand for cybersecurity insurance and therefore be able to increase premiums (Haislip & Kolev, 2019). This could put an organization's financial security in question.

### **What Is Security?**

Security is defined as finding a method to protect an object as well as the need for protection of that object (Lee, 2020). Physical security includes using diverse methods and techniques to protect facilities against man-made and natural disasters (Lee, 2020). Within physical security, there are four lines of defense: perimeter security, exterior and interior security, inner security, and content security. Perimeter security includes outdoors measures such as fences, gates, police patrolling in cars, and security guards patrolling on foot. Exterior and interior security may comprise alarms on doors and windows, and doors with locks. The third type of physical security

defense, inner security, encompasses doors that automatically close and lock, security guards at the entrance checking people in, and checking incoming packages. The final physical security defense, content security, includes safes for files and money (Lee, 2020). The purpose of physical security defenses is to stop an attacker, delay the attacker, and deny access to the most important items or people within a facility (Lee, 2020). Important areas such as computer centers or spaces with large servers should not be in basements, below ground level, or on the first floor of a building due to natural disaster flooding or intruders (Lee, 2020). These areas are better suited on higher floors whose access requires going through physical security measures (security guards and metal detectors) as well as forms of authentication such as badge readers. Multiple questions in the Indiana cybersecurity scorecard address business operations and physical security (questions 5, 7, 8, and 16). As such, the new implementation guide will address physical security as well as ease of access to ensure information is protected and unavailable to those who should not access it.

#### **Access Control**

Along with physical security is access control. In the Target data breach of 2013, Target did not separate its climate control systems from its information services or credit card processing systems. Therefore, hacker that accessed one system had access to them all (Manworren et al., 2016). Implementing access control by limiting system access for users as well as limiting the interaction of systems that should not be connected could prevent situations like this. While securing, maintaining, protecting, and separating data are extremely important, funding these operations is imperative to accomplish these goals. One model used to understand the costs of implementing a cybersecurity protocol is the GL model developed by Gordon, Loeb, and Zhou (2020). The GL model helps organizations decide on an appropriate amount to spend on cybersecurity and then to select an appropriate NIST implementation tier level (Gordon et al., 2020). There are four tiers, increasing in robustness and detail at each level. These tiers provide a foundation for how users of the Indiana cybersecurity scorecard can move between responses. The model is based on a given time period and includes formulas related to the expected benefits of an investment in cybersecurity. These formulae are given in Appendix B. Cost is one of the largest prohibiting factors for an organization that wants to secure its information and networks. The Indiana cybersecurity scorecard implementation guide will utilize this framework to help organizations understand what costs they will encounter with each security implementation or advanced protection.

#### **Data Breaches**

Data breaches cause a loss in trust by customers, investors, and lenders in private companies. For public companies, this equates to citizens, local businesses, and government officials from other counties as well as officials at the state and federal levels (Manworren et al., 2016). For both sectors, increasing consumer trust after a data breach is critical. Researchers found that after a data breach on wearable smart technology, companies that apologize to their customers and then compensate them (without being told to do so by the federal government) benefit from greater feelings of satisfaction from affected customers (Masuch et al., 2021). Another aspect of mediating a breach is reporting it to the proper authorities. The State of Indiana provides guidance on reporting security incidents, as Indiana House Bill 1169 requires any business within the state of Indiana to report an information security incident within two business days of the event. Still discussed is one of the largest cybersecurity breaches involving poor reporting, which occurred at Equifax, a credit aggregation and reporting agency. On August 15, 2017, the CEO of Equifax was notified that personally identifiable information of its 140 million US consumers had been breached (Wang & Johnson, 2018). Equifax announced the breach to the public on September 7, twenty-three days later (Wang & Johnson, 2018). Equifax's chief information security officer and chief information officer had retired on September 15, eight days after the breach was made public.

One way the Equifax breach response letters could be addressed is through text mining applications. Text mining is defined as taking text from sources such as websites and blogs (unstructured data) and transforming the text by categorizing the data for machine learning applications to identify any patterns in the text (IBM, 2020). In 2018, Wang and Johnson used TextSTAT, a text mining application that calculates word frequency and the context in which a word lies. Understanding word frequency and context is critical for understanding an organization's response to a cybersecurity incident as they can indicate emphasis, associations, and projections (Wang & Johnson, 2018). An issue that organizations with a smaller budget may encounter is the lack of understanding of where to begin in a cybersecurity incident in regard to the technical, legal, and publicity aspects. Along with understanding how to deal with poor publicity during a breach, it is important to consider how a breach affects reputation. In 2007, Coombs developed the situational crisis communication theory (SCCT), which has become the foundation for press releases like those used in the Equifax data breach. SCCT provides a framework for how to protect reputation during a crisis by using factors such as crisis history, crisis responsibility, and prior reputational

opinion to understand how to minimize the threat to reputation. However, there is little research suggesting how to protect reputation during a cybersecurity attack on the public sector. Providing resources for organizations within the implementation guide that help with incident response will help with developing a plan as well as avoiding critical mistakes that may be detrimental to stock prices and reputation, for example.

Another prevalent issue in data breaches is the duty of care; Deloitte defines the duty of care as “the moral or legal obligation to ensure the safety and well-being of others” (Whitehead, 2019). In a corporate structure, this could mean which director or officer will take responsibility for the breach as well as which director or officer will be in charge of mediating this issue. Mediating the issue includes public responses, internal responses, fixing and eliminating current threats to a system, and reporting to the appropriate authorities. In the 2013 Target data breach, Target failed to fix or eliminate the threats to its system promptly. Due to its negligence, Target failed its customers as the company knew there was an information security issue yet continued to allow customers to interact with the Target network (Manworren et al., 2016).

## METHODOLOGY

### *Study Design*

This research uses the Indiana cybersecurity scorecard that was developed in 2018 by Jim Lerums (Lerums, 2019). The scorecard reviews six previous cybersecurity measuring tools, included standards from the NIST cybersecurity framework and is available to the public on the State of Indiana’s website.

A critical aspect of this research is ensuring the accessibility of the supplemental guide provided. In 2021, CVE-2021-44228, better known as the log4j vulnerability, affected remote code execution in logging software. This vulnerability was given a Common Vulnerability Scoring System score of critical, stating that this vulnerability will greatly impact any affected organizations (CVE, n.d.). With many organizations using logging features that may use log4j, organizations with limited knowledge about either the vulnerability or patches must scramble to fix the issue. The goal of this research is to provide resources and materials in a supplemental guide for organizations that may, unfortunately, be in similar situations in the future. In late 2021, at the height of increased variants of the COVID-19 virus, the State of Maryland’s health department website was shut down due to ransomware. The ransomware hackers demanded payment in bitcoin (Hellgren, 2021). We hope the supplemental guide provided can help organizations develop a plan of action for

situations like this as well as help them make decisions on when paying a ransom may be appropriate. Along with open access, the resources selected for the supplemental guide come from credible resources such as federal and local governments, accredited higher education institutions, and respected groups within the cybersecurity sector. The resources selected also needed to be timely in order to have a true understanding of the current cybersecurity landscape.

Along with using this previously designed scorecard and these resources, an after-action survey was developed for participants to take. This after-action survey is composed of ten questions. A majority of them use Likert scales to obtain quantitative data about how participants felt about using the scorecard. For five questions, the respondents could respond *not at all useful*, *slightly useful*, *moderately useful*, *very useful*, or *extremely useful*. These were coded as 0 through 4, respectively, for our analysis. For four questions, participants were able to type in their responses, giving qualitative data. A full list of survey questions is given in the appendix.

The counties within the state of Indiana were selected by population and distribution occurred through email. Questions were presented to those within a county who had the most knowledge on the cybersecurity infrastructure. Measures were taken to encode identifiers such as emails, county, and population. This data was analyzed using Statistical Package for the Social Sciences (SPSS) to determine statistical significance.

### *Participants and Recruitment Strategies*

This research is intended to be a pilot study. A pilot study is best suited for this as it could help determine the feasibility of launching such a program across the state of Indiana.

The pilot test includes three stages.

1. Counties will use the cybersecurity scorecard to understand the state of their current cybersecurity practices.
2. Counties will then be provided feedback about the supplemental guide and Scorecard (Qualtrics).
3. Counties will then take the after-action survey to provide feedback on the materials they received and the scorecard.

The Indiana Office of Technology was asked to nominate five volunteer counties that varied in size as well as population to participate in this pilot program. Anonymity was taken into consideration during the data analysis and reporting phases to increase transparency in results.

### **Data Collection Procedure**

Data was gathered over four months, from the development of the survey to data analysis. The cybersecurity scorecard as well as the after-action survey are outlined in the appendix. These were distributed via Qualtrics to the participating counties. Purdue University has a partnership with Qualtrics that allows for use of built-in tools.

### **Data Analysis**

Data from the after-action survey includes both qualitative and quantitative questions. All quantitative and qualitative questions required a response through Qualtrics. Qualitative responses were checked for clarity prior to analysis. Quantitative data was exported from Qualtrics to Microsoft Excel to IBM SPSS. When exporting to Excel, radio button responses were coded into numerical values from 0 to 4, with *Not at all useful* being a 0 and *Extremely useful* being a 4. Qualitative data was exported from Qualtrics to Microsoft Excel.

For the after-action survey, the quantitatively coded questions will be the measurements used to determine if the survey was considered useful. A higher score would indicate that users found it useful, while a lower score would indicate a lack of usefulness. The qualitative questions will be used to determine if there are any biases or misunderstandings in the cybersecurity scorecard. Appendix A gives both the Cybersecurity Scorecard and the after-action survey. This research uses linear regression to see if those who scored highly on the cybersecurity scorecard found the scorecard useful through the after-action survey.

## **RESULTS**

The survey was distributed to approximately fifteen individuals with ties to county cybersecurity in the state of Indiana through the Office of Technology. Of the twelve counties that completed the initial cybersecurity scorecard, six counties completed the after action-survey in its entirety. There was one duplicate in the initial scorecard survey but none in the after-action survey.

### **Response Rate**

The response rates for the Indiana cybersecurity scorecard and the after-action survey are as follows. The Indiana cybersecurity scorecard had thirteen responses, with two being identical and from the same respondent. For analysis this duplicate response was removed, therefore the response rate for the Indiana cybersecurity scorecard was twelve. The Indiana cybersecurity scorecard was sent to 15 people, giving a response rate of 80%.

The after-action survey had six responses with no identical responses. All 6 responses were used for

analysis. In order to complete the after-action survey, respondents had to use the Indiana cybersecurity scorecard. The response rate for the after-action survey was 50%.

### **Cybersecurity Scorecard Scores**

In the cybersecurity scorecard survey, respondents were asked questions that related to the five NIST cybersecurity framework functions; identify, protect, detect, respond, and recover. Below are the summary statistics for each function as well as the respondents' total scores. The total score for each respondent was calculated by adding each function's scores together. A significance level of .05 was used to determine if a distribution was normal.

The *identify* section of the scorecard included eight scored questions. Respondents could earn a score between 0 to 40. The range of respondent scores was 16 to 39. The scores followed a normal distribution.

The *detect* section of the scorecard included one scored question. Respondents could earn a score between 0 to 5. The range of respondent scores was 0 to 5. The scores did not follow a normal distribution.

The *respond* section of the scorecard included two scored questions. Respondents could earn a score between 0 and 10. The range of respondent scores was 4 to 10. One respondent scored all 10 points. The scores did not follow a normal distribution.

The *recover* section of the scorecard included two scored questions. Respondents could earn a score between 0 to 10. The range of respondent scores was 5 to 10. One respondent scored all 10 points. The scores did follow a normal distribution.

The *protect* section of the scorecard included nine scored questions. Respondents could earn a score between 0 to 40. The range of respondent scores was 16 to 37. The scores did not follow a normal distribution.

The total scores for each respondent included the sum of the five subscores. Respondents could earn a score between 0 to 100. The range of respondent scores was 44 to 91. The scores did follow a normal distribution.

### **After-Action Survey Scores**

1. Did you find the Cybersecurity Scorecard was useful in helping you understand where your organization may be lacking related to identifying cybersecurity issues?
  - a. Not at all useful = 1 county
  - b. Slightly useful = 0 counties
  - c. Moderately useful = 2 counties
  - d. Very useful = 2 counties
  - e. Extremely useful = 1 county

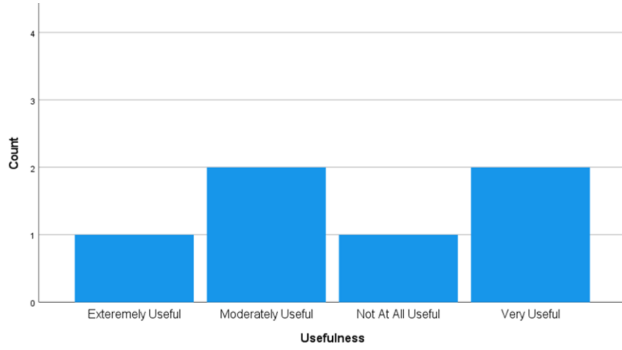


Figure 2. Usefulness of identifying cybersecurity issues

2. Did you find the Cybersecurity Scorecard was useful in helping you understand where your organization may be lacking related to protecting your organization's assets?
  - a. Not at all useful = 1 county
  - b. Slightly useful = 0 counties
  - c. Moderately useful = 3 counties
  - d. Very useful = 1 county
  - e. Extremely useful = 1 county

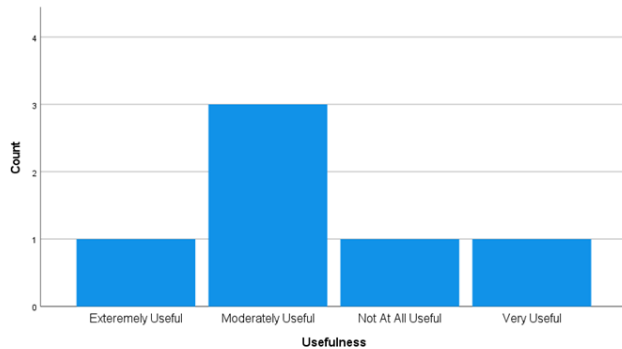


Figure 3. Usefulness of protecting your assets

3. Did you find the Cybersecurity Scorecard was useful in helping you understand where your organization may be lacking related to detecting attacks on your organization's assets?
  - a. Not at all useful = 1 county
  - b. Slightly useful = 0 counties
  - c. Moderately useful = 3 counties
  - d. Very useful = 0 counties
  - e. Extremely useful = 2 counties
4. Did you find the Cybersecurity Scorecard was useful in helping you understand where your organization may be lacking related to protecting against attacks on your organization?
  - a. Not at all useful = 1 county
  - b. Slightly useful = 0 counties
  - c. Moderately useful = 3 counties

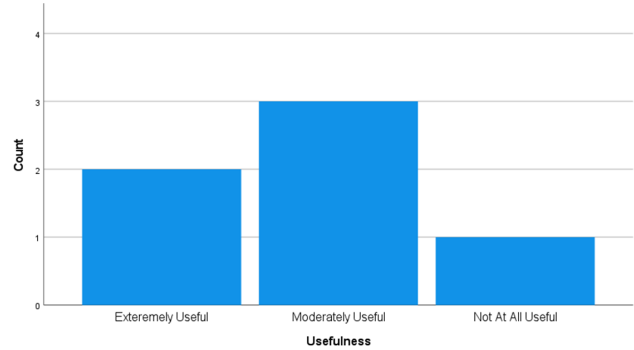


Figure 4. Usefulness of detecting cybersecurity attacks

- d. Very useful = 1 county
- e. Extremely useful = 1 county

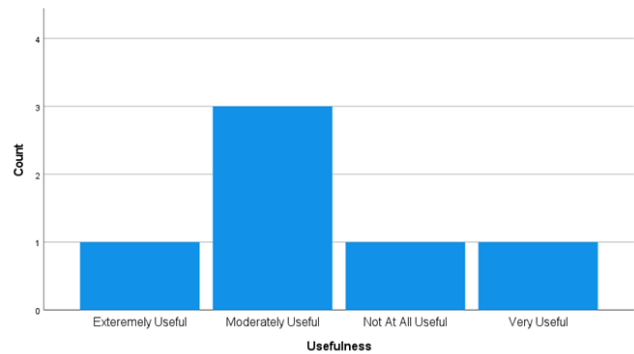


Figure 5. Usefulness of protecting against cybersecurity attacks

5. Did you find the Cybersecurity Scorecard was useful in helping you understand where your organization may be lacking related to recovering from attacks on your organization?
  - a. Not at all useful = 1 county
  - b. Slightly useful = 0 counties
  - c. Moderately useful = 4 counties
  - d. Very useful = 0 counties
  - e. Extremely useful = 1 county

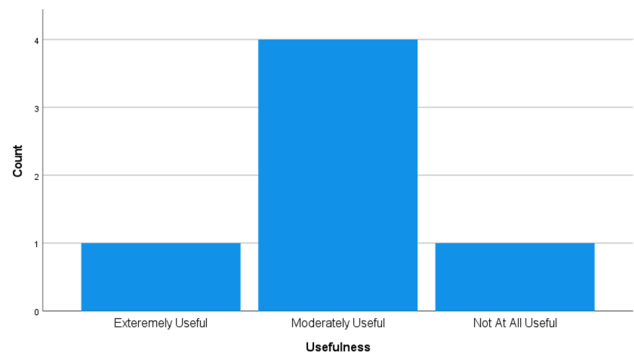


Figure 6. Usefulness of recovering from cybersecurity attacks

**Table 1.** Descriptive statistics of scores

	<i>N</i>	Minimum	Maximum	Mean	Std. deviation
Identify	6	0	4	2.33	1.366
Protect	6	0	4	2.17	1.329
Detect	6	0	4	2.33	1.506
Attacks	6	0	4	2.17	1.329
Recover	6	0	4	2.00	1.265
Valid <i>N</i> (listwise)	6				

All scores above have an average usefulness from 2.0 to 2.33. With the lowest potential average being a 0.0 (*Not at all useful*) and the highest potential average being a 4.0 (*Extremely useful*), an average of 2.0 to 2.33 would lie in the *Moderately useful* category, respectively. This information shows that Indiana counties that use the Indiana cybersecurity scorecard and the subsequent resources found it useful. The research team believes that there is room to improve these usefulness scores by improving the wording of questions in the cybersecurity scorecard as well as providing more information with the resources.

#### **Qualitative Results**

Of the six responses received, four respondents gave some form of written response on the after-action survey.

Question 6 asked respondents, “Were there any portions of the Scorecard that were confusing?” This question had four responses. Two respondents stated that they had no confusion. One respondent stated that the scoring confused them; they noted that they selected *agree* on the survey but felt they scored low on the survey. Another respondent said that some of the questions were ambiguous.

Question 7 asked respondents, “Were there any portions of the Resources page that were confusing?” Only two responded to this question, both answering No.

Question 8 asked respondents, “Were there any portions of the Resources email that were confusing?” Again, only two responded to this question, both answering No.

The last question gave respondents an opportunity to provide any additional feedback they felt wasn’t prompted for in the previous questions. Three respondents answered this question. One stated that the survey and resources were “useful”; another said it was “very helpful and [they] liked the resources.” A different respondent stated that the scale used for the scorecard “[may not be an] appropriate way to answer some of the questions.”

#### **Summary**

We found that respondents found the resources to be moderately useful, per the mean scores of each category. Few respondents left comments about the resources and the scorecard overall. The scoring on the scorecard was

brought up multiple times in the comments of the after-action survey. With this in mind, it would be beneficial to see how the scoring could be improved.

## **DISCUSSION**

### ***Usefulness of Cybersecurity Scorecard***

The researcher hypothesized that Indiana counties that use the cybersecurity scorecard will find the resource guide useful. With this hypothesis, the researcher found that each subsection score from the after-action survey had a mean greater than or equal to 2.00, which is equivalent to *Moderately useful* on the scale used for the after-action survey. One explanation for this is that the term “useful” can be interpreted differently, therefore causing responses that may not fit a respondent’s true feelings. A common definition in academia for usefulness is “the degree to which someone believes that a system or object could enhance their job performance” (Keil et al., 1995). Respondents without a technical background may have found the scorecard more useful than those with a stronger technical background. More research should be done to see if there is a relationship between technical background and finding this scorecard and the subsequent resources provided useful, as well as to determine the usability of the scorecard. Another explanation for the lower mean is that a respondent answered *Not at all useful* (0.00) for the entire after-action survey. They mentioned that they felt the scoring in the Indiana cybersecurity scorecard was “off” and “did not make sense.” Answering 0.00 for six responses decreased the mean.

### ***Biases Within the Cybersecurity Scorecard***

The researcher hypothesized that there would not be misunderstandings in the cybersecurity scorecard that inhibit utilizing the scorecard to its full potential. With this hypothesis, the researcher found that there were some misunderstandings within the scorecard, such as scoring and ambiguous questions. A possible explanation is that some questions such as “Our organization values cybersecurity” may be too vague or rely on the interpretation of the respondent. Some questions also included language such as “system checks” and “cyber-threat” that may have been inaccessible to those without a technical background. As well, respondents could have differing technical backgrounds, from cybersecurity to application development, and therefore the understanding of topics discussed in the scorecard may differ. Levels of bias and misunderstanding found could also be attributed to the scores respondents earned. One respondent stated that they answered “average” on every question yet “earned a low score.” More research should be done on ways to understand if the scoring



mechanism hindered respondents from wanting to use the scorecard to its full potential.

### **Recommendations for Future Studies**

Future research using this study could include a larger pilot program and increased length of research in order to do a longitudinal study of implemented cybersecurity changes. Doing a larger pilot program or a statewide program would provide a more thorough survey of the State of Indiana's cybersecurity practices. Partnering with the State of Indiana again would provide additional support that could gain additional contacts and a larger sample size. If the response rate this research received is to be expected going forward, using half of the counties within the state of Indiana (46) could yield more data points. Conducting a longitudinal study for the implemented cybersecurity changes could potentially aid researchers in understanding if providing these resources are influential in making a change related to cybersecurity practices or if other educational tools such as workshops or conferences are significant turning points for changing cybersecurity practices. Conducting interviews within either of these studies could be beneficial to see if there are any recurring ideas brought up by respondents. Conducting both interviews and using a longitudinal study could help better determine usefulness of these materials or if other outside factors such as vendor access, resources such as money and time, or other information are impactful on organizations making organizational changes to improve their cybersecurity. One written response from the after-action survey discusses how the survey had some level of ambiguity to it. This could have potentially led to bias and respondents selecting an answer that may not have suited their actual thoughts or feelings. Further research should look into how to minimize ambiguity within the scorecard.

This study researched how useful the Indiana cybersecurity scorecard was and the biases or misunderstandings that the scorecard may have. This research suggests that while the scorecard was useful, there may be some misunderstandings within the scorecard that could be improved. A possible cause of this is vague language in the questions and after-action survey as well as different respondent knowledge levels. Future research should use interviews or a longitudinal study to understand usefulness and impact at the organizational level.

### **REFERENCES**

- Acharya, S., Mieth, R., Konstantinou, C., Karri, R., & Dvorkin, Y. (2022). Cyber insurance against cyberattacks on electric vehicle charging stations. *IEEE Transactions on Smart Grid*, 13(2), 1529–1541. <https://doi.org/10.1109/tsg.2021.3133536>
- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy* (pp. 265–300). Springer. [https://doi.org/10.1007/978-3-642-39498-0\\_12](https://doi.org/10.1007/978-3-642-39498-0_12)
- Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. *Journal of Legal, Ethical and Regulatory Issues*, 16(1), 7–14.
- Atkins, S., & Lawson, C. (2021). An improvised patchwork: Success and failure in cybersecurity policy for Critical Infrastructure. *Public Administration Review*, 81(5), 847–861. <https://doi.org/10.1111/puar.13322>
- Beuran, R., Pham, C., Tang, D., Chinen, K.-ichi, Tan, Y., & Shinoda, Y. (2017). CyTrONE: An integrated cybersecurity training framework. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy* (pp. 157–166). SciTePress. <https://doi.org/10.5220/0006206401570166>
- Brown University. (n.d.). *Writing an evaluation plan*. Retrieved November 18, 2021, from <https://www.brown.edu/research/conducting-research-brown/preparing-and-submitting-proposal/proposal-development-services/writing-evaluation-plan>.
- Capgemini Worldwide. (2022, January 18). 2022 key trends in the public sector. Retrieved January 21, 2022, from <https://www.capgemini.com/2022/01/2022-key-trends-in-the-public-sector/>
- CISA. (n.d.). *Compromise of U.S. water treatment facility*. Retrieved October 13, 2021, from [https://us-cert.cisa.gov/sites/default/files/publications/AA21-042A\\_Joint%20Cybersecurity%20Advisory\\_Compromise%20of%20U.S.%20Water%20Treatment%20Facility.pdf](https://us-cert.cisa.gov/sites/default/files/publications/AA21-042A_Joint%20Cybersecurity%20Advisory_Compromise%20of%20U.S.%20Water%20Treatment%20Facility.pdf)
- CISA. (n.d.). *Stop ransomware*. Retrieved October 13, 2021, from <https://www.cisa.gov/stopransomware>
- Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, 10(3), 163–176.
- CrowdStrike. (2022, February 14). *Ransomware as a service (RAAS) explained: CrowdStrike*. Retrieved March 28, 2022, from [https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/#:~:text=What%20is%20Ransomware%20as%20a,service%20\(SaaS\)%20business%20model](https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/#:~:text=What%20is%20Ransomware%20as%20a,service%20(SaaS)%20business%20model)
- CSRC. (n.d.). *Critical infrastructure glossary*. Retrieved October 14, 2021, from [https://csrc.nist.gov/glossary/term/critical\\_infrastructure](https://csrc.nist.gov/glossary/term/critical_infrastructure)
- CVE. (n.d.). *CVE-2021-44228*. Retrieved March 9, 2022, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>
- Eboibi, F. E. (2020). Cybercriminals and coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: Cyber hygiene and preventive enforcement measures. *Commonwealth Law Bulletin*, 47(1), 113–142. <https://doi.org/10.1080/03050718.2020.1834424>
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb model. *Journal of Cybersecurity*, 6(1). <https://doi.org/10.1093/cybsec/tyaa005>

- Haislip, J. Z., Kolev, K., Pinsker, R., & Steffen, T. (2019). *The economic cost of cybersecurity breaches: A broad-based analysis*. Workshop on the Economics of Information Security (WEIS).
- Harknett, R. J., & Stever, J. A. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management*, 6(1). <https://doi.org/10.2202/1547-7355.1649>
- Hellgren, M. (2021, December 6). *Cyberattack hits Maryland Department of Health; government agencies increasingly targets of hackers*. CBS Baltimore. Retrieved March 22, 2022, from <https://baltimore.cbslocal.com/2021/12/06/cyberattack-hits-maryland-department-of-health-government-agencies-increasingly-targets-of-hackers/>
- IBM. (n.d.). *Cost of a data breach report 2021*. Retrieved November 19, 2021, from <https://www.ibm.com/security/data-breach>
- IBM. (2020, November 16). *What is text mining?* Retrieved April 22, 2022, from <https://www.ibm.com/cloud/learn/text-mining>
- IN H 1169, 2021 Reg. Session (Ind. 2021). [https://custom.statenet.com/public/resources.cgi?id=ID:bill:IN2021000H1169&ciq=ncsl&client\\_md=b855328257971532340ced71f40ee0a8&mode=current\\_text](https://custom.statenet.com/public/resources.cgi?id=ID:bill:IN2021000H1169&ciq=ncsl&client_md=b855328257971532340ced71f40ee0a8&mode=current_text)
- Indiana Office of Technology. (n.d.). *IECC Cybersecurity Scorecard*. Retrieved October 15, 2021, from <https://www.in.gov/cybersecurity/files/IECC-Cybersecurity-Scorecard-Public-fillable.pdf>.
- Kävrestad, J., & Nohlberg, M. (2021). Evaluation strategies for cybersecurity training methods: A literature review. In *Human Aspects of Information Security and Assurance* (pp. 102–112). Springer. [https://doi.org/10.1007/978-3-030-81111-2\\_9](https://doi.org/10.1007/978-3-030-81111-2_9)
- Keil, M., Beranek, P. M., & Konsynski, B. R. (1995). Usefulness and ease of use: Field study evidence regarding task considerations. *Decision Support Systems*, 13(1), 75–91. [https://doi.org/10.1016/0167-9236\(94\)e0032-m](https://doi.org/10.1016/0167-9236(94)e0032-m)
- Krutilla, K., Alexeev, A., Jardine, E., & Good, D. (2021). The benefits and costs of cybersecurity risk reduction: A dynamic extension of the Gordon and Loeb Model. *Risk Analysis*, 41(10), 1795–1808. <https://doi.org/10.1111/risa.13713>
- Lee, S. (2020). A basic principle of physical security and its link to cybersecurity. *International Journal of Cyber Criminology*, 14(1). <https://doi.org/10.5281/zenodo.3749780>
- Lerums, J. E. (2019). *Measuring the State of Indiana's Cybersecurity (Version 1)*. Purdue University Graduate School. <https://doi.org/10.25394/PGS.7449230.v1>
- Lockheed Martin. (2020, January 15). *Cyber Kill Chain*. Retrieved March 28, 2022, from <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>
- Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the target data breach. *Business Horizons*, 59(3), 257–266. <https://doi.org/10.1016/j.bushor.2016.01.002>
- Masuch, K., Greve, M., & Trang, S. (2021). What to do after a data breach? Examining apology and compensation as response strategies for health service providers. *Electronic Markets*, 31(4), 829–848. <https://doi.org/10.1007/s12525-021-00490-3>
- McAfee. (2019, November 26). *What is malware and why do cybercriminals use malware?* Retrieved October 13, 2021, from <https://www.mcafee.com/en-us/antivirus/malware.html>.
- Morgan, S. (2020, November 13). *Cybercrime to cost the world \$10.5 trillion annually by 2025*. Cybercrime Magazine. Retrieved October 18, 2021, from <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>
- Nussbaum, B., & Park, S. (2018). A tough decision made easy? *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age* (art. 28). ACM. <https://doi.org/10.1145/3209281.3209368>
- Peñaloza, M. (2021, May 9). *Ransomware attack shuts down a top U.S. gasoline pipeline*. NPR. Retrieved October 13, 2021, from <https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-down-a-top-u-s-gasoline-pipeline>
- Pew Charitable Trusts. (n.d.). Florida hack exposes danger to water systems. Retrieved October 13, 2021, from <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems>
- Radziwill, N. M., & Benton, M. C. (2017). *Cybersecurity cost of quality: Managing the costs of cybersecurity risk management*. <http://arxiv.org/abs/1707.02653>
- Rodin, D. N. (2015). The cybersecurity partnership. *Public Contract Law Journal*, 44(3), 505–528. <https://www.jstor.org/stable/26419479>
- Singer, H. (2014, May 28). *Don't be fooled: Calculate the real cost of employees and consultants*. Toptal Engineering Blog. Retrieved November 19, 2021, from <https://www.toptal.com/freelance/don-t-be-fooled-the-real-cost-of-employees-and-consultants>
- Taylor, H. (2021, May 4). *What is a cyber range?* Cybersecurity Guide. Retrieved October 14, 2021, from <https://cybersecurityguide.org/resources/cyber-ranges/>
- Trautman, L. J. (2016). Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2883607>
- UTEP. (n.d.). *Writing an evaluation plan*. Retrieved November 18, 2021, from [https://www.utep.edu/orsp/\\_Files/docs/writing-an-evaluation.pdf](https://www.utep.edu/orsp/_Files/docs/writing-an-evaluation.pdf)
- Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128, 113160. <https://doi.org/10.1016/j.dss.2019.113160>
- Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: A case study of the Equifax data breach. *Issues In Information Systems*, 19(3), 150–159. [https://doi.org/10.48009/3\\_iis\\_2018\\_150-159](https://doi.org/10.48009/3_iis_2018_150-159)
- Whitehead, M. (2019, November). *Duty of care: What does it mean in the context of a data breach under GDPR?* Deloitte United Kingdom. Retrieved October 16, 2021, from <https://www2.deloitte.com/uk/en/pages/risk/articles/duty-of-care-what-does-it-mean-in-the-context-of-a-data-breach-under-gdpr.html>

## APPENDICES

### Appendix A

Cost of Quality (CoQ) = Cost of Conformance + Cost of Nonconformance

Cost of Conformance = Cost of Prevention + Cost of Appraisal

Cost of Nonconformance = Cost of Internal Failures + Cost of External Failures

Cost of Quality = Cost of Prevention + Cost of Appraisal + Cost of Internal Failures + Cost of External Failures

### Appendix B: GL Model Formulas

Expected benefits from an investment (z) in cybersecurity (EBC(z)) is

$$(EBC(z)) = [v - s(z,v)]L$$

v = vulnerability

L = potential monetary loss

s(z,v) = security breach probability function

Z = some level of cybersecurity investment

### Appendix C: Survey Instrument—Cybersecurity Scorecard



Thank you for participating in the Indiana Executive Council on Cybersecurity's (IECC) scorecard!

Our goal is to help businesses and organizations gain a greater understanding of their cybersecurity readiness. At the same time, we want to share with you more resources that can help you improve, and in doing so, better protect your data and critical systems.

The IECC developed the following scorecard around the 5 core categories of the NIST (National Institute of Standards and Technology): Identify, Protect, Detect, Respond, and Recover.

You will be asked questions regarding your business in each of these five areas. Each area will have between two and eight statements for you to complete, for a total of 22 items. We expect this will take you approximately 10 minutes to complete.

As you finish each section, we will provide resources based on your responses. These resources will also be in a summary that will be emailed to you so that you can review your scorecard and access these resources at your convenience.

At the end of the scorecard, you will be provided a link via the Indiana Cybersecurity Hub website at: [www.in.gov/cybersecurity](http://www.in.gov/cybersecurity).

0% ————— 100%

Please provide your email so you can be sent the resources based on your score:

← BACK

→ NEXT

0% ————— 100%

#### Section 1: Identify

Identify is the first and most important function of NIST. Each category in NIST deals with various cybersecurity subcategories. We are not going to go into detail here on all the subcategories, instead we tackle the function as a whole. The questions in the Identify category will range from: why cybersecurity is important to every organization; how to identify the different assets in the organization; helping you understand the various risks involved if you have not identified everything; the importance of identifying all the smart devices connected to your network.

Businesses need to understand that it is the top priority to take the time to find every system and update within their infrastructure, and the risks involved if not done correctly. It is important to know the criticality of each asset, meaning what is the level of importance of each system, service, data, personnel, and facility to your organization. Similarly, it is imperative to find all the "Smart devices" connecting or interacting with your organization, as each one of these devices can be an opportunity for a cybercriminal to use against you.

→ NEXT

Section 1: Identify

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree Nor Disagree (3)	Agree (4)	Strongly Agree (5)
Our organization values cybersecurity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We have evaluated the operational need of my data and systems to our organization's function (if we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our business/organization model influences the way we approach cybersecurity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We are familiar with the cybersecurity threats or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

← BACK

→ NEXT

**Section 2: Protect**

Protect is the second function of NIST. The Protect function builds on the work accomplished in Identify. In the first function, Identify, we dealt with how to find, focus on, and prioritize your assets. The next question that comes to mind is now that we have identified all the assets, and rated how critical they are to our organization, how do we protect all of it?

If "an ounce of prevention is worth a pound of cure", then this is the prevention part of your cybersecurity work. Yet, it can only be accomplished if you have first accomplished Identify. The questions in this category will help a business understand to what level they are protecting all the assets that are involved in their business. There are going to be resources along the way to help you "level up" your cybersecurity scores. There are going to be tips and checklists to help determine what to do next. Protect not only deals with protecting the hardware and the software involved, it also deals with the protection of data, physical assets, and personnel an organization or business deals with, so that it can better protect itself from cyber-attacks.

The questions in the Protect function emphasize the need to control access to all assets involved in an organization. They will emphasize the need to have policies, procedures, training, and technologies in place so that organizations better protect themselves.

Section 2: Protect

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree Nor Disagree (3)	Agree (4)	Strongly Agree (5)
We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We have system checks in place to make sure that our data is not compromised or changed.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our data is available to employees or clients when needed. (If our government or commerce site was unavailable to customers or employees, we would know what to do).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our cybersecurity technology (such as antivirus, wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our executive leadership receives periodic status, physical, and cybersecurity updates.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We provide our employees cybersecurity awareness and/or training.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We protect our business and customer information so that only the employees that need to see it, can.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

→ NEXT

**Section 3: Detect**

Detect is the third function of NIST. What the Detect function reveals is that relying too much on the Protect function will cause your organization to not know when a cyberthreat is occurring that will negatively affect the organization. This function's main job is to help you discover cybersecurity events in a timely. The important thing to remember about Detect is that not only does it deal with making sure your organization has the technology to detect attacks on every device, system, and service, but also your organization is making sure that the processes you have in place to protect your organization are following best practices, documented, and being continuously improved. Since most attacks are stealthy and not obvious, organizations must be able to detect anomalies or events that may seem insignificant by themselves, but when happening together, they are dangerous to your organization.

Section 3: Detect

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree Nor Disagree (3)	Agree (4)	Strongly Agree (5)
We would know if our cybersecurity technology detected a cyberthreat.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Section 4: Respond**

Respond is the fourth function of NIST. The two questions dealing with this category are based on knowing that the protections you have in place for your organization will never be perfect. Therefore, when a cyberattack does happen, know that how you handle the response can make or break the outcome for your organization, both financially and public perception. It is very important to remember that a timely response is imperative in case of a cybersecurity incident. Any delay can create additional opportunities for cyber criminals to continue inflicting harm to your organization. The articles that we have can help you "level up" the plan you already have. They can also serve as templates so that you can create a plan unique to your organization.

Section 4: Respond

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree Nor Disagree (3)	Agree (4)	Strongly Agree (5)
We have a process in place to address a cyber-threat.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
We have a cyber emergency response plan in place to address a cyber-attack on our organization.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

→ NEXT

**Section 5: Recover**

Recover is the fifth and last function of NIST. As we have emphasized a proactive approach is very important, organizations must prepare for the possibility a cyberattack happens. Detecting and Responding is not enough, you will have to get everything impacted by the attack operating normally. All though there are many types of cyber attacks, the costliest cyberthreat is when a data breach occurs. If your organization stores any kind of personal information from users, clients, or employees, the organization is responsible to safeguard the data. Therefore, you need to plan both how you will Recover after different forms of cyberattacks, data breaches, etc..., and how your organization will use the lessons learned, throughout the incident, to improve your overall cybersecurity processes.

Section 5: Recover

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree Nor Disagree (3)	Agree (4)	Strongly Agree (5)
If we were impacted by a cyber emergency (e.g. ransomware), we know how our organization would recover our data and/or operational systems.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
After a cyber-threat or emergency, our organization will make changes to people, process, technology, etc. to improve our security.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Identify Section Score**

You scored 0 out of a possible 40 in the area of Identify. You will likely find the following introductory resources valuable to help promote cybersecurity in your business.

- [Question 1 - Cybersecurity is no longer optional](#)
- [Question 2 - Digital Asset Management](#)
- [Question 3 - Criticality in Asset Management](#)
- [Question 4 - Business Value in Cybersecurity](#)
- [Question 5 - Cybersecurity Threats](#)
- [Question 6 - What is a Cybersecurity Assessment?](#)
- [Question 17 - Data Inventory Guide](#)
- [Question 21 - What is IoT Security?](#)

Based on your responses to the scorecard, easy ways to "Level Up" your cybersecurity score from Low to Medium will be to 1) begin integrating cybersecurity into your daily business decisions because small and medium businesses are easy targets for cybercriminals, 2) Understand your top priority is that if you don't know what you have, you can't protect it. Therefore, create a list / inventory of all your digital assets, systems, services, and data. Ensure the inventory includes "smart" devices such as wearables, smart locks, connected cameras, mobile credit card readers / point of sale (POS), inventory & stock control, shipping trackers, supply-chain data monitoring, temperature / climate control / water leak sensors, voice assistants, smart lights, smart thermostats and HVAC, connected alarm systems / smoke / carbon monoxide, smart televisions, etc... 3) Determine your businesses priority for each of the assets in your inventory. The higher the priority something is to your business, the better the protections need to be.

**Protect Section Score**

You scored 0 out of a possible 40 in the area of Protect. You will likely find the following introductory resources valuable to help promote cybersecurity in your business.

- [Question 7 – Resource 1 – FTC Physical Security](#)
- [Question 7 – Resource 2 – Physical Access Control](#)
- [Question 8 – How to effectively log](#)
- [Question 9 – Access Control](#)
- [Question 10 – Cybersecurity for Small Organizations](#)
- [Question 11 – Device Security](#)
- [Question 16 – Leadership in Cybersecurity](#)
- [Question 18 – Employee Training](#)
- [Question 19 – Network Access Control](#)
- [Question 22 – What is IoT Security?](#)

Based on your responses to the scorecard, easy ways to "Level Up" your cybersecurity score from Low to Medium will be to 1) Keep all of your operating systems and software up to date by setting up automatic patching/updates to install either daily or at multiple points during the week, 2) Educate both yourself and employees on cybersecurity awareness so your organization doesn't fall prey to cyber criminal's attempts because many attacks require individuals to take actions such as visit a malicious website, click on a link in a phishing email, etc... 3) Create layers of defenses that will secure data wherever it resides such as 2FA/MFA (two-factor/multi-factor authentication), restrict all logins to the least amount of access each needs and no more, firewalls, anti-malware and ransomware protection, etc...

**Detect Section Score**

You scored 0 out of a possible 10 in the area of Detect. You will likely find the following introductory resource valuable to help promote cybersecurity in your business.

- [Question 20 – 5 Ways to detect a cyber attack](#)

Based on your responses to the scorecard, easy ways to "Level Up" your cybersecurity score to from Low to Medium will be to 1) Ensure that you are patching all of your digital assets as soon as possible because this will stop 90% of attacks before they ever begin (Panda Security), 2) Ensure all staff receive frequent cyber awareness training so they are able to avoid phishing attacks and malicious websites, 3) Ensure you are using a next generation anti-virus (NGAV) solution and research if an endpoint detection and response (EDR) solution makes sense for your organization's continuous monitoring needs, 3) Setup and document which threats you want to receive alerts for so you know when significant attacks are occurring, and 4) research whether a managed security service provider is right for your organization.

**Respond Section Score**

You scored 0 out of a possible 10 in the area of Respond. You will likely find the following introductory resources valuable to help promote cybersecurity in your business.

- [Question 12 – 10 Steps to Cyber Security](#)
- [Question 13 – What is an Incident Response Plan for IT?](#)

Based on your responses to the scorecard, easy ways to "Level Up" your cybersecurity score from Low to Medium will be to 1) Develop a cyber incident response plan that includes key company stakeholder input and the who, what, when, where, why, and how your organization will execute your response, 2) Develop both internal communication flows during the response, and multiple external public relations (PR) statements for multiple scenarios, 3) Analyze the attack to determine how it affected the business, assess the damage, understand the scope of the attack to know how to stop it, and begin cyber forensics measures, and 4) Determine which internal team or external service provider has the ability to remove all traces of the threat from your entire organization.

**Recover Section Score**

You scored 0 out of a possible 10 in the area of Recover. You will likely find the following introductory resources valuable to help promote cybersecurity in your business.

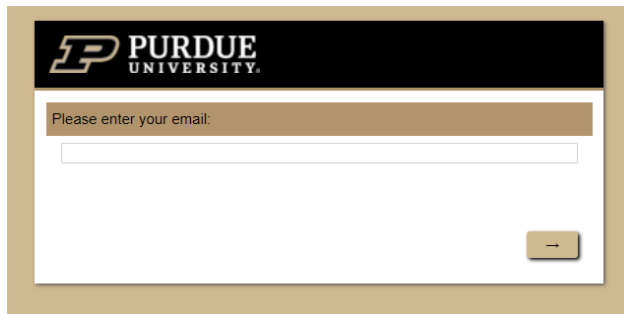
- [Question 14 – How to Recover from a Cyber Attack](#)
- [Question 15 – Cybersecurity Incident After Action Report](#)

Based on your responses to the scorecard, easy ways to "Level Up" your cybersecurity score from Low to Medium will be to 1) Utilize your physical and digital asset inventory developed in the Identify function to complete a cyber risk assessment (CRA) and business impact analysis (BIA) for your organization, to identify the critical data, services, and systems and their cyber interdependencies, which allows you to determine the order you recover critical services, 2) Determine how your organization will be cyber resilient during times of reduced capacity or when recovering over a period of time because only the most critical systems are available at the beginning, 3) Document the specific personnel, their emergency communications information, the steps involved during a restore from backups, and a comprehensive communications plan that will coordinate the entire effort.

Thank you for taking this questionnaire. The following link will take you to our main index of resources regarding cybersecurity. Again we encourage you to come back and retake this questionnaire periodically to learn more about protecting your business and the state of Indiana.

[IECC Cybersecurity Resources and Training](#)

## Appendix D: Survey Instrument—After-Action Survey



**Did you find the Cybersecurity Scorecard was useful in helping you understand where your organization may be lacking related to identifying cybersecurity issues?**

- Not at all useful
- Slightly useful
- Moderately useful
- Very useful
- Extremely useful

**Did you find the Cybersecurity Scorecard was useful in helping you understand where your organization may be lacking related to protecting your organizations assets?**

- Not at all useful
- Slightly useful
- Moderately useful
- Very useful
- Extremely useful

**Did you find the Cybersecurity Scorecard was useful in helping you understand where your organization may be lacking related to detecting attacks on your organizations assets?**

- Not at all useful
- Slightly useful
- Moderately useful
- Very useful
- Extremely useful

**Did you find the Cybersecurity Scorecard was useful in helping you understand where your organization may be lacking related to protecting against attacks on your organization?**

- Not at all useful
- Slightly useful
- Moderately useful
- Very useful
- Extremely useful

**Did you find the Cybersecurity Scorecard was useful in helping you understand where your organization may be lacking related to recovering from attacks on your organization?**

- Not at all useful
- Slightly useful
- Moderately useful
- Very useful
- Extremely useful

**Were there any portions of the Scorecard that were confusing?**

**Were there any portions of the Resources page that were confusing?**

**Were there any portions of the Resources email that were confusing?**

**Do you have any additional feedback?**

# An Empirical Comparison of Continuous and Periodic Cybersecurity Monitoring Toward Securing the Defense Industrial Base Supply Chain

**Vijay Sundararajan**

CERIAS, Dept. of Computer and Information Technology  
Purdue University  
sundar17@purdue.edu

**Arman Ghodousi**

Secure Open Solutions (SOS)  
aghodousi@secureopensolutions.com

**J. Eric Dietz**

Purdue Homeland Security Institute, Dept. of Computer and Information Technology  
jedietz@purdue.edu

**Abstract** The US Department of Defense (DoD) introduced mandatory cybersecurity compliance to secure the Defense Industrial Base (DIB) supply chain and communication with its private partners, who were obligated by the Defense Federal Acquisition Regulations (DFARS) to conform with the latest standards in computer and data security. The Cybersecurity Maturity Model Certification (CMMC) is a compliance regulation built on existing DFARS 252.204-7012 and the NIST SP 800-171 security controls. These private partners or contractors currently test their organizational networks, systems, and devices that process and/or transmit controlled unclassified information (CUI) once in three years during certification and accreditation. Two to three years is a vastly long time in an age with daily technological changes, transforming organizational cyber infrastructure and improving adversarial threats. Periodic assessments through triennial cycles are therefore not an effective method of securing the DIB supply chain, and providing near real-time security status updates would help secure any weak links between those periods. This paper discusses current literature and demonstrates how a heuristic measure of risk, the number of vulnerabilities, are drastically reduced in a continuous or real-time monitoring model as compared to a quarterly monitoring or periodic assessment model. Both these models were implemented for nine DoD contractors across two years, with the periodic model used in the first year and the continuous model in the second.

**Keywords.** continuous monitoring, risk assessment, vulnerabilities, periodic monitoring, quarterly assessments, cybersecurity, telemetry

## INTRODUCTION

As of December 1, 2020, cybersecurity is no longer optional for organizations pursuing contracts with the DoD (Atherton, 2020), with the CMMC being mandatory. CMMC has five levels of certification, where level 3 corresponds to good cyber hygiene and is mandatory for organizations dealing with CUI. CMMC level 3 encompasses all 110 NIST SP 800-171 controls along with an additional 20 controls included in three new domains or control families: Asset Management, Recovery and Situational Awareness. Assessing these 130 controls is

comprehensive and expensive, and conducting these assessments with high frequency is impractical for many organizations. These are primarily self-assessments with no mechanism for the DoD to verify the contractor’s compliance (Toth, 2017). The current CMMC/NIST SP 800-171 compliance roll-out has been met with several challenges, the main concern being that it does not fully secure the DIB supply chain. The self-assessment process and a contractor’s subjective interpretation on what is “periodic” led to a data leak (Wakeman, 2022).

Under each CMMC control family, there are basic security requirement controls that are followed by more



specific derived controls. For cybersecurity monitoring, the control families Risk Assessment and Security Assessment (3.11 and 3.12) provide the guidelines. The basic security requirement control 3.11.1 and its derived control 3.11.2 in the Risk Assessment control family focus on assessing the risk to an organization processing CUI. Control 3.11.1 states, “Periodically assess the risk to organizational operations” with no assessment frequency mentioned (Toth, 2017). NIST SP 800-137A, which provides specific guidelines for assessing an information security continuous monitoring program, mentions differing frequency requirements based on security-related information applicable to affected processes for each organization level (Dempsey et. al., 2020). This leaves room for organizations to dispute the ideal frequency for maintaining security. In this paper, an empirical comparison on the effectiveness of real-time continuous monitoring and periodic quarterly monitoring is presented. The study utilizes data from nine anonymized real-world organizations across two years (2020–2021) to give an understanding as to which method of cybersecurity monitoring provides lesser risks. The number and severity of vulnerabilities is the heuristic measure of risk used.

The rest of the paper is organized as follows. The current literature on the methods and metrics of how risk is measured, with an emphasis on the metric of vulnerabilities, is first presented. The next section presents the architecture and methodology of the cybersecurity monitoring model to measure vulnerabilities, with respect to the network topology of the organization. The analysis and interpretation of the results along with the conditions, constraints, and metrics are discussed next. The practical limitations and challenges are explained in the subsequent section, followed by the conclusion. This research was conducted through working with a compliance service provider based in Sterling, Virginia.

## MEASURING CYBERSECURITY RISK

Threats to information systems processing CUI remain a major and persistent concern in the DIB supply chain.

Yet protecting these systems against impending risks requires resources that are limited. Hence assessing the risk and understanding the “return on risk mitigation” is important. As per Hubbard and Seiersen, to mitigate the ever-increasing and constant cyber threats and utilize the limited resources optimally we must (Hubbard and Seiersen, 2016)

- come up with a risk assessment policy;
- measure reduction in risk through a mitigation, security control, or strategy/methods;
- continuously improve on implementation methods.

A Monte Carlo simulation plotting likelihood and impact scores on a risk matrix is suggested. This is visualized using a loss-exceedance curve, which shows the probability of loss based against the monetary value. An example is shown in Figure 1.

The authors explain how continuous integration and continuous deployment help reduce the probability of loss in the loss-exceedance curve. This is because of continuous and quick remediations as new developments occur. With this assertion, a continuous or real-time monitoring is favored with the resultant decrease in the risk matrix. NIST provides the definition of risk in the context of cybersecurity in the SP 800-30 document (Stoneburner et al., 2002): “Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.” Assessing this risk to information technology (IT) systems involves analysis of threats alongside potential vulnerabilities and security controls for an IT system. Compliance with NIST SP 800-171 and CMMC security controls measures reduction in risk for an organization and its systems with each fully compliant control. A high score in the NIST SP 800-171 assessment can be directly associated with lower risk. The Plan of Action & Management (POAM) is the resulting document from the risk assessment, which explains the implementation methods to mitigate the risk each

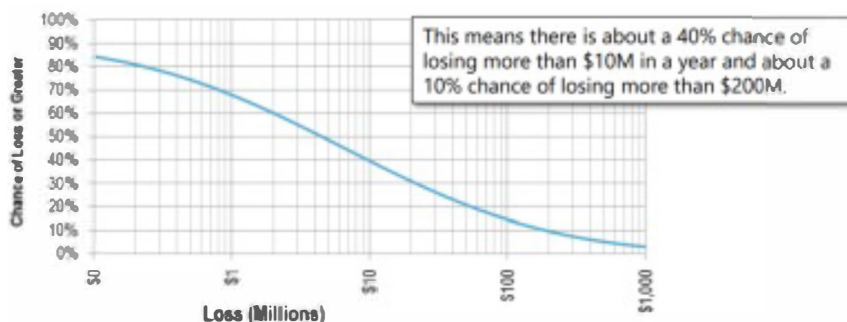


Figure 1. Loss-exceedance curve showcasing chance of losing X million dollars a year.

security control is meant to alleviate. The cybersecurity monitoring models provide a framework for the various implementation methods. With risk being a function of the likelihood of a vulnerability being exploited, the continuous monitoring model reduces the time window for an exploitation to occur, thereby reducing risk. Risk assessments must be conducted repeatedly in a periodic fashion suitable to every organization, according to NIST. The results of the implementation methods in reducing the risk are measured and improvements and changes are incorporated into the POAM. Florackis et al. in 2020 proposed a firm-level cybersecurity risk measurement framework using analysis and comparisons of organizations that were hacked and their cybersecurity risk disclosures as compared to those that were not. The organizations were US-listed firms. Further research was done to see if the risk is reflected in their stock prices. Reassuringly, the research shows that the risk exhibits a positive trend for organizations that rely extensively on information systems for their operation. This provides direct relation to future cyberattacks as well. With a larger network of information systems, cybersecurity monitoring becomes imperative.

Lee in 2021 proposed a cybersecurity risk management framework based on a constant feedback cycle to the cyber ecosystem and a cyber risk quantification to complement existing frameworks such as the NIST cybersecurity framework (Barrett, 2018) and the Cyber Kill Chain framework (Yadav and Rao, 2015). This constant feedback cycle would form the basis of a continuous monitoring model, where not only is the network monitored for vulnerabilities, but remediations can be subsequently applied in a timely manner.

Another study on cybersecurity risk for critical infrastructure in the nuclear industry was done by Shin et al. in 2015 using a risk model based on a Bayesian network. This model integrates both procedural and technical aspects of cybersecurity related to the compliance guidelines. An activity-quality analysis model is proposed that assumes that when cybersecurity activities are performed correctly following regulatory guides, the activity quality is good, and the risk is low. These activity-quality values can be updated through cybersecurity monitoring, with a periodic model more suitable as they are not subject to frequent change according to the author. As for the regulatory guides, NIST SP 800-171 is widely adopted by organizations, regardless of whether they process CUI or not. Each security control provides a data point toward estimating the risk for an organization, and with a base system security plan and POAM there is a consistent foundation and feedback to reduce risk. The CMMC builds on this, particularly focusing on CUI processing systems.

## PROPOSED ARCHITECTURE AND METHODOLOGY

A centralized architecture was implemented for cybersecurity monitoring in each of the nine organizations. These were small to midsized businesses where the architecture was implemented but can be scaled to handle larger environments. They belonged to various industries, namely, IT solutions, commercial and industrial machinery, and logistics and communication systems. This section will explain the centralized cybersecurity monitoring architecture and how it is configured for an organizational network.

### Core Block

A sample network topology used for cybersecurity analysis was presented by Nikolov and Slavyanov (2018), with testing systems conducting the analysis present in the internal network. Organizational networks these days heavily rely on firewalls (Kerner, 2018), generally opting for two types. One firewall is configured specifically to be placed in front of the servers and another is used to protect the clients (Cisco, 2022).

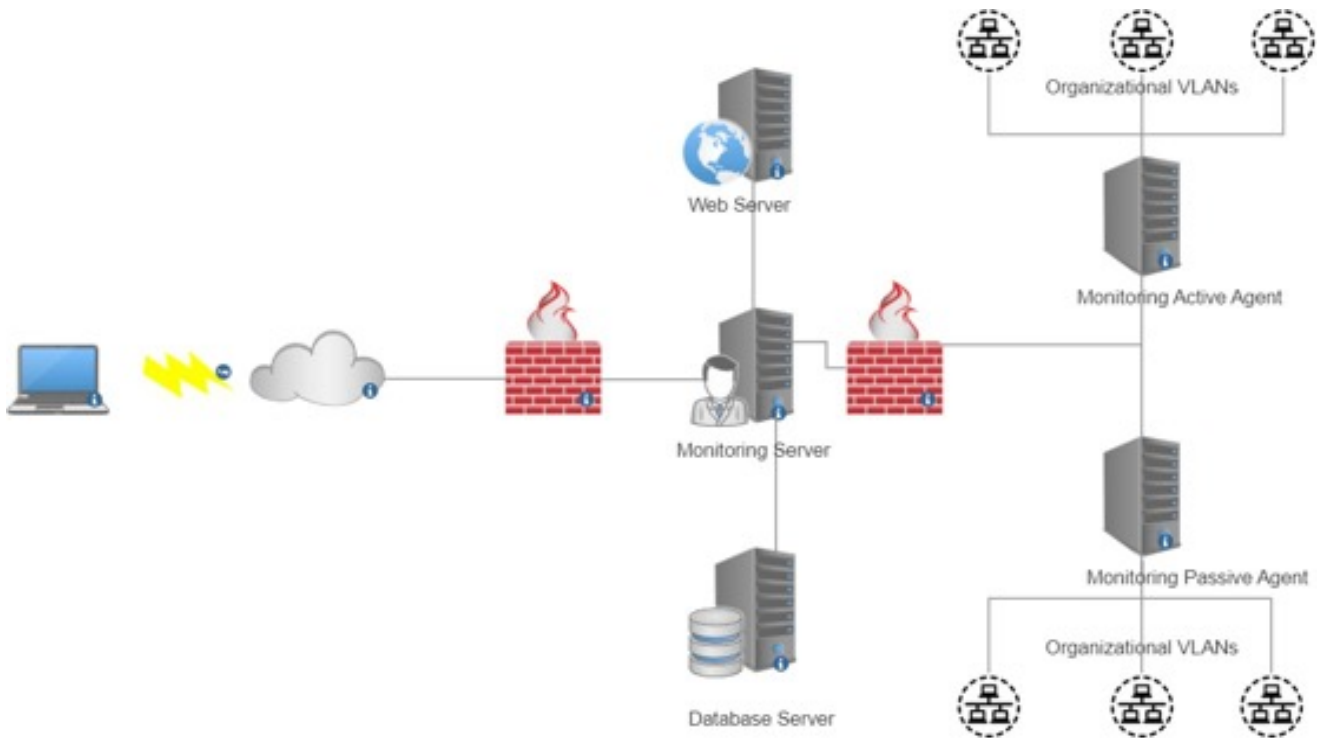
The core of the architecture is the cyber monitoring server (CMS) used for centrally gathering telemetry from organizational local area networks (LANs). This server is supported by a relational database management server (RDBMS) to store telemetry for cybersecurity monitoring, analysis, and raising events. For smaller-scale organizations for which this model was implemented, the CMS and RDBMS were integrated to the same server. The CMS and its corresponding RDBMS are placed alongside the company web server, behind the organizational firewall facing the Internet. The CMS, RDBMS, and web server form the core block, as shown in Figure 2.



Figure 2. Core block of cybersecurity monitoring architecture

### Architecture

The cybersecurity monitoring architecture consists of the core block between the external Internet-facing firewall and the client firewall. Within the internal network, proxies or agents that communicate with the server are present in each of the LANs in the organization. The agents can be active or passive proxies. Active proxies initiate communication with the server and send configuration change requests and data, whereas passive proxies request configuration details and data from the



**Figure 3.** Cybersecurity monitoring configuration used for organizational networks

server. The choice of proxy is based on the network policies. The proxies and server maintain communication regarding the status of the nodes and network. This allows internal network monitoring and vulnerability scanning. A computer outside the organization network is authorized for penetration testing to scope out vulnerabilities externally testing the firewall configurations. The complete architecture is shown in Figure 3.

### **Methodology**

Both the periodic and continuous cybersecurity monitoring models are implemented in the same architecture described. The tools and procedure used in the monitoring process were also the same but were conducted differently. For the periodic monitoring process the operations were conducted manually at quarterly intervals for each organization. Automating these processes using various scripts allowed for the monitoring to be conducted on a near real time basis. The following methods and their respective tools were used to measure vulnerabilities:

1. Internal Network Testing. A comprehensive study was done on various vulnerability scanning tools (Wang and Yang, 2017), comparing their capabilities in processing, and extracting key insights and vulnerabilities from client telemetry. Many

tools are available, such as Tenable's Nessus (Nessus, n.d.) and Greenbone's OpenVAS (Greenbone, n.d.), which are widely used across many organizations (G.P. Insights, n.d.).

2. External Network Testing. Any computer connected to the Internet outside the organizational network can be used to conduct external penetration testing, as shown in Figure 3. Kali Linux is a commonly used operating system that can be used for (Beggs, 2014)
  - (i) footprinting and reconnaissance,
  - (ii) network scanning and enumeration,
  - (iii) sniffing and evasion,
  - (iv) privilege escalation and persistent access,
  - (v) presence diminishing.
3. Log Monitoring. Log monitoring is conducted by hosting logstash servers on the monitoring agent communicating with the internal network of the organization. Any node connected to the internal network shares the required logs to the logstash servers based on the operating system of the node. These logs are then viewed through Kibana, a data visualization tool.
4. Social Engineering. Two aspects of social engineering are tested on organizations: phishing and dark web scans.

## RESULTS AND ANALYSIS

### Background

The periodic assessment was conducted once in each fiscal quarter to set up the POAM. This was accomplished in 2020 and then transitioned to the continuous monitoring model through automation for 2021. The aim of cybersecurity monitoring is to ascertain the risk to an organization. NIST defines risk as “a measure of the extent to which an entity is threatened by a potential circumstance or event and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence” (Stoneburner, 2018). Based on this definition, the formulation for calculating risk in terms of cybersecurity where the likelihood is the combination of a threat exploiting a vulnerability (Nichols et. al., 2021):

$$(\text{threat} * \text{vulnerability}) * \text{consequence} = \text{risk}$$

The heuristic measure of risk used in this paper is the number of vulnerabilities for an organizational network. The Common Vulnerability Scoring System (CVSS) assigns scores of 0 to 10 to publicly disclosed common vulnerabilities and exposures. The CVSS score for a vulnerability represents the consequence, critical vulnerabilities having higher consequences compared to high or medium vulnerabilities (Mell et al., 2006). This data is taken from all nine organizations through 2020–2021 and is anonymized.

### Extracting Significant Data

The severity of the internal network vulnerabilities is represented by their CVSS scores, as shown in Table 1. In a real-world scenario, the score can be misleading. The probability for an external threat actor to enter the internal network to exploit the vulnerabilities is low. Outcomes of penetration testing which are vulnerabilities in the external network can allow any threat actor with an Internet connection to compromise an organization. These vulnerabilities pose much higher risk as compared to high severity vulnerabilities in the internal network from an organization standpoint.

**Table 1.** Numeric ranges, categories, and colors for CVSS versions 2 and 3

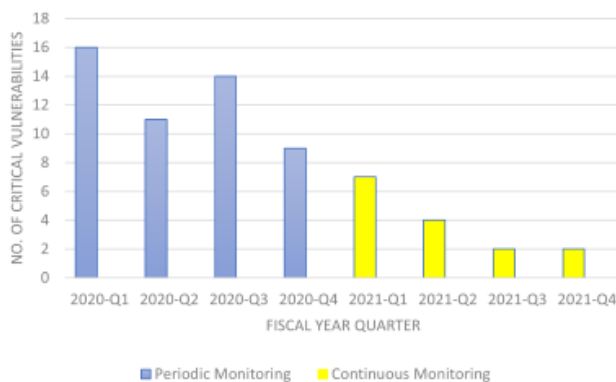
CVSS score	CVSSv2	CVSSv3
9.0 – 10.0	High	Critical
7.0 – 8.9		High
4.0 – 6.9	Medium	Medium
0.1 – 3.9	Low	Low
0.0		None

For simple and practical classification, medium-high severity vulnerabilities in the external network fall into the high-risk category. This includes successful exploits on open ports and services, successful brute force on public network facing login pages, and deprecated protocols and services. Critical and high severity vulnerabilities in the internal network are the medium category. All others are grouped and recorded as low risk and have lowest priority in the POAM.

### Periodic and Continuous Monitoring Results Analysis

For the nine aforementioned organizations, periodic cybersecurity monitoring tests were conducted once each quarter through 2020. For 2021, continuous monitoring was set up and results were taken at quarterly checkpoints for the purpose of comparison. The total vulnerabilities based on the classification mentioned in subsection B are shown in Figure 4. Although continuous monitoring was set up after fixes for vulnerabilities found through Periodic monitoring were implemented, there is a significant and consistent drop in the total vulnerabilities in 2021. For a business, a quarter or three months is sufficient for many changes in their network and systems. This leads to new vulnerabilities being found in the organizational network. The increase in the vulnerabilities in 2020 Q3 demonstrates this. In 2021, an average of 55 new software vulnerabilities were being published everyday (Cisco, 2022).

While most vulnerabilities were promptly fixed and/or patched with updates, an average of 1.67, or close to two, vulnerabilities were unfixed from the previous quarter and carried over to the next in the results data. While these are critical vulnerabilities, their complexity and the time and resources needed to remediate them were limiting factors for the organizations in addressing them. According to InfoSec Institute, the average number



**Figure 4.** Total vulnerabilities among nine organizations in 2020 with periodic monitoring and 2021 with continuous monitoring

of days to patch a vulnerability is between 60 and 150 (Morrow, 2021).

Continuous monitoring through automation allows for a quick turnaround from vulnerability discovery to fix. This is crucial in the recent cybersecurity landscape as vulnerabilities have been exploited in less than five minutes from disclosure. When Microsoft announced a zero-day vulnerability was in the exchange server, it only took five minutes before the Hafnium hacking group began its scan for vulnerabilities (Morrow, 2021). With an overall lower number of vulnerabilities and consistency across the quarters, the results indicate continuous monitoring provides better cybersecurity toward meeting compliance.

Four categories were taken into consideration when testing for vulnerabilities in order to be compliant: internal network testing, external penetration testing, log monitoring, and social engineering. The vulnerabilities discovered thus also fall into these categories and the breakdown is shown in Figure 5.

Internal network vulnerabilities constituted the majority. This is due to testing every node in the organization and scanning for critical vulnerabilities. This process is also the most comprehensive among the methods used. Log monitoring indicated the next highest number of vulnerabilities, of which invalid login attempts and misconfigured or malicious software generating massive numbers of logs were the primary causes. External network vulnerabilities were patched by the end of 2020 in Q4 via periodic monitoring efforts, and comprehensive continuous monitoring prevented any further vulnerabilities exposed to the Internet from showing up. Successful phishing emails from the 2020–2021 campaign had few successes, indicating most employees of DoD contractors were aware of commonly used phishing techniques. A large number of user names were found in the dark web scans, but credentials with clear text passwords were very few. Most organizations store user credentials with the passwords salted and hashed in their databases and these unreadable credentials are stolen and released

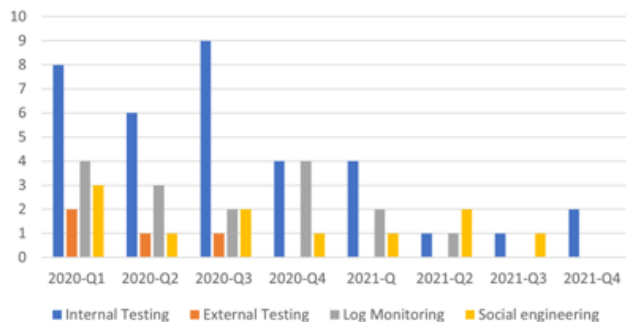


Figure 5. Vulnerabilities in Figure 4 by category

in the dark web. This is practically useless for bad actors to utilize and exploit, brute force access with just the username being the only viable exploit. Strong password guidelines with multifactor authentication prevent unauthorized access.

## LIMITATIONS AND CHALLENGES

In this section, the limitations and challenges of the implemented cybersecurity monitoring models are discussed. The major limitation is the lack of simultaneous comparison of both models, as continuous monitoring was implemented after the initial periodic monitoring. With a significant reduction of vulnerabilities in 2021 from 2020, the initial periodic monitoring improved the cybersecurity awareness of organizations. However, the impact of continuous monitoring is shown in quick discoveries and fixes. Automation also saves time and money in the long run. Another limitation is that vulnerability remediation is at the behest of the organizations. Although fixes and recommendations are suggested, the organizations set up the course of action and timeline for addressing the vulnerabilities. Continuous monitoring gives alerts and feedback quickly, so issues are addressed as soon as possible. This makes comparison at quarterly checkpoints skewed in favor of continuous monitoring.

The sample size of nine small and midsized organizations is insufficient to make general conclusions on the best cybersecurity monitoring approach toward compliance, despite representation from various industries. They can however be construed as solid recommendations. The methodology used in the models meets NIST 800-153 and CMMC level 3 control requirements but does not provide complete and total cybersecurity. A crucial component of CMMC level 3 is the incidence response procedures, which these models do not address. The human factor in making decisions in critical moments after an incident can be added to the monitoring model, but not every incident is the same.

## CONCLUSION

Hence, in this paper an empirical comparison of a periodic and continuous cybersecurity model was discussed. The results indicate that continuous monitoring provides all-around better security in safeguarding CUI and meeting compliance. Both modes reduce the number of vulnerabilities, but in the general digital landscape, the number of vulnerabilities is increasing rapidly and there are many more threat actors trying to exploit them. A study by researchers at NIST shows the significant increase in vulnerabilities from 2008 to 2016. The increasing trend of all low, medium, and high severity vulnerabilities being

listed in the US National Vulnerability Database shows us the security issues the expanding digital landscape and technology bring (Kuhn et al., 2017). Hence mandatory compliance is now being considered across the federal government, such as at the Department of Homeland Security and the Department of Energy. It is only a matter of time before cybersecurity monitoring becomes imperative across industries to prevent both financial losses and loss of credibility. To this end, more frequent or near-real-time cybersecurity monitoring is recommended, as per the research data shown in this paper.

## REFERENCES

- Atherton, K. (2020). *Starting Dec. 1, cybersecurity is no longer optional*. Breaking Defense. <https://breakingdefense.com/2020/11/starting-dec-1-cybersecurity-is-no-longer-optional/>
- Barrett, M. P., et al. (2018). *Framework for improving critical infrastructure cybersecurity version 1.1*. NIST.
- Beggs, R. W. (2014). *Mastering Kali Linux for advanced penetration testing*. Packt Publishing.
- Cisco. (2022). *How many firewalls does your business need?* SonicWall Sales. <https://www.sonicwall-sales.com/news/how-many-firewalls-does-your-business-need.html/>
- Dempsey, K. Pillitteri, V. Y., Baer, C., Niemeyer, R., Rudman, R., & Urban, S. (2020). *Assessing information security continuous monitoring (ISCM) programs* (NIST Special Publication 800).
- Florackis, C., Louca, C., Michaely, R., & Weber, M. (2020). *Cybersecurity risk* (Technical report). National Bureau of Economic Research.
- G.P. Insights. (n.d.). *Vulnerability assessment solutions*. <https://www.gartner.com/reviews/market/vulnerability-assessment>
- Greenbone Networks. (n.d.). *OpenVAS*. <https://www.openvas.org>
- Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. John Wiley & Sons.
- Kerner, S. M. (2018). *94 percent of organizations see firewalls as critical infrastructure*. <https://www.eweek.com/security/94-percent-of-organizations-see-firewalls-as-critical-infrastructure/>
- Kuhn, D. R., Raunak, M. S., & Kacker, R. (2017). An analysis of vulnerability trends, 2008-2016. In *Proceedings of the International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 587–588). IEEE.
- Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659–671.
- Mell, P., Scarfone, K., & Romanosky, S. (2006). Common vulnerability scoring system. *IEEE Security & Privacy*, 4(6), 85–89.
- Morrow, S. (2021). *Time to patch: Vulnerabilities exploited in under five minutes?* <https://resources.infosecinstitute.com/topic/time-to-patch-vulnerabilities-exploited-in-under-five-minutes>
- Nessus. (n.d.). Tenable. <https://www.tenable.com/products/nessus>
- Nichols, C., Stoker, G., & Clark, U. (2021). Heuristic evaluation of vulnerability risk management leaders' presentations of cyber threat and cyber risk. In *International Conference on Human-Computer Interaction* (pp. 212–225). Springer.
- Nikolov, L., & Slavyanov, V. (2018). Network infrastructure for cybersecurity analysis. In *Proceedings of the International Scientific Conference*.
- Shin, J., Son, H., Khalil R., & Heo G. (2015). Development of a cybersecurity risk model using Bayesian networks. *Reliability Engineering & System Safety*, 134, 208–217.
- Stoneburner, G., Goguen, A., Feringa, A., et al. (2002). *Risk management guide for information technology systems* (NIST Special Publication 800-30). National Institute of Standards and Technology, US Department of Commerce.
- Toth, P. (2017). *NIST MEP cybersecurity self-assessment handbook for assessing NIST SP 800-171 security requirements in response to DFARS cybersecurity requirements*. National Institute of Standards and Technology, US Department of Commerce.
- Wakeman, N. (2022). *How CMMC raises legal exposures for contractors and their suppliers*. Washington Technology. <https://washingtontechnology.com/companies/2022/11/how-cmmc-raises-legal-exposures-contractors-and-their-suppliers/379821/>
- Verizon data breach investigations report. (2022). <https://www.verizon.com/business/resources/Td46/reports/dbir/2022-data-breach-investigations-report-dbir.pdf>
- Wang, Y., & Yang, J. (2017). Ethical hacking and network defense: Choose your best network vulnerability scanning tool. In *Proceedings of the 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (pp. 110–113). IEEE.
- Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. In *International Symposium on Security in Computing and Communication* (pp. 438–451). Springer.

# A Natural Approach for Synthetic Short-form Text Analysis

Ruiting Shao,<sup>1</sup> Ryan Schwarz,<sup>1</sup> Christopher Clifton, and Edward J. Delp

Video and Image Processing Laboratory (VIPER)

School of Electrical and Computer Engineering

Purdue University

shao72@purdue.edu, schwarzr@purdue.edu, clifton@cs.purdue.edu, ace@ecn.purdue.edu

**Abstract** Detecting synthetically generated text in the wild has become increasingly difficult with advances in natural language generation techniques and the proliferation of freely available large language models (LLM). Social media and news sites can be flooded with synthetically generated misinformation via tweets and posts, while authentic users can inadvertently spread this text via shares and retweets. Most modern natural language processing techniques designed to detect synthetically generated text focus primarily on long-form content, such as news articles, or incorporate stylometric characteristics and metadata during their analysis. Unfortunately, for short-form text like tweets, this information is often unavailable, is usually detached from its original source, is displayed out of context, and is often too short or informal to yield significant information from stylometry. This paper proposes a method of detecting synthetically generated tweets via a Transformer architecture and incorporating unique style-based features. Additionally, we have created a new dataset consisting of human-generated and LLM-generated tweets for four topics.

**Keywords.** natural language processing, natural language generation, synthetic text detection, twitter

## INTRODUCTION

The impact of general misinformation and bot-generated text has been witnessed on a large scale in the last decade. In 2014, Twitter was flooded with an army of bots tweeting about a small technology company, Cynk (Ferrara et al., 2016). This flurry of artificial posts created a large amount of chatter, which automatic trading scripts attempted to capitalize on. This led to the stock price inflating by over 500%. When it was discovered that the original social media posts were synthetic, the stock price responded by decreasing below its original value, trading was halted, and unfortunate investors were left to realize massive financial losses. In 2016, both the US presidential election and the Brexit referendum were believed to have been partially influenced by Twitter bots (Gorodnichenko et al., 2021).

Although currently most discovered bot activity incorporates manually written sentences rather than model-generated ones (Vargo et al., 2018), with the proliferation and availability of robust large language models (LLMs), such as ChatGPT, it is highly likely that future bot activity will include some combination of synthetic and human-generated sentences.

Language generation can easily be structured as a product of conditional probabilities lending to its sequential nature (Radford et al., 2019).

$$p(x) = \prod_{i=1}^n p(s_i | s_1, s_2, \dots, s_{n-1}) \quad (1)$$

where  $x$  represents a sample of generated text and is represents individual tokens as the  $i$ th location. With the invention and popularity of self-attention architectures, such as the transformer (Vaswani et al., 2017), many language models have been created that can estimate these probabilities with sufficient prose and verbosity. While the transformer uses an encoder-decoder structure to understand language, popular models such as the Generative Pretrained Transformer (GPT) series from OpenAI and BERT (Devlin et al., 2018) make use of either the encoder or the decoder for increase performance in certain tasks.

Detecting short-form text generated by an LLM is a relatively unexplored and challenging task for many applications. Previous work on general synthetic text detection, such as GROVER, incorporate a transformer-based architecture as both a generator and a detector on paragraph and article-length text sequences (Zellers et al., 2019). This is helpful in the context of determining the validity of a news article attempting to spread propaganda or a long-form social media post containing misinformation, but it relies heavily on the stylometric features of the given text. The shorter the sequence of text becomes, the less importance the same stylometric features have in aiding in a classification (López-Escobedo et al., 2013).

Recently, the unique TweepFake dataset has been created specifically for the purpose of synthetic tweet detection and attribution to specific bot and human authors (Fagni et al., 2021). While high accuracy was achieved by BERT-based classifiers such as RoBERTa (Liu et al., 2019) the data chosen largely comprised authentic human accounts and bots impersonating those humans, making the dataset more effective when analyzing detection in the context of a specific, well-known user. Other variations of BERT, such as BERTAA (Fabien et al., 2020), have also proved successful at the tangential task of authorship attribution on similar datasets.

In similar work, tweets across a Twitter user’s timeline were collected and analyzed for potential synthetically generated samples (Kumarage et al., 2023). The authors analyzed timelines consisting of wholly synthetic or authentic tweets, placing emphasis on determining a point in a timeline where tweets became synthetic, in the event of an account hijacking. Intuitively, this work showed that the shorter the timeline, the harder it is to accurately classify the synthetic text. This is likely due to less overall text, leading to a lower amount of semantic information for the model to learn. The authors did note, however, that for lower values of timeline transition point, there was an increase in benefit from infusing external stylometric features compared to using word embedding and bag-of-word representations.

Incorporating metadata into detection methods can greatly improve a classifier’s results (Hovy, 2016); however, this data is not always available. A synthetically generated tweet can often be incorrectly attributed to a legitimate author, spread by legitimate users through retweets and shares, or displayed independently of Twitter altogether via articles, news reports, and memes. These factors make it difficult to rely on external features derived from metadata in a realistic scenario.

Work such as that by Sadasivan et al. (2023) further examines the difficulties of detecting artificial intelligence-generated text and describes the problem in terms of a given classifiers area under receiver operator characteristic (AUROC):

$$AUROC(D) \leq \frac{1}{2} + TV(M, H) - \frac{TV(M, H)^2}{2} \quad (2)$$

where  $D$  represents a synthetic text detector,  $TV$  references the total variation distance between two distributions, and  $M, H$  represent the distributions of machine-generated and human-generated samples, respectively. As the  $TV$  distance shrinks, or two distributions become more similar, any classifier  $D$  will tend toward a random classifier. Shorter text, which has less unique characteristics between synthetic and human-generated text, inherently reduces  $TV$  distance and thus detector accuracy.

This difficulty even extends to watermarked text, such as the work presented by Kirchenbauer et al. (2023). Watermarking techniques attempt to apply a machine-detectable watermarked pattern to text generated by an LLM while hiding the pattern from the average human reader. Popular techniques involve dividing the vocabulary  $|V|$  of an LLM evenly into a red and green list of tokens. In a hard watermarking scheme, only the green tokens will be considered during token generation. This has the effect of providing an easily detectable pattern, with the trade-off of sentence verbosity. The more popular soft watermarking scheme samples from the green tokens inverse to the entropy from a given prompt. The phrase “The quick brown fox,” for example, has an incredibly low entropy with an almost deterministic completion of “jumps over the lazy dog.” Therefore, even if one of the completion tokens is on the red list, it will likely be chosen, whereas a prompt with relatively high entropy is almost certain to generate a token from the green list.

In this case, detection simply involves comparing the number of tokens seen in a sample with the red list tokens. Because the lists are evenly divided, a human-generated sample will utilize approximately 50% from the red list, while the watermarked model will utilize almost none. A simple  $p$ -score threshold provides a highly accurate detector of the applied watermark. Unfortunately, these types of schemes are susceptible to spoofing attacks. A malicious actor, with sufficient access to known watermarked text, can recreate the green list tokens with a high degree of accuracy (Sadasivan et al., 2023).

In this paper, we seek to explore a method of synthetic text detection of tweets via an ensemble of reasonable stylistic features incorporated with an LLM-based language model.

## DATASET

To accurately test our detection method on short-form text, we created a new dataset consisting of synthetically generated tweets from three popular LLMs: GPT-J 6B (Wang and Komatsuzaki, 2021), GPT2 (Radford et al., 2019), and GPT3 (Brown et al., 2020). Using the Twitter API, we extracted approximately 300k tweets across four diverse categories: politics, science, climate, and COVID. These tweets were selected from primarily verified Twitter accounts between 2016 and 2021, and the categories were selected according to various hashtags and keywords as shown in Table 1.

We then used the corresponding APIs, provided by OpenAI, to fine-tune the three LLMs on randomly selected samples of 5,000, 10,000, and 15,000 human-generated tweets from each of the four categories. These fine-tuned models were then used to generate 20,000



**Table 1.** Category of harvested tweets, search words, and corresponding number of tweets

Category	Key Words	Size
Politics	#Trump, #DonaldTrump	20k
Science	#Science, #Engineering, #Physics, #Biology, #Chemistry	36k
Climate	#Climate, #GlobalWarming, #ClimateChange	54k
COVID	#Coronavirus, #COVID, #COVID-19	195k

synthetic tweets each. GPT2 and GPT3 could generate convincing tweets with no input prompt, while GPT-J 6B required the first 10 words of the GPT3-generated text as a prompt for completion. Both the human-generated and the synthetically generated tweets contain English words and sentences as well as emojis, Twitter links, and unique punctuation such as the Twitter hashtag.

We also evaluate our method on a TweepFake dataset that contains deepfake tweets that are generated based on Markov chains, recurrent neural networks, long short-term memory networks, GPT2, and other technologies.

## METHOD

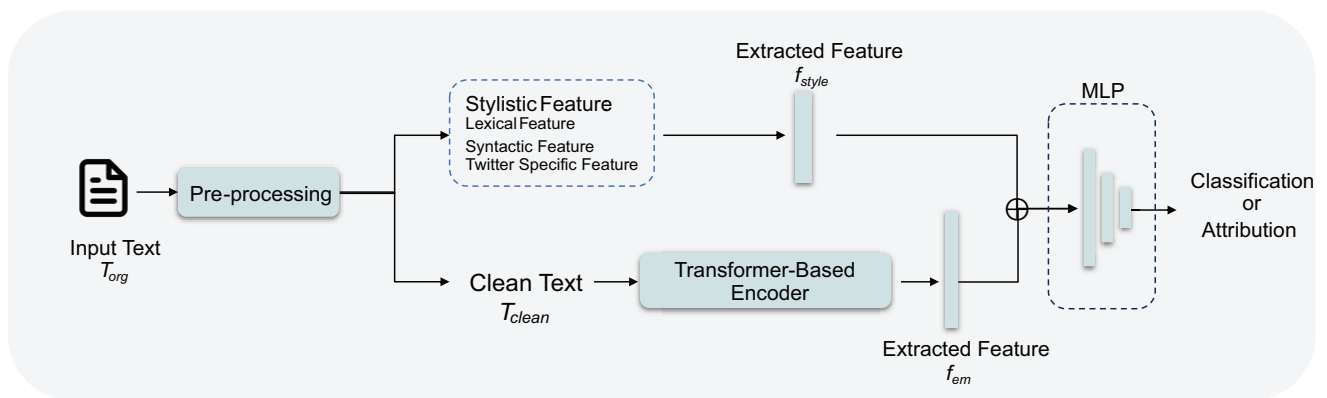
The structure of the proposed system is illustrated in Figure 1. The input tweet  $T_{org}$  will first be normalized, removing noise information (like URLs and mentions) to get a cleaned tweet  $T_{clean}$ . At the same time, we will perform preliminary statistic calculations based on the original input tweet, such as word count per sentence, average word length, and lexical richness. In addition to this, we also perform lexicographic processing and syntax analyzing on input tweets. The most popular machine learning techniques, such as bag-of-words,  $n$ -gram, and TF-IDF, help convert text into dictionary-based statistical features. Since we want to extract intrinsic stylistic

features of the synthetic tweets, which should be content independent, we choose to use a character-level  $n$ -gram and a part-of-speech (PoS) tag  $n$ -gram as part of our self-defined stylistic features. Here we introduce the PoS tag  $n$ -gram as a rule-based matching feature. It helps us to extract and classify different writing patterns in phrases. Besides this, we are also curious about the emojis shown in tweets. According to Emojipedia’s statistics (Broni, 2022), by 2022, more than 22.4% of all tweets contained at least one emoji, while more than half of the comments on Instagram included emojis. Emojis are an easy and concise way to express emotion and convey meaning, so it should also be a feature used to detect synthetic tweets. Thus, the extracted stylistic features  $f_{style}$  can be categorized into three types: Twitter-specific feature, lexical feature, and syntactic feature. Table 2 gives detailed information of the self-defined stylistic feature.

Then a contextualized feature  $f_{em}$  will be extracted from the cleaned tweet  $T_{clean}$  by a transformer-based encoder. Here we choose to use RoBERTa for two reasons: (1) it is a powerful and effective language model that achieves a good performance in a variety of NLP sub-tasks, and (2) it uses byte-pair encoding (Gage, 1994) for text encoding, which enables the encoding of any rare words in the vocabulary with appropriate subword tokens without introducing any “unknown” tokens. This is important for Twitter posts since they may contain some nondictionary phrases or abbreviations.

The stylistic feature  $f_{style}$  and contextualized feature  $f_{em}$  will be concatenated together to form a new feature vector and fed into a multilayer perceptron for detection of human-generated and synthetic tweets.

During the training time, we will first build and memorize character-level and PoS tag  $N$ -grams dictionaries based on the training dataset. We will use these to calculate the corresponding feature vectors in training and testing phrases.



**Figure 1.** The block diagram of the proposed method

**Table 2.** List of extracted self-defined stylistic features

Type	Size	Descriptions	Examples
Twitter specific feature	10	Statistical features based on Twitter-specific features	Total emoji count, unique emoji count, emoji repeated times, emoji frequency, emoji richness, email count, hashtag count, mention count, hashtag frequency, mention frequency
Lexical feature	122	Stylistic features based on characters and words	Word length, word count, sentence count, character count, word frequency, digits counts, upper case word count, vocabular richness, character level ngram, contractions, count, readability
Syntactic feature	136	Stylistic features based on the organization of sentences	Stop words, count, stop word frequency, special punctuation frequency, proper noun count, noun count, Part-of-Speech (PoS) tag ngram

## EXPERIMENTS

We first conduct an experiment to determine how to preprocess the emojis in the text using three approaches: remove emojis directly, encode emojis directly, and use emoji descriptions instead. We tested the three preprocessing approaches with a RoBERTa model on our dataset and found that encoding emojis directly or using emoji description instead can achieve  $\sim 1.4\%$  accuracy over removing all emojis entirely. The accuracy for encoding emojis directly and using emoji description instead was about the same, with  $\sim 0.1\%$  difference. We will directly encode the emojis for the experiments.

To show the advantage of our proposed method, we conduct experiments on the synthetic tweets dataset we designed and the TweepFake dataset for comparison. Our proposed method is implemented in PyTorch and trained using the adaptive moment estimation (Adam) optimizer with a start learning rate of  $5e-4$  and weight decay of  $0.001$ . To prevent overfitting from happening in the training phase, we use two strategies: (1) an early

stop execution will take place if five successive epochs stop improving on validation loss, and (2) label smoothing is implemented in cross-entropy loss function (Szeged et al., 2016).

Table 3 shows the results for synthetic tweets detection with different stylistic feature setups on the TweepFake dataset. In this experiment, we isolate the stylistic features into three portions, preliminary statistical features, character-level N-gram, and PoS N-gram, to check the effectiveness of these features. Here we use RoBERTa fine-tuned on the TweepFake dataset as a baseline. Experimental results show that stylistic feature can help to improve the performance of synthetic tweet detection.

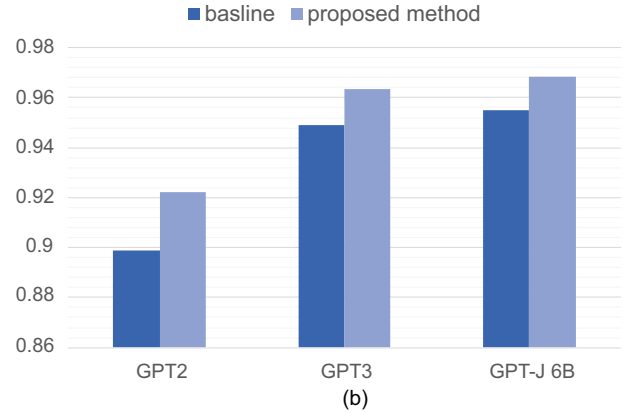
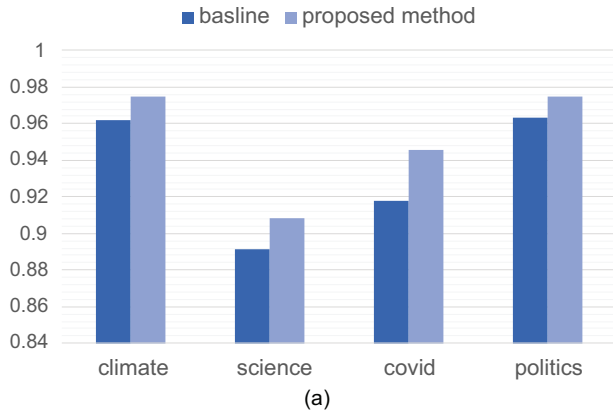
Table 4 shows the results for synthetic tweets detection on the generated synthetic tweets dataset. Here the stylistic features are the combination of preliminary statistical features, character-level N-gram, and PoS N-gram, i.e., the full stylistic features described in Table 1. Figure 2 presents a more detailed evaluation on different topics and different generative models. It indicates that the

**Table 3.** Performance of the proposed method testing on the TweepFake dataset for synthetic tweets detection

	Accuracy	Precision	Recall	F1
RoBERTa (baseline)	0.88398	0.87488	0.90313	0.88878
RoBERTa + prelim	0.92205	0.92293	<b>0.92564</b>	0.92428
RoBERTa + prelim + char	0.92257	0.92383	<b>0.92564</b>	0.92473
RoBERTa + prelim + char + PoS	<b>0.92461</b>	<b>0.93209</b>	0.91842	<b>0.92521</b>

**Table 4.** Performance of the proposed method testing on the Generated Synthetic Tweets Dataset for synthetic tweets detection

	Accuracy	Precision	Recall	F1
RoBERTa (baseline)	0.93432	0.91678	0.95535	0.93567
RoBERTa + stylistic feature	<b>0.95136</b>	<b>0.94155</b>	<b>0.96248</b>	<b>0.95190</b>



**Figure 2.** A more detailed inspection of synthetic tweet detection results. (a) Detection accuracy on different topics; (b) detection accuracy on different generative models.

**Table 3.** Performance of the proposed method on generated synthetic tweets dataset for generative attribution identification

	RoBERTa (baseline)	RoBERTa + stylistic feature
Human	0.9599	<b>0.9668</b>
GPT2	<b>0.8965</b>	0.8835
GPT3	0.9042	<b>0.9123</b>
GPT-J 6B	<b>0.9739</b>	0.9718
Avg.	0.9363	<b>0.9419</b>

proposed method will generally improve performance regardless of the generative models and content.

We also conduct a preliminary experiment on the generative model attribution task using our method on our generated synthetic tweets dataset. In this task, the goal is to determine which generative model is used to create the synthetic tweets. In Table 3, we compared the accuracy score of our method to the baseline. The results indicate that the proposed method shows some improvement in human-generated and GPT3 attribution identification, but performs slightly worse in the GPT2 and GPT-J 6B cases. Overall, the proposed method achieves higher balance accuracy than the baseline.

## CONCLUSION

In this paper, we create a dataset of synthetic tweets on four different topics utilizing three popular LLMs (GPT2, GPT3, and GPT-J 6B). We also introduced a method that exploits the efficiency of certain stylistic features combined with popular LLM models. We validated this method by pretraining the model on a public dataset (TweepFake) and our generated dataset. The pretrained models perform well for both the synthetic text detection and generative model attribution tasks.

Future work in this area will explore improved feature integration in a zero-shot setting, in order to detect synthetic tweets generated by unknown LLMs. Additionally, further experimentation will be conducted regarding the generative model attribution task, to evaluate how malicious activity such as watermark spoofing and paraphrasing attacks affect classifier accuracy and to improve defenses against these activities. As LLMs expand and open-source tools continue to be built utilizing them, the tasks of detecting and attributing synthetically generated text will continue to be important.

## ACKNOWLEDGMENTS

This material is partially based on research sponsored by DARPA and the Air Force Research Laboratory (AFRL) under agreement FA8750-20-2-1004. The US government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA and AFRL or the US government. Address all correspondence to Edward J. Delp, [ace@ecn.purdue.edu](mailto:ace@ecn.purdue.edu).

## NOTE

1. Equal contribution

## REFERENCES

- Broni, K. (2022). Global emoji use reaches new heights. Retrieved June 17, 2023, from <https://blog.emojipedia.org/global-emoji-use-reaches-new-heights/>
- Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell,

- A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D., Wu, J., Winter, C., Hesse, C., Chen, M., Sigler, E., Litwin, M., Gray, S., Chess, B., Clark, J., Berner, C., McCandlish, S., Radford, A., Sutskever, I., & Amodei, D. (2020). Language models are few-shot learners. *Advances in Neural Information Processing Systems*, 33, 1877–1901.
- Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2018). *BERT: Pre-training of deep bidirectional transformers for language understanding*. <https://arxiv.org/abs/1810.04805>.
- Fabien, M., Villatoro-Tello, E., Motlicek, P., & Parida, S. (2020). BertAA: Bert fine-tuning for authorship attribution. In *Proceedings of the 17th International Conference on Natural Language Processing* (pp. 127–137).
- Fagni, T., Falchi, F., Gambini, M., Martella, A., & Tesconi, M. (2021). Tweepfake: About detecting deepfake tweets. *PLOS One*, 16(5), e0251415
- Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, 59(7), 96–104.
- Gage, P. (1994). A new algorithm for data compression. *C Users Journal*, 12(2), 23–38.
- Gorodnichenko, Y., Pham, T., & Talavera, O. (2021). Social media, sentiment and public opinions: Evidence from# Brexit and# USElection. *European Economic Review*, 136, 103772.
- Hovy, D. (2016). The enemy in your own camp: How well can we detect statistically-generated fake reviews—an adversarial study. In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics*, Vol. 2 (pp. 351–356).
- Kirchenbauer, J., Geiping, J., Wen, Y., Katz, J., Miers, I., & Goldstein, T. (2023). *A watermark for large language models*. <https://arxiv.org/abs/2301.10226>.
- Kumarage, T., Garland, J., Bhattacharjee, A., Trapeznikov, K., Ruston, S., & Liu, H. (2023). *Stylometric detection of AI-generated text in Twitter timelines*. <https://arxiv.org/abs/2303.03697>.
- Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., Levy, O., Lewis, M., Zettlemoyer, L., & Stoyanov, V. (2019). *Roberta: A robustly optimized BERT pretraining approach*. <https://arxiv.org/abs/1907.11692>
- López-Escobedo, F., Méndez-Cruz, C.-F., Sierra, G., & Solórzano-Soto, J. (2013). Analysis of stylometric variables in long and short texts. *Procedia—Social and Behavioral Sciences*, 95, 604–611.
- Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). *Language models are unsupervised multitask learners*.
- Sadasivan, V. S., Kumar, A., Balasubramanian, S., Wang, W., & Feizi, S. (2023). *Can AI-generated text be reliably detected?* <https://arxiv.org/abs/2303.11156>.
- Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., & Wojna, Z. (2016). Rethinking the inception architecture for computer vision. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 2818–2826).
- Vargo, C. J., Guo, L., & Amazeen, M. A. (2018). The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. *New Media & Society*, 20(5), 2028–2049.
- Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, 30.
- Wang, B., & Komatsuzaki, A. (2021). *GPT-J-6B: A 6 billion parameter autoregressive language model*. Retrieved June 18, 2023, from <https://github.com/kingoflolz/mesh-transformer-jax>.
- Zellers, R., Holtzman, A., Rashkin, H., Bisk, Y., Farhadi, A., Roesner, F., & Choi, Y. (2019). Defending against neural fake news. *Advances in Neural Information Processing Systems*, 32.

## A Data-Driven Approach to Digital Literacy

Alexis Bradstreet and Nicolas Starck

United States Military Academy

alexis.bradstreet@westpoint.edu, nicolas.starck@westpoint.edu

**Abstract** Strategic competition between nations is increasingly unfolding in the global information environment. As such, the national security and defense workforce is exposed to various types of information attacks, including online mis- and disinformation. This awareness has led to the adoption of digital literacy interventions within defense and academic organizations. While this is a positive initial response, without a quantitative understanding of the misinformation susceptibility across the workforce or the efficacy of the interventions, the selection process is entirely subjective and not tailored to the differing needs within the defense workforce. To address this gap in the current approach to digital literacy, we conducted a study to evaluate the misinformation susceptibility of 228 cadets at the United States Military Academy from January to April 2023. As part of this study, we evaluated the efficacy and durability of a popular digital literacy intervention, the Bad News game. We demonstrated a practical quantitative methodology for the evaluation of a digital literacy intervention tailored to a population. Based on our findings in this study, we propose a novel quantitative methodology for the selection and implementation of tailored digital literacy interventions for the defense workforce.

### INTRODUCTION

Throughout the past decade, we have witnessed the appearance of intensified strategic competition between the United States and emerging regional hegemony in Eurasia—namely the People’s Republic of China and the Russian Federation. A fundamental aspect of this strategic competition is the contest for power and influence in the international system (Mazarr, 2021) which is captured in a “Key Theme” and an “Emerging Dynamic” in the Office of the Director of National Intelligence’s Global Trends 2040 report. A significant portion of this strategic competition is unfolding in the information environment. As such, there has been an increase in focus by defense and academic institutions on the threat that mis- and disinformation poses to our national security (Keenan, 2022). This focus has led to an increase in the search for and adoption of digital literacy interventions within such institutions. The goal of these interventions is to improve the resilience of individuals to the range of challenges that they face across platforms and media types.

This effort has resulted in a variety of approaches by a range of organizations. For example, the Department of State’s Global Engagement Center funded the development and promotion of Cat Park—a video game-style digital literacy intervention available in four languages (Games, 2023). The Department of Defense developed a joint Influence Awareness training that takes a more traditional military training approach. At the United States Military Academy, cadets may enroll in an optional course, RS103, Information Literacy and Critical Thinking. Within

academia, digital literacy interventions like the Bad News game are used across the world, are translated into many languages, and are supplemented with instructions and fact sheets for educators. These responses share the general goal of improving resilience to an antagonistic information environment, but they adopt different principles of change, methods of delivery, and duration to reach that goal. While this diversity in approaches is useful to search for a solution to the complex challenge of threats in the information environment, there is a consistent lack of deliberate quantification. This gap exists in both scoping the problem—identifying the extent to which individuals are susceptible to this information—and measuring the effectiveness of the interventions. Without this quantification, there is no way to determine if these efforts are addressing a perceived but nonexistent problem, are addressing a real problem but ineffectively, or are the ideal approach to a very real problem.

### THE CHALLENGE

Given the potential strategic importance of the information environment among a host of competitive threats, bringing a deliberate and data-driven approach to bear is crucial. With data informing many government, corporate, and individual decisions, the subjective and resource intensive approach to the information environment is a notable outlier. Despite the differing needs within the defense workforce, the selection of digital literacy interventions is subjective rather than data-driven. We believe that the process of deploying a

digital literacy program can be improved by adopting a quantitative approach in two areas: the characterization of the population's susceptibility to the information environment and the testing and selection of a digital literacy intervention.

Quantifying the initial information posture, or susceptibility, of the members of an organization is a crucial first step in any digital literacy response. Without this baseline understanding of the nature of their information vulnerability, organizations are left to commit resources toward an undefined problem with interventions that may be counterproductive to their goals. Take, for example, an organization whose population is predisposed to be highly skeptical. In this instance, an improvement in digital literacy for this population might look like a reduction in skepticism of real news. By contrast, another organization may have members who are more likely to trust any information they read online. For this population, an improvement in digital literacy may focus on increasing skepticism. Without this baseline quantitative understanding of their population's initial susceptibility, these notional organizations may select a popular digital literacy intervention that may be ineffective or even counterproductive for their situation.

Once an organization has quantified their susceptibility to the information environment, they must then select an appropriate digital literacy intervention. Given the variability in susceptibility and goals across organizations, there is no "one size fits all" approach to digital literacy. At the organizational level there is a wide range of factors, like population size and goals, that may favor different approaches. For example, in a small organization of like-minded individuals, a single digital literacy intervention may be an effective and efficient solution. However, this may not hold true for a large organization like the US Army with a wide range of subpopulations such as cadets, AIT soldiers, officers, DA civilians, and senior NCOs—each with their own educational experience and levels of institutional trust. In this case, a single intervention may be efficient but not *effective*. Each organization will need to use its understanding of their population's susceptibility and their organizational goals to evaluate and implement a digital literacy intervention tailored to their situation. Rather than prescribe a specific digital literacy program, in the following section we will describe a deliberate, data-driven methodology toward the challenge of mis- and disinformation and the factors that an organization may consider in making that decision.

## THE METHODOLOGY

The goal for our proposed methodology is to introduce quantitative rigor to the evaluation and implementation

of digital literacy interventions. As this is an emerging field of study and practice, we did not aim to develop an exhaustive methodology. Rather, our goal was a practical process to serve as a starting point for organizations, especially in defense and academia. At a high level, our methodology is simple but aims to build experience and understanding of the domain over time. The five steps are the identification of a population to receive the intervention, the selection of a method of evaluation, an initial assessment of the population's digital literacy, identification of a goal for digital literacy intervention, and iterative testing of the intervention(s). These steps provide an overall structure that can and should be adapted to suit each organization's situation and needs.

### *Identify Population*

The first step in our proposed methodology is to identify the population intended to receive the digital literacy intervention. The greatest concern during this step is ensuring that the population is adequately sized so that researchers may generalize their findings to the entire population. Our recommendation is that researchers should identify a population large enough to support statistically significant findings but also capture demographics or other attributes that vary within the population (such as age, occupation, education, or unit) that will allow later segmentation, comparison, and correlative investigation. In initial iterations of this methodology, this may include the organization's entire workforce or students in a certain age range. This has the practical benefit of providing a broad understanding in the initial stages of development while further refinement and tailoring can occur in the future.

### *Method of Evaluation*

The next step is to select the method of evaluation, which will provide a quantifiable baseline measurement of misinformation susceptibility against which researchers can evaluate their chosen interventions. Many tests of misinformation susceptibility used in digital literacy studies consist of news items that the participant evaluates as true or false (Roozenbeek et al., 2022). We believe the primary consideration at this stage is the type of news items used in the test. These may consist of news headlines, news headlines with images and media, Twitter or social media posts, memes, and more. Each capture misinformation and digital literacy differently. A news headline, for example, measures the participant's ability to discern false text from true text. A news headline paired with images, however, also measures whether the media associated with the text influences the participant. We recommend that the study investigator consider these differences as they choose a method of evaluation that

best matches the priorities for their population. An organization could, for example, select a test that uses news items reflecting the predominant form of media used within that organization. They could also select a news item based on the typical media usage of the selected population, as it better represents the primary source of that population's information.

Another consideration is the scoring system used in the method of evaluation. While some methods of evaluation capture just the overall ability to discern true from false news (like one would, for example, grade the results of a school examination), others capture more than one score—such as the separate abilities to detect real and fake news. Additionally, variation also exists in how the questions are framed. Most commonly, tests ask the participant to evaluate the news items' accuracy; however, other tests might ask the participant to evaluate the news items' reliability and trustworthiness. Research shows, though, that a strong association exists between these judgments (Roozenbeek et al., 2022).

The final consideration we will discuss (though there are others) is the substance of the news items in the method of evaluation—to include their cultural and political context. Some means of evaluation—like the one developed in a 2020 study evaluating coronavirus-related misinformation—used actual fake news content (Roozenbeek et al., 2020). Meanwhile, other tests like MIST-20 use synthetic fake news headlines created by language models (in MIST's case, GPT-2), which replicate common mis- and disinformation techniques (Maertens et al., 2021). This is an important consideration as real-world news items may be more likely to trigger existing beliefs within a population—especially if the method then labels those existing beliefs as false. This may be a useful test for an organization to gauge its population's views on real-world issues in the current cultural and political climate, though it is not without risk. By contrast, synthetic content may be less likely to trigger existing beliefs, though this might less accurately capture how their population would interact in the real world. Ultimately, this decision will rely on the organization's goals for its digital literacy program.

These considerations—type of news item, scoring system, and context of news item—should all inform the ultimate decision of whether to create a method of evaluation or use a pre-existing one. We recommend that organizations utilize existing methods if one exists that satisfies the organization's preferences. This is because research in misinformation susceptibility already suffers from a lack of standardization and cross-study comparability (Roozenbeek et al., 2022). However, neither of these goals could have been reliably developed without understanding the populations' initial disposition.

### ***Initial Evaluation***

Once the study investigator chooses the method of evaluation, the next step is to record an initial evaluation of the given population's digital literacy. This measurement is crucial because it provides a baseline understanding of the population's digital literacy before intervention. This baseline will be used in later steps to measure the efficacy of the chosen digital literacy interventions. It may also be used as a covariate for future research or comparison between different populations of interest.

### ***Goal Identification***

After reviewing the results of the baseline evaluation, the investigator will identify the quantitative goal of the future digital literacy before intervention. It is at this point that the researcher must define what an improvement in digital literacy looks like. It is crucial that this goal is informed by the baseline evaluation. Recall the two notional populations we introduced earlier: the highly skeptical population and the highly naïve population. Both populations require different treatment to improve their digital literacy (an increase in trust in real news and a decrease in trust in fake news, respectively). However, neither of these goals could have been reliably developed without understanding the populations' initial disposition.

### ***Iterative Testing***

Once the study investigator determines the goals of the intervention, he or she may select the specific digital literacy interventions. We propose several considerations for this decision, to include the number of interventions to be evaluated, the duration of each intervention, and the compatibility between the interventions and method of evaluation. The number and duration of interventions are particularly important when dealing with a limited sample size. Because each individual intervention is its own treatment condition, an increase in the number of tested interventions is inversely related to the sample size available for each treatment group. Furthermore, we theorize that longer interventions will result in higher attrition rates and thus produce lower sample sizes. The most important consideration is whether the selected interventions are compatible with the method of evaluation. This means, in other words, whether the efficacy of the digital literacy interventions in question will be captured by the method of evaluation. The efficacy of an intervention that teaches its participants to critically evaluate images, for example, might not be captured by a test that uses news headlines.

Next, the study investigator should evaluate the efficacy of the chosen interventions by administering them to their participants and re-evaluating their misinformation susceptibility immediately thereafter. Researchers

could also repeat this step at selected intervals to evaluate the durability of the chosen interventions over time. These results should inform the optimal frequency of future training. While many organizations, including the army, often conduct training on an annual basis, studies like Maertens et al.'s suggest that the durability of digital literacy interventions vary greatly and should be timed accordingly (2021). To gain a quantitative understanding of the durability of the digital literacy interventions, we recommend repeating measurements one to three times after the initial pretest. This may also capture whether the efficacy of an intervention degrades over time.

## IN PRACTICE

To address the lack of quantifiable data on mis- and disinformation susceptibility in the military, we set out to test our proposed methodology in practice. We selected the cadet population of the United States Military Academy (USMA). This selection has the practical advantage of leveraging the existing institutional mechanisms for conducting studies that exist in academia. We recruited a group of 228 cadets for the study from January to April 2023. As part of this study, we evaluated the efficacy and durability of a popular digital literacy intervention, the Bad News game.

In our study, we used the Misinformation Susceptibility Test (MIST-20) as the method of evaluation, which consists of twenty text-based news items that the participants classify as either true or false. We selected the Bad News game as the intervention to test. We measured the misinformation susceptibility of the cadet population immediately before and after they completed the Bad News game to identify the effect of the intervention. Finally, we administered MIST-20 again, three months later. Although our initial findings from the study were insightful in their own right, we also learned how to analyze and select tailored interventions based on a population's needs.

We chose MIST-20 rather than create our own test for several reasons. First, its use in other studies allowed us to compare the misinformation susceptibility of USMA cadets to that of the US population. This gave us a relative understanding of USMA cadets in comparison to Americans of a similar age and educational experience. Second, the creators of MIST-20 conducted a series of psychometric validations on the test, in which they extensively tested and confirmed that MIST-20 evaluates what it claims to measure. Many other measurements of misinformation susceptibility lack psychometric validation and thus are questionable in this regard (Maertens et al., 2021). Finally, we chose MIST-20 because it provides a holistic view of misinformation susceptibility.

In addition to measuring overall news veracity discernment, it measures real news detection ability, fake news detection ability, distrust, and naivete. This is important because it captures facets of misinformation susceptibility that simpler tests would otherwise miss.

## LESSONS LEARNED

We also acknowledge several limitations in our approach. First, because the news items used in MIST-20 consisted of text-based news headlines, we must exercise caution when generalizing our findings. Because misinformation susceptibility truly encompasses many different media types and may be influenced by various contextual factors, "misinformation susceptibility" as defined by our study is truly just the ability to distinguish real news *headlines* from fake news *headlines*.

The most notable limitation of our study was due to its design—a one-group pretest posttest. In this type of study, the dependent variable (the misinformation susceptibility of the population) is measured both before and after the implementation of the intervention (the Bad News game). This design lacked a control group and, as a result, was prone to threats of internal validity, including *history* (when events occur between the two measurements that might affect their outcomes), *maturatation* (when participants grow or learn between the two measurements), *testing* (when the act of measuring affects the participants' responses), and *instrumentation* (when the characteristics of measuring change and participants develop different attitudes toward the measurement) (Price et al., 2017).

Since our study consisted of two posttests, with the second one taking place three months after the pretest, it is possible that participants relied on memory rather than active decision-making, were affected by a semester's worth of classes, or developed less serious attitudes toward the test and therefore gave less effort. Again, because we did not include a control group, our results might not provide a realistic portrayal of misinformation susceptibility or the effectiveness of the Bad News game as an intervention. This, however, was the result of a deliberate trade-off: had we included a control group, we would have had half the sample size and would have been unable to make any statistically significant findings.

Our study provided valuable insight for areas of improvement during future iterations. For example, we collected minimal demographic information. In hindsight, collecting more detailed demographics and participant attributes would have been useful for exploring potential correlative relationships between these various covariates and the facets of MIST performance. Such potential covariates include institutional trust (which we suspect



might explain why cadets score higher on MIST than the general US population) or actively open-minded thinking, which is the “willingness to consider alternative opinions, sensitivity to evidence contradictory to current beliefs, the willingness to postpone closure, and reflective thought” (Stanovich and Toplak, 2023). This additional data would have improved our ability to more effectively tailor future iterations of assessments and ultimately our ability to identify effective and tailored digital literacy interventions for the cadet population.

Another focus for improvement of our study includes selecting the optimal time between the first posttest and the second posttest, which, in our case, was three months. We found that most of the facets of misinformation susceptibility returned to their pretest levels after this span of time—but we are uncertain when this decline in durability occurred. Had we selected a shorter time interval, we would have gained a more accurate understanding of the durability of our selected intervention.

## CONCLUSION AND FUTURE WORK

The competition in the information environment poses a complex challenge for every organization, but especially those charged with ensuring national security. Given the complexity of the challenge and the diverse set of organizational considerations, it is impossible to prescribe a single digital literacy. Further, as we discussed, even describing a deliberate data-driven approach to the problem can fail to adequately address the complexity for a single, relatively small population like the cadets of the USMA. This could lead some to conclude that it is not worth the commitment of resources and effort to engage in the methodology we propose to ultimately produce more questions than answers. We believe this is not a viable option for the defense workforce, who are likely to remain a consistent target of constantly evolving adversarial information operations.

We believe that a sustained, iterative testing approach driven by data is the best way to keep pace with and succeed in light of the information operations faced by the defense workforce. This demand highlights the need for a practical, quantitative methodology for the selection and implementation of tailored digital literacy interventions. The first several iterations of this effort are

likely to generate more questions than answers; however, continuing to engage in this process is no less critical. In this regard, this type of effort presents a natural opportunity for collaboration between academia and the defense workforce. We believe that, over time, building on a foundation of quantifiable data and in partnership with academia, defense organizations will be able to improve the resilience of their personnel. Engaging in this process is vitally important to face the intensified international strategic competition for power and influence taking place in the information environment.

## REFERENCES

- “Games are a weapon in the war on disinformation.” (2023). *The Economist*, April 8.
- Keenan, L. (2022, March 30). *True or false? The fight against disinformation*. Modern War Institute. Retrieved from <https://mwi.westpoint.edu/true-or-false-the-fight-against-disinformation>.
- Maertens, R., Götz, F. M., Golino, H., Roozenbeek, J., Schneider, C. R., Kyrychenko, Y., Kerr, J. R., Stieger, S., McClanahan, W. P. I., Drabot, K., He, J. K., & van der Linden, S. (2021, July 6). *The Misinformation Susceptibility Test (MIST): A psychometrically validated measure of news veracity discernment*. PsyArXiv. <https://doi.org/10.31234/osf.io/gk68h>.
- Mazarr, M. J. (2021). *Understanding influence in the strategic competition with China*. RAND Corporation, Santa Monica, CA.
- Office of the Director of National Intelligence. (2023). *Global Trends 2040: A More Contested World*.
- Price, P. C., Jhangiani, R. S., Chiang, I. A., Leighton, D. C., & Cuttler, C. (2017). Quasi-experimental research. In *Research Methods in Psychology*. Pressbooks. <https://opentext.wsu.edu/carriecuttler>.
- Roozenbeek, J., Maertens, R., Herzog, S. M., Geers, M., Kurvers, R., Sultan, M., & van der Linden, S. (2022). Susceptibility to misinformation is consistent across question framings and response modes and better explained by myside bias and partisanship than analytical thinking. *Judgment and Decision Making*, 17(3), 547–573.
- Roozenbeek, J., Schneider, C. R., Dryhurst, S., Kerr, J., Freeman Alexandra, L. J., Recchia, G., van der Bles, A. M., & van der Linden, S. (2020). Susceptibility to misinformation about COVID-19 around the world. *Royal Society Open Society*, 7(10).
- Stanovich, K. E., and Toplak, M. E. (2023). Actively open-minded thinking and its measurement. *Journal of Intelligence*, 11(2).

# An Ocean Apart: Island Disaster Response Logistics

Paul L. Knudsen

2023 PMRI Defense & Security Research Symposium

Mary Johnson, PhD

Department of Aviation and Transportation Technology  
Purdue University

**Abstract** Natural disasters inflict three times the death and injury in island nations compared to their continental counterparts. The dramatically worse outcomes of island nations invite an analysis of contributing differences between islands and continental nations and their corresponding disaster response efforts. This paper analyzes the casualty disparity between islands and continental nations using both qualitative and quantitative approaches. Qualitatively, the paper reviews scholarly articles on disaster response logistics, island disaster case studies, and unique facets of the maritime domain. Quantitatively, the paper analyzes 4,598 disasters occurring between 2010 and 2022 and compares outcomes against key logistics indicators to determine areas of correlation using the *Pearson product moment correlation*. Analyzing these factors reveals that islands are inherently disadvantaged in disasters because of logjamming of limited logistics mechanisms and greater time-distance gaps to prepositioned stock locations. These disadvantages are particularly pronounced in midsized islands with low per capita gross domestic product (GDP). The results also indicate a heavy reliance by islands on aerial resupply and that, though islands possess a comparative advantage in merchant marine fleets, there is no significant correlation between an island’s fleet size or number of ports and the number of dead and injured. These findings indicate that alternative employment of merchant marine assets and sea-based prepositioned stock may create a more resilient system that improves the outcomes of island nations during disasters. A subsequent study involving modeling of sea-based resupply solutions may reveal new disaster response logistics techniques, particularly for midsized, low per capita GDP islands.

## INTRODUCTION

From 2010 to 2022, island nations worldwide suffered 934 natural disasters, causing more than 276,000 deaths and affecting 188 million people—three times the amount suffered by continental nations in the same period (International Disaster Database, 2022). Island populations are particularly disadvantaged in a disaster as their isolation limits the options for delivery of critical supplies and increases the time-distance gap to access prepositioned stocks (Kim & Bui, 2019). Though the scale and frequency of natural disasters continues to increase across the globe, disaster response logistics has remained relatively static (Roh et al., 2015). The problem inherent in the status quo is that disaster response logistics is not adapting to the unique requirements of islands, causing the outcomes of those islands to continually worsen.

Though there is extensive research on disaster response logistics and even case studies involving islands, an alternative logistics approach for islands compared to continental nations is relatively unexplored. Three

research questions are central to this difference in approach: What are the unique logistics strengths and weaknesses of islands compared to continental nations in a disaster scenario? Which logistics variables correlate with better outcomes in a disaster? Based on island strengths and correlated variables, which areas of disaster response logistics merit modeling for improved outcomes? By framing a research approach that answers these questions, this paper contributes a new perspective to disaster response logistics that may improve disaster outcomes for islands.

This paper analyzes disaster response logistics factors that influence negative island nation outcomes to identify opportunities for improvement. The paper defines disaster response logistics as the planning, implementing, and controlling of efficient, cost-effective flow and storage of goods, materials, and money, as well as related information from the point of origin to the point of consumption for the purpose of alleviating the suffering of vulnerable people (Kim & Bui, 2019). The paper first presents a concise background of disaster response

logistics, island disaster case studies, and unique facets of the maritime domain. Second, variables influencing the problem are described: paved airstrips, ports, merchant marine ships, per capita gross domestic product (GDP), and island size. With this foundation established, the investigation applies *Pearson product moment correlation* to identify possible relationships between these variables and the number of dead and injured during a disaster. The paper concludes by presenting opportunities for further investigation and modeling that might improve disaster outcomes for island nations.

## LITERATURE REVIEW

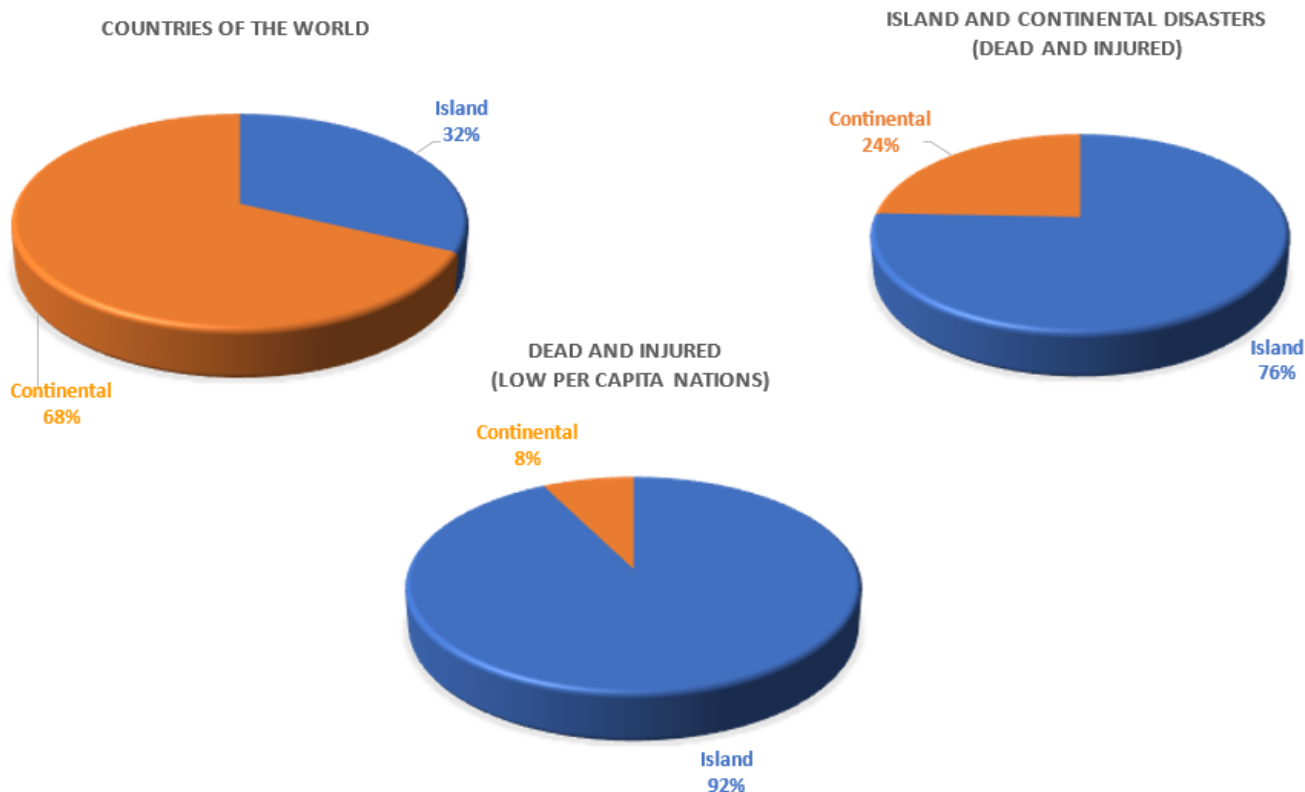
### Problem

Understanding the unique position island nations hold in relation to disaster response is best achieved by zooming in gradually from the big picture to a narrower focus. In the big picture, some basic facts place island nations in the context of their continental counterparts. Island nations make up 32% of the world's countries yet

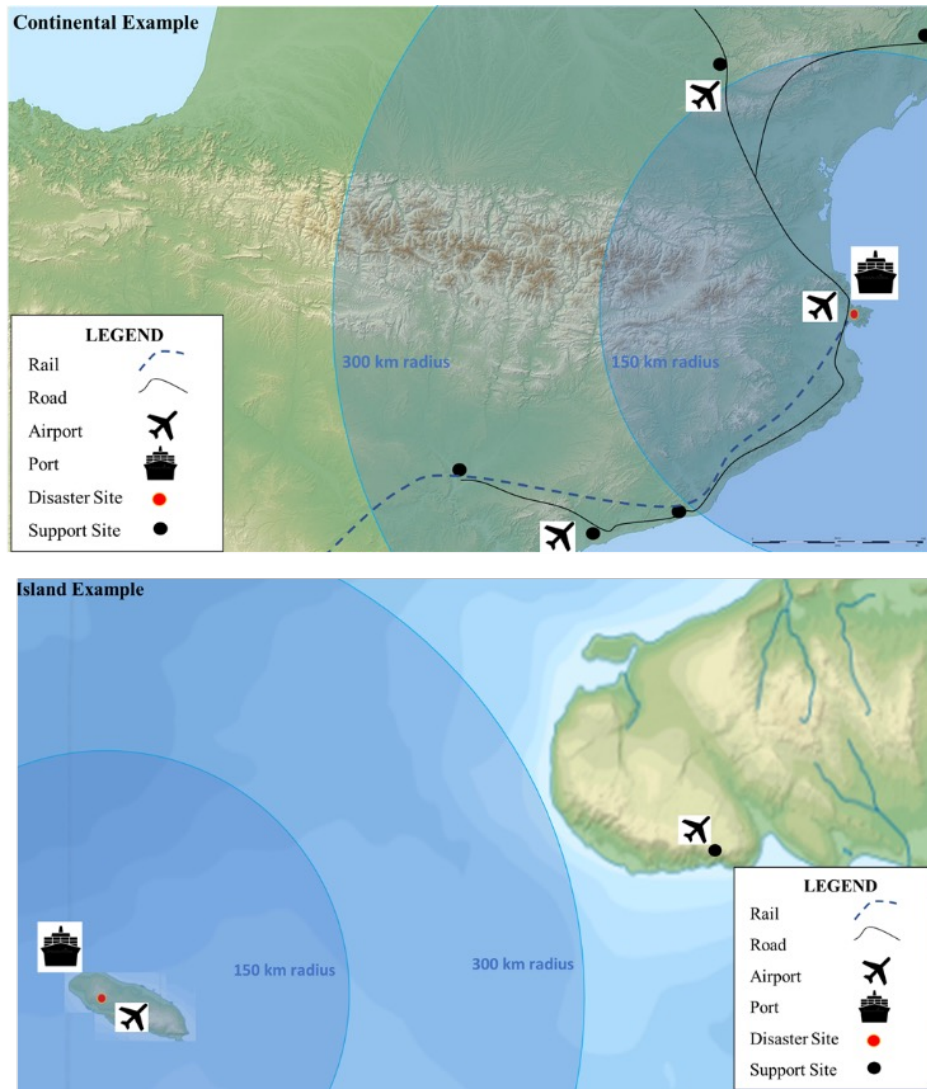
between 2010 and 2022 accounted for 76% of deaths and injuries caused by natural disasters. This statistic is even more shocking when comparing low per capita GDP countries (<\$16,500), where island nations suffered 92% of the total dead and injured (International Disaster Database, 2022; World Bank, 2021a). Figure 1 visualizes the disproportionate casualties suffered by island nations.

Though the lopsided distribution of disaster casualties is sobering, most scholars favor individual case studies over holistic data analysis. In the aggregate, the narrow focus of these case studies reveals several themes of island nations struggling in a disaster: lack of redundant resupply methods, large time-distance gaps to resupply nodes, poor infrastructure resilience, and overwhelmed interior lines. Figure 2 visualizes these themes of disadvantage using notional continental and island examples.

One case study investigated Hurricane Maria and the respective disaster response efforts of Puerto Rico and Hawaii. Accounts from both locations highlighted



**Figure 1.** Island and continental comparisons. Top left: Percentage of island countries and continental countries in the world. Top right: Percentage of island and continental dead and injured globally from natural disasters between 2010 and 2022. Center: Percentage of island and continental dead and injured globally from natural disasters between 2010 and 2022 among low per capita GDP nations. Figure created with World Bank National Accounts Data and the International Disaster Database (World Bank, 2021a; International Disaster Database, 2022).



**Figure 2.** Notional island and continental disaster response logistics comparison. These examples theorize an area of relative safety and useful time-distance gap between 150 km and 300 km from the site of the disaster-affected area. The continental example shows the greater number of support sites and methods of external resupply (rail/highway) available. Created with base topographic imagery from Wikimedia Commons, <https://commons.wikimedia.org/>.

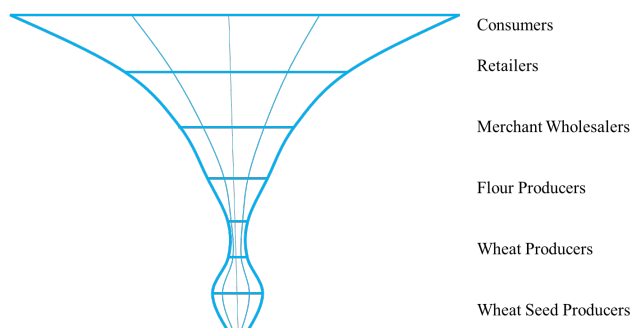
the limited external support and transportation alternatives, which slowed delivery of essential supplies and evacuation of the injured. Due to the reliance of both islands on imports, particularly agricultural goods, the criticality of port operations to disaster response featured prominently; Puerto Rico’s port was inoperable for four days, while Hawaii’s port operations never ceased (Kim & Bui, 2019). In both locations, the ports became backlogged with goods as internal delivery mechanisms (primarily trucks) converged on the ports and overwhelmed the capacity of available interior lines (roads).

A second case study comparing post-earthquake Haiti in 2010 with post-Hurricane Katrina New Orleans in 2005 documented a similar overwhelming of interior lines. Dubbed the “islanding effect,” disaster response efforts in both Haiti and New Orleans saw the arrival of external support limit the mobility of internally displaced persons (Sheller, 2012). In the context of continental versus island comparisons, this study showed that overwhelming interior lines occurs in both continental and island disasters, but the lack of alternative modes of resupply made the effect worse in Haiti.

## CURRENT APPROACHES AND GAPS

### Disaster Response Logistics

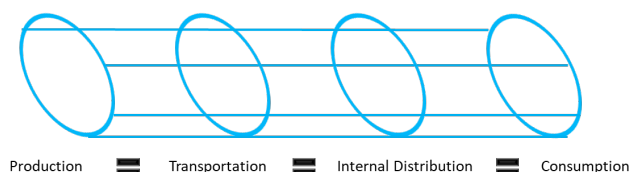
Disaster response logistics emerged as a specialized field within the wider context of supply chain management. Ronald Ballou illustrates fundamental principles of supply chain management and its evolution from simple logistics in a 2007 journal article (Ballou, 2007). In its infancy, the field of logistics focused on procurement, maintenance, and transportation of goods, but it gradually broadened to comprise total cost as well as the inward and outward flow and storage of goods, services, and related information between the point of origin and point of consumption (Ballou, 2007). Of particular importance to all logistics fields is the concept of the supply chain. A supply chain diagram identifies the producer, consumer, and key intermediary factors for the transportation of goods and then visualizes the relationship in the form of a scaled pipeline. Figure 3 demonstrates a simple supply chain concept for the transport of flour.



**Figure 3.** Supply chain choke points in a multiechelon chain for wheat production and distribution. Adapted from Ballou (2007).

The supply chain concept in Figure 3 introduces a useful tool with which to make broad visual comparisons of the strengths and weaknesses of island and continental supply chains. For the purposes of this literature review, the supply chain comparison is simplified to four echelons: production, transportation, internal distribution, and consumption. If production perfectly matched transportation, internal distribution, and consumption, the supply chain would resemble a very efficient tube structure like that shown in Figure 4.

Looking at the four echelons in sequence, production highly favors continental locations for oil, agriculture, and manufactured products, while island nations hold a moderate advantage in freshwater per capita (CIA World Factbook, 2021; Global Change Data Lab, 2018). Transportation heavily favors continental locations largely because of the presence of international rail and highway modes of transport that are wholly unavailable to islands. In the two categories where islands can compare with continental locations, maritime and air, the results are split. Island nations hold a small advantage in average number of merchant marine vessels, while continental locations outperform islands with nearly six times the average number of paved airports.



**Figure 4.** Basic idealized supply chain with four basic echelons: production, transportation, internal distribution, and consumption.

**Table 1.** Island and continental supply chain comparison

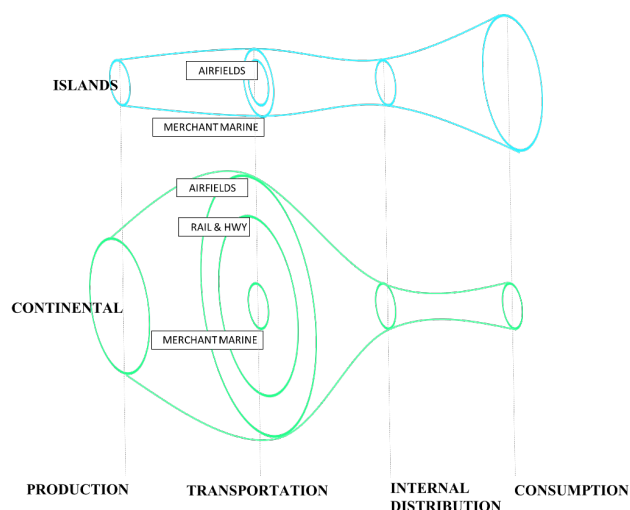
Echelon	Indicator	Island	Continental
Production	Oil production (barrels per day, 2021)	12%	88%
	Agricultural production (maize, wheat, rice, barley, rye, millet, and others, tonnes, 2021)	4%	96%
	Manufacturing production output (USD, 2021)	17.5%	82.5%
	Renewable freshwater per capita (cubic meters, 2018)	65.7%	34.3%
Transportation	Average number merchant marine vessels	574	451
	Average number paved airports	16	92
	International rail	—	Unmeasured
	International highway	—	Unmeasured
Internal Distribution	Average LPI	2.89	2.86
	Average infrastructure score from LPI	2.78	2.71
	Average service (competence and quality, LPI)	2.85	2.71
Consumption	Dead and injured	75.6%	24.4%

Note. Table data compiled from the CIA World Factbook (Central Intelligence Agency, 2022a,b,c); the Global Change Data Lab (2018; 2020); Macro Trends (2021); the International Disaster Database (2022); and World Bank National Accounts Data. (2021b).

(CIA World Factbook, 2021). In terms of internal distribution, judged here by the World Bank's logistics performance index (LPI), island and continental locations score roughly equal on average (World Bank, 2021a,b). Last, in terms of consumption, in this case the number of casualties requiring support in documented disasters, islands hold a significant negative advantage over continental locations. Table 1 provides a concise accounting of these findings.

Visualizing the relative strengths and weaknesses from this data is achievable by transferring the scale of disparity onto a supply chain diagram. Figure 5 shows both the island and continental supply chains for disaster response. The island supply chain is striking in several ways that may contribute to the worse outcomes of island disasters. The difference between production and consumption is the inverse of the continental supply chain, meaning that islands are forced to procure external production to meet consumption (dead and injured). To do this, they face an immediate bottleneck compared to continental nations both in the number of options for delivery and the scale of those options. In only the merchant marine transport category are islands superior to continental nations. The story told by this visual is that there is a significant disadvantage for island nations while supply chains are intact and, in a disaster, when supply chains break down.

Disaster response logistics emerged as its own sub-field due to the assumption of broken supply chains in a disaster, the need to forge new chains, and the delicate



**Figure 5.** Island and continental supply chain comparison using four echelons: production, transportation, internal distribution, and consumption. Note that the transportation echelon shows the relative scale and redundancy of transport modes available to island and continental nations.

balance between prioritizing cost and expedience. Paramount to any disaster response is the selection of support sites or supply hubs, the placement of which is complicated by the opposing characteristics of relative safety and short time-distance gap to the disaster site. One of the better explorations of methodology for support site selection was written in 2015 by Roh, Petit, Harris, and Beresford. The authors highlight the unique features of disaster response logistics, namely the field's reactive nature, inherent supply chain disruptions, premium transport charges, and high assumed losses. They then propose five criteria for site selection, summarized in Table 2: location, national stability, cost, cooperation, and logistics (Roh et al., 2015).

A 2010 article by Javier Salmeron and Aruna Apte introduced a simple two-phase construct to disaster response logistics: predisaster and postdisaster. Stage 1, predisaster, involves expansion of existing resources in the affected area, and stage 2, typically defined as three days postdisaster, involves surging additional assets to the affected area (Salmeron & Apte, 2010). To achieve optimal supply chains in each phase, their modeling finds the following variables to be the most important considerations: travel time between affected area and relief locations, airport ramp space, health care providers, warehouses, methods of transportation and capacity, and prepositioning costs. These findings are consistent with those of other investigations of disaster response logistics and demonstrate a bias for air resupply.

**Table 2.** Criteria and definitions for prepositioned warehouse selection

Criterion	Definition
Location	Location affected by geographical location, proximity to beneficiaries, disaster-free location, donor's opinion, climate, nearness to other warehouse, and proximity to disaster prone areas
National stability	Location affected by geographical location, proximity to beneficiaries, disaster free location, donor's opinion, climate, closeness to other warehouse, and proximity to disaster prone areas
Cost	Cost affected by storage, logistics, replenishment, labor, and land
Cooperation	Cooperation affected by support from host government, UN, neighbor countries, logistics agents, and international/local NGOs
Logistics	Logistics affected by availability and capabilities of airport, seaport, road, and warehouse

### Resilient Systems

Resilient systems are a growing and important consideration in many fields, and the concept is particularly central to the problem of island disaster outcomes. The concept of resilience management is easily understood in comparison to the more prevalent and corollary considerations of risk management. The approach of risk management is to fortify a system against failure by identifying risks, assessing their likelihood and impact, and then mitigating them (Park et al., 2011). Though admirable, this concept inherently focuses on making systems “fail-safe” rather than “safe-to-fail.” A 2011 article by Jerry Park, Thomas Seager, and Suresh Rao attempts to define problem sets where resilience management is essential through the study of three disasters: Fukushima nuclear reactors (2011), Deepwater Horizon oil spill (2010), and Hurricane Katrina (2005). The findings of this study indicate that situations requiring resilience management are marked by a large number of unknown, inestimable, or low-probability, high-consequence events (Park et al., 2011). Given the reactive nature and assumed supply chain failures at the core of disaster response logistics, resilience management has advantages over risk management.

Understanding resilience management characteristics reveals some of the weaknesses inherent in current island disaster response. Resilience-managed systems possess diversity, distribution, coherence, efficiency, and adaptability, which are summarized in Table 3 (Fiksel, 2003). In the island-continental comparison in Figure 5, each of these characteristics is violated in the instance of island disaster response. The status quo response efforts for islands have few forms and behaviors, incur

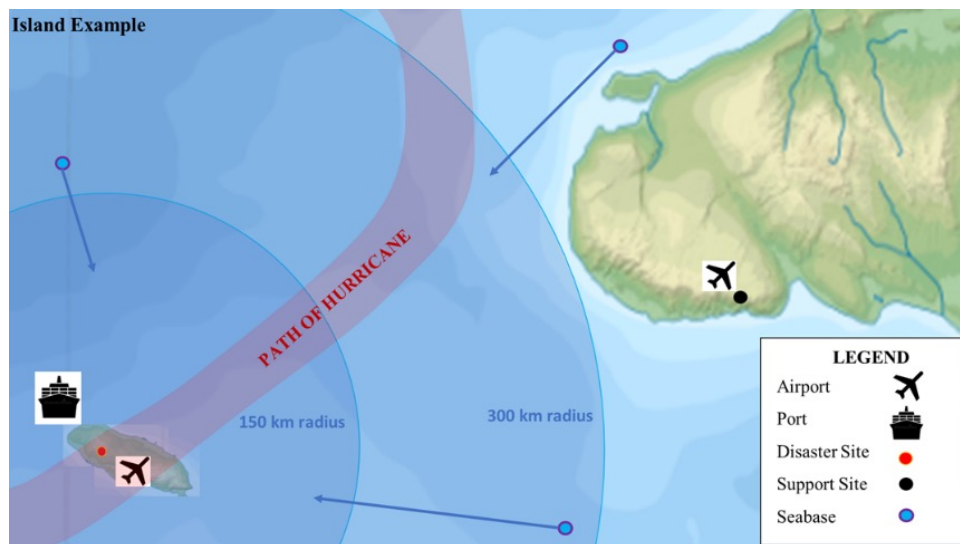
**Table 3.** Core characteristics of resilient systems

Characteristic	Application
Diversity	Existence of multiple forms and behaviors
Efficiency	Performance with modest resource consumption
Adaptability	Flexibility to change in response to new pressures
Cohesion	Existence of unifying forces or linkages

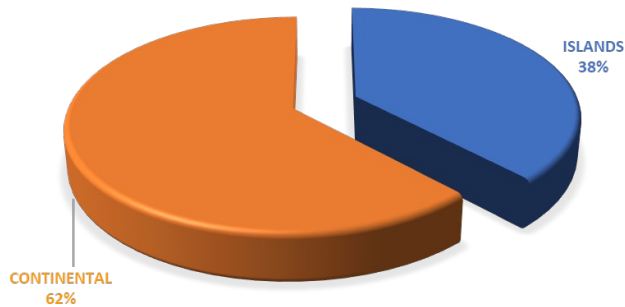
inordinate resource consumption, cannot easily adapt to changes, and, particularly in the case of low per capita GDP islands, are reliant on a unified collection of NGOs for support. Though continental disaster response often fails at one or more of these characteristics, the holistic resilience failure of current island systems may illuminate why the disaster outcomes for islands are so poor.

### Sea-Basing

Sea-basing is a military maritime resupply concept that if applied to disaster response could turn some of the disadvantages of island nations into sources of competitive advantage. US military writings on the subject define sea-basing as the deployment, assembly, command projection, reconstitution, and reemployment of joint power from the sea without reliance on land bases within the operational area (Tangredi, 2011). Simply put in the disaster response framework, sea-basing transposes the resource storage and maintenance capabilities of a land-based support center onto a collection of mobile, maritime platforms, as shown in Figure 6. Given that the



**Figure 6.** This notional example shows mobile sea-bases achieving closer proximity to the disaster-affected area and maneuvering around the path of an incoming hurricane. Created with base topographic imagery from Wikimedia Commons, <https://commons.wikimedia.org/>.



**Figure 7.** Island and continental merchant marine

average hurricane width is 300 miles and merchant marine vessels travel around 25 miles per hour, a sea-based flotilla could arrive at a disaster site within 6 hours (Lee et al., 2016).

Though primarily a military concept, the implications of sea-basing for humanitarian relief and disaster response (HA/DR) is already a leading consideration. Naval War College research concluded that sea-basing constitutes the best sustained logistical platform for HA/DR in littoral regions (Tagredi, 2011). The promise of sea-basing to island disaster response was further supported in military modeling or “wargaming” exercises in 2016. Best practices from the exercise included dividing the area of operations into sectors, combining multiple smaller forces into a larger capacity sea-base, leasing commercial cargo vessels, and utilizing an afloat regional humanitarian coordination center (Lee et al., 2016).

Notably, sea-basing best practices align superbly with the criterion for ideal prepositioned warehousing and the characteristics of resilience management discussed earlier in the literature review. A sea-base achieves all five criteria for warehousing—location, national stability, cost, cooperation, and logistics. Additionally, sea-basing reflects three of the four characteristics of ideal resilience management: diversity, adaptability, and cohesion. The promise of sea-basing would appear to pair well with the comparative advantage island nations possess in the average size of their merchant marine fleets compared to continental nations. Island nations possess an average of 574 ships, compared with only 451 for continental nations, and they control 38% of the world’s merchant marine force, as shown in Figure 7 (CIA World Factbook, 2022a). Unfortunately, previous scholarly writing has not investigated the employment of merchant marine fleets in disaster response.

### INTERVENTION AND CONTRIBUTION

The literature review revealed the depth of the problem, current approaches related to the problem, and gaps in

**Table 4.** Research questions

Research question	Approach
What are the unique logistics strengths and weaknesses of islands compared to continental nations in a disaster scenario?	Literature review
Which logistics variables correlate with better outcomes in a disaster?	Pearson product moment correlation
Which areas of disaster response logistics merit modeling for improved outcomes?	Pearson product moment correlation literature review

existing research. This paper contributes to the field by investigating holistic trends of island and continental disaster response rather than focusing on narrow case studies. This investigation also takes into account the weaknesses of island nations in terms of logistical isolation and their strengths in terms of maritime capability. Cross-applying these strengths and weaknesses with the principles of prepositioning, resilience management, and sea-basing, the analysis studies correlation, or the lack thereof, between the size of a nation’s merchant marine fleet, number of ports, number of paved airstrips, land mass, and per capita GDP. By combining the results of the literature review and the correlation analysis of select variables, the paper seeks to answer the three research questions shown in Table 4.

### METHODS

#### Study Design

This research study comprises six steps culminating in a series of correlation tests across island and continental disasters stratified across three classes of per capita GDP. The first step was compiling a list of every natural disaster from 2010 to 2022. Second, the study expanded this list into a multisource database with the key variables of merchant marine fleet, ports, paved airstrips, land mass (km), and per capita GDP (current USD). The third step comprised purging the database of insignificant and poorly documented entries. To meet the criteria for “significant” and “well-documented,” a discrete disaster event had to have data for number of dead, number of injured, and total cost. This step eliminated any disaster event for which no record existed for one of those three fields. The fourth step divided the refined database of discrete events into separate “island” and “continental” databases. The fifth step stratified these databases into



**Table 5.** Study design methodology

Step	Description
1	Compile list of natural disaster events between 2010 and 2022
2	Create database of disaster events with added variables (merchant marine, ports, paved airstrips, land mass (km), and per capita GDP (current USD))
3	Purge database of insignificant and poorly documented entries
4	Subdivide database into island and continental event databases
5	Stratify databases into three classes of per capita GDP
6	Correlation analysis

per capita GDP classes. The final step was a correlation analysis across key variables and the number of dead and injured for each discrete event. Table 5 summarizes this study design methodology.

### Population

The population for this study began as a list of 4,636 entries for natural disasters occurring in the period from 2010 to 2022. After purging the list of insignificant and poorly documented entries, 514 discrete events were left. Of these remaining events, 173 occurred in island nations and 341 occurred in continental nations. After stratification by per capita GDP, the island database contained 114 “low” entries, 16 “medium” entries, and 43 “high” entries. The continental database contained 48 low entries, 206 medium entries, and 87 high entries.

Of note, the presence of repeat disasters in the same location and steep differences in per capita GDP between nations made the creation of similarly populous classes of the same GDP range impossible. The resulting populations of each class make comparisons of the high and low GDP classes statistically viable, while the small population of medium GDP island nations precludes its use. Table 6 illustrates the gradual refinement of the disaster event population.

### Data Collection Instruments

This study relied on three primary sources for data collection: the EM-DAT international disaster database, the Central Intelligence Agency (CIA) World Factbook, and the World Bank National Accounts Data. EM-DAT is maintained by the Université Catholique de Louvain (UCLouvain), a Belgian university with its registered office at Place de l’Université, 1, B-1348 Louvain-la-Neuve, Belgium, and acting through its Center for Research on the Epidemiology of Disasters. This study used EM-DAT to compile the list of disaster events with associated location, damage cost, and number of dead and injured. The CIA World Factbook is maintained by the CIA, a US intelligence agency based in Langley, Virginia. This study used the CIA World Factbook to compile the number of merchant marine ships, the number of paved airstrips, the number of ports, and the country size. The World Bank National Accounts Data is maintained by the World Bank, a subsidiary of the United Nations and headquartered in Washington, DC. This study used the World Bank to compile per capita GDP data for each country. Table 7 shows the data collected from each source.

**Table 6.** Study population

Description	Population (discrete events)	
Natural disasters (2010–2022)	4,636	
Refined disaster list (significant and well-documented)	514	
Categorization	Island: 173	Continental: 341
Stratification by per capita GDP	Island	Continental
	Low 114	48
	Medium 16	206
	High 43	87

**Table 7.** Data collection sources

Source	Data collected
EM-DAT International Disaster Database	Disaster events, location, damage cost, dead, injured
CIA World Factbook	Merchant marine, paved airstrips, ports, country size
World Bank National Accounts Data	Per capita GDP

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}}$$

$$t = r\sqrt{\frac{n-2}{1-r^2}}$$

**Figure 8.** Pearson product moment correlation and test statistic formulas

### Data Analysis Procedures

#### Pearson Product Moment Correlation

This study employs the Pearson product moment correlation,  $r$ , and the test statistic for correlation,  $t$ , to reach its conclusions (Figure 8). In both calculations, the number of dead and injured remained a constant variable against which paved airports, merchant marine, ports, and size were compared. The study paired a scatterplot chart as a data visualization with each  $r$  and  $t$  result. In the highest instances of correlation, the study transitions to hypothesis testing, creating a bell curve visualization for the theoretical population correlation coefficient,  $\rho$ , and calculating the confidence interval,  $\alpha$ , which would merit rejection of the null hypothesis.

#### Per Capita GDP Classes

Per capita GDP classes were calculated by averaging class distributions for the range of values in the total revised disaster database, the island database, and the continental database. In each of these class distributions, high and low outliers were selected for “overflow” classes. Choosing to maintain standardized class sizes across each of the databases required a sacrifice in the population size of the medium per capita island group, but the high and low GDP classes contained sufficient discrete events for statistical analysis.

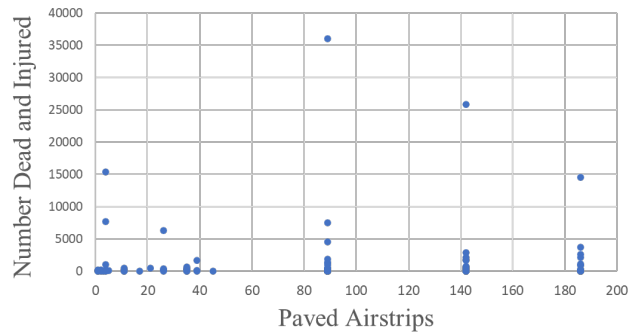
### RESULTS

The correlation testing found a significant negative correlation between the number of paved airstrips and casualties for both island and continental events. Unexpectedly, the study also found a significant negative correlation between continental ports and casualties but no such correlation in islands. Last, and also unexpectedly, the study found no correlation between island merchant marine size and number of casualties. Of the three per capita GDP divisions, the low group showed the strongest correlations in the same areas.

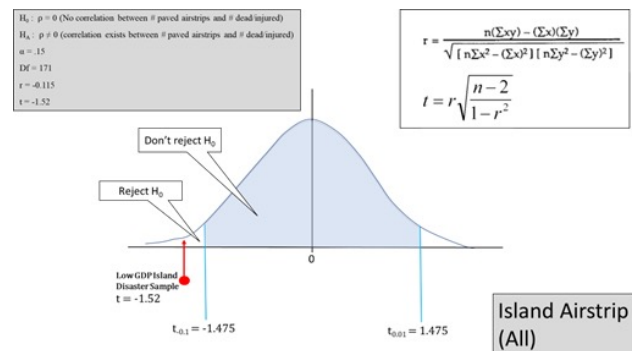
The relationship between paved airstrips and dead/injured on islands irrespective of per capita GDP showed visual correlation trends as in Figure 9. Calculations confirmed the significance of this correlation with an  $r$  value of  $-0.115$  and a  $t$  value of  $-1.518$ . These values justified rejecting the null hypothesis in favor of correlation using an  $\alpha$  of  $0.15$ , as in Figure 10.

The relationship between paved airstrips and dead/injured for low per capita GDP islands showed visual correlation trends as in Figure 11. Calculations confirmed the significance of this correlation with an  $r$  value of  $-0.137$  and a  $t$  value of  $-1.46$ . These values justified rejecting the null hypothesis in favor of correlation using an  $\alpha$  of  $0.2$ , as in Figure 12.

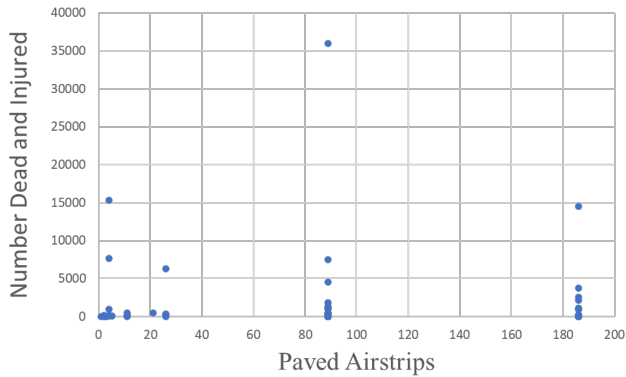
The relationship between ports and dead/injured in continental nations irrespective of per capita GDP showed visual correlation trends as in Figure 13. Calculations confirmed the significance of this correlation with an  $r$  value of  $-0.103$  and a  $t$  value of  $-1.900$ . These values justified rejecting the null hypothesis in favor of correlation using an  $\alpha$  of  $0.15$ , as in Figure 14.



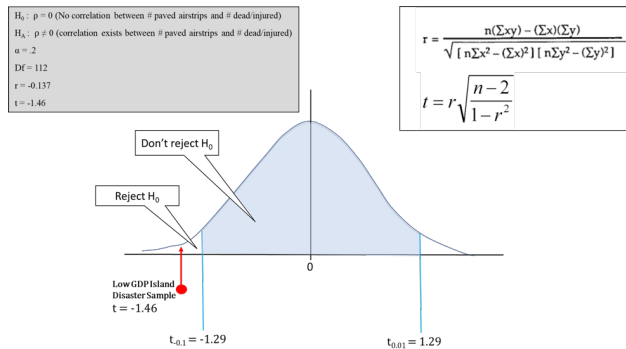
**Figure 9.** Relationship chart for island paved airstrips and dead/injured.  $n = 172$ , accounting for the removal of one outlier—the 2010 Haiti earthquake with a dead and injured total of 522,570.



**Figure 10.** Hypothesis testing diagram for island paved airstrips and dead/injured.  $n = 173$ ,  $r = -0.115$ ,  $t = -1.52$ , and  $\alpha = 0.15$ .



**Figure 11.** Relationship chart for low per capita GDP island paved airstrips and dead/injured. n = 113, accounting for the removal of one outlier—the 2010 Haiti earthquake with a dead and injured total of 522,570.

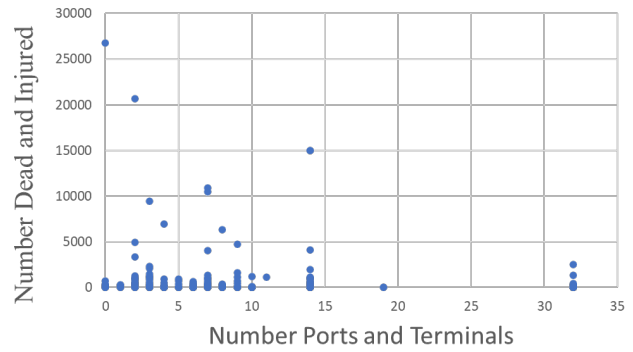


**Figure 12.** Hypothesis testing diagram for low per capita GDP island paved airstrips and dead/injured. n = 114, r = -0.137, t = -1.46, and alpha = 0.2.

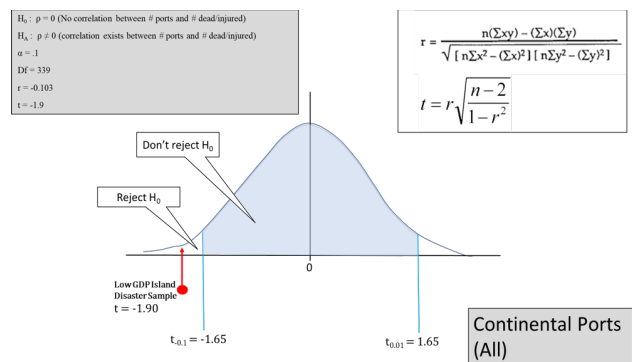
## DISCUSSION

### Theoretical Interpretation

The results of the correlation study, interpreted through the lens of the literature review, conform to a compelling explanation. Island nations have vastly more dead and injured than continental nations because disasters worsen already disadvantaged supply chains. The failure to coordinate merchant marine assets into a viable and centralized disaster response force combines with damage to ports to nullify any competitive advantage islands might have. Unlike continental locations, which have more and greater alternate methods of resupply, island ports take longer to restore once damaged. This predicament leaves islands overreliant on air resupply despite having a great disadvantage in number of paved airstrips. When supplies do arrive at the few locations capable of receiving them, interior lines to those locations become overwhelmed.



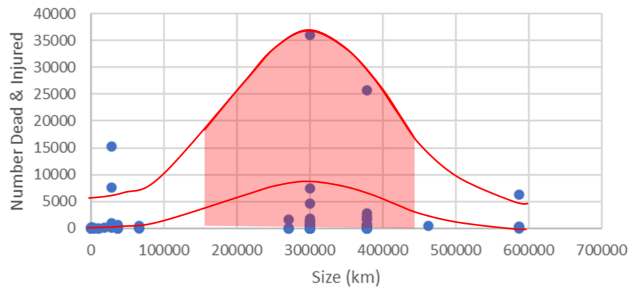
**Figure 13.** Relationship chart for continental ports and dead/injured. n = 341.



**Figure 14.** Hypothesis testing diagram for continental ports and dead/injured. n = 341, r = -0.103, t = -1.900, and alpha = 0.1.

Though testing this theory requires follow-on modeling, some additional data manipulation provides preliminary support. If more people are dying because only a few resupply locations are operational and these exceed the capacity of interior lines, one would expect small and large islands to be less affected than medium-sized ones. In small islands, even if only a single airport or harbor can receive resupply, the distance to any point within the island is minimal. In large islands, there are not only more airports and ports, but there may be safe areas to preposition supplies on the island itself. The most disadvantaged islands would be somewhere in the middle: too large to easily move supplies from limited resupply nodes but not large enough to have relative safe areas for prepositioning. Figure 15 shows the relationship of dead and injured compared with the size of each island.

The relationship graph in Figure 15 supports the conclusion that midsized islands of between 160,000 and 440,000 km<sup>2</sup> may be more likely to experience higher casualties due to overwhelmed interior lines. Combined with the correlation of overreliance on air resupply in low per capita GDP islands, a template emerges of the



**Figure 15.** Relationship of island size and number of dead/injured.  $n = 169$ ; four outliers removed for both size and number of dead and injured.

locations for which improved logistics options might be most effective.

### Implications for Practitioners

If the explanation for these findings is correct, islands should explore more resilient options for sea-based resupply. In applying the principles of resilience management, islands need resupply options that don't rely exclusively on ports and airstrips. More specifically, islands should pool merchant marine resources among regional neighbors and explore undersea prepositioned stock. In at least one instance, this activity is already happening. In the Caribbean Community, several island nations agreed to form the Caribbean Disaster and Emergency Management Agency (CDEMA) (Thompson, 2015). CDEMA is a regional disaster response organization that would be an ideal place to test any of the sea-base concepts that emerge from modeling.

## CONCLUSION

### Response to Research Questions

The qualitative and quantitative arms of this study produced answers to all three research questions. As summarized in Table 8, islands possess only one area of strength in disaster logistics—their merchant marine fleets. Conversely, they are weak in most other areas, most prominently in redundant transportation, lower airlift capability, lack of production, and overwhelmed interior lines. Despite the strength of their merchant marines, islands see no benefit from their ports or fleets and appear to rely on paved airports almost exclusively during a disaster. These strengths, weaknesses, and correlations make sea-basing and undersea prepositioned stock attractive modeling areas.

### Limitations and Future Research

The study purged many discrete disaster events due to a large number of incomplete entries. Though removing

**Table 8.** Research questions

Research question	Answer
What are the unique logistics strengths and weaknesses of islands compared to continental nations in a disaster scenario?	<i>Strength:</i> merchant marine <i>Weaknesses:</i> lack of redundant transportation, lower airlift capability, lack of production, overwhelmed interior lines
Which logistics variables correlate with better outcomes in a disaster?	Number of ports Number of paved airports
Which areas of disaster response logistics merit modeling for improved outcomes?	Sea-basing Undersea prepositioned stock

these entries improved the quality and consistency of the data, it also lowered the population size dramatically, which in turn decreased accuracy. Though the trade-off was for the better, future studies with more data would improve results. The study also faced trade-offs in per capita GDP stratification. Because of multiple disaster entries for the same country and large disparities among GDPs, establishing same-size classes with significant representation in each was not possible. This trade-off diluted the value of statistics in the middle per capita GDP class. Finally, the light correlation between variables placed the confidence interval anywhere between 20% and 10% for two-tailed hypothesis testing. Though these are still excellent percentages with which to test a hypothesis, these do not meet the gold standard 5% of most hypothesis testing.

Future research on sea-basing should model resilience using merchant marine vessels and ship-to-shore delivery. If modeling indicates improvement in disaster survivability based on sea-basing, then investigation into the historical locations of merchant marine vessels after disasters would help confirm or deny the theorized explanations in this paper. Due to the advanced regional partnerships in the Caribbean, interviews and modeling with input from CDEMA would further strengthen future studies. Follow-on modeling should also simulate the prepositioning and recovery of stocks placed undersea. Such a technique may alleviate the overwhelming of internal lines and improve outcomes for island nations. More importantly, initial research indicates that hurricane disruption on the sea floor is significantly lower than on the surface (Vaughan, 1987). If this is accurate, prepositioned stocks could be placed closer to isolated disaster sites and improve the outcomes for those communities.

## REFERENCES

- Ballou, R. (2007). The evolution and future of logistics and supply-chain management. *European Business Review*, 19(4), 332–348. <http://doi.org/10.1108/09555340710760152>
- Central Intelligence Agency. (2021). *CIA World Factbook*. <https://www.cia.gov/the-world-factbook/about/archives/2021/>
- Central Intelligence Agency. (2022a). *Country comparisons—merchant marine* [Data set]. *CIA World Factbook*. <https://www.cia.gov/the-world-factbook/field/merchant-marine/country-comparison>
- Central Intelligence Agency. (2022b). *Country comparisons—airports with paved runways* [Data set]. *CIA World Factbook*. <https://www.cia.gov/the-world-factbook/field/airports-with-paved-runways/>
- Central Intelligence Agency. (2022c). *Country comparisons—crude oil exports* [Data set]. *CIA World Factbook*. <https://www.cia.gov/the-world-factbook/about/archives/2021/field/crude-oil-exports/country-comparison>
- Fiksel, J. (2003). Designing resilient, sustainable systems. *Environmental Science & Technology*, 37(23), 5330–5339. <https://pubs.acs.org/doi/pdf/10.1021/es0344819>
- Global Change Data Lab. (2018). *Renewable water resources per capita* [Data set]. Our World in Data. <https://ourworldindata.org/grapher/renewable-water-resources-per-capita>
- Global Change Data Lab. (2020). *Cereal production 2020* [Data set]. Our World in Data. <https://ourworldindata.org/agricultural-production>
- International Disaster Database. (2022). *Emergency management database query tool* [Data set]. <https://public.emdat.be>
- Kim, K., & Bui, L. (2019). Learning from Hurricane Maria: Island ports and supply chain resilience. *International Journal of Disaster Risk Reduction*, 39, 101244. <https://doi.org/10.1016/j.ijdrr.2019.101244>
- Lea, C., McGrady, E., Jackson, D., Powell, D., Collins, E., & Samaranyake, N. (2016). *Gaming sea-based multinational HA/DR operations at PACOM Amphibious Leaders Symposium 2016*. Center for Naval Analyses. <https://apps.dtic.mil/sti/pdfs/AD1023326.pdf>
- Macro Trends. (2021). *Manufacturing output* [Data set]. <https://www.macrotrends.net/countries/ranking/manufacturing-output>
- Park, J., Seager, T., & Suresh, P. (2011). Lessons in risk-versus resilience-based design and management. *Integrated Environmental Assessment and Management*, 7(3) 396–399. <https://setac-onlinelibrary-wiley-com.ezproxy.lib.purdue.edu/doi/pdfdirect/10.1002/ieam.228>
- Rezaei, J., van Roekel, W. S., & Tavasszy, L. (2018). Measuring the relative importance of the logistics performance index indicators using Best Worst Method. *Transport Policy*, 68, 158–169. <https://doi.org/10.1016/j.tranpol.2018.05.007>
- Roh, S., Pettit, S., Harris, I., & Beresford, A. (2015). The pre-positioning of warehouses at regional and local levels for a humanitarian relief organization. *International Journal of Production Economics*, 170, 616–628. <http://dx.doi.org/10.1016/j.ijpe.2015.01.015>
- Salmeron, J., & Apte, A. (2010). Stochastic optimization for natural disaster asset prepositioning. *Production and Operations Management*, 19(5) 561–574. <https://online.library-wiley-com.ezproxy.lib.purdue.edu/doi/pdfdirect/10.1111/j.1937-5956.2009.01119>
- Sheller, M. (2012). The islanding effect: Post-disaster mobility systems and humanitarian logistics in Haiti. *Cultural Geographies*, 20(2), 185–204. <https://doi.org/10.1177/1474474012438828>
- Tangredi, S. (2011). Sea basing: Concept, issues, and recommendations. *Naval War College Review*, 64(2). [https://www.jstor.org/stable/pdf/26397242.pdf?refreqid=excelsior%3A4ab4a70c872166d168c5a071d49607d4&ab\\_segments=&origin=&acceptTC=1](https://www.jstor.org/stable/pdf/26397242.pdf?refreqid=excelsior%3A4ab4a70c872166d168c5a071d49607d4&ab_segments=&origin=&acceptTC=1)
- Thompson, D. (2015). Disaster logistics in small island developing states: Caribbean perspective. *Disaster Prevention Management*, 24(2), 166–184. <https://www.emerald.com/insight/content/doi/10.1108/DPM-09-2014-0187/full/pdf>
- Thomson, J., Garrett, M., Taylor, M., George, T., Melancon, M., & Behrens, K. (2005). *Sonar surveys for pipeline inspection show extent of pipeline displacement and seafloor instability following Hurricane Ivan* [Paper presentation]. Offshore Technology Conference, OnePetro. <https://doi.org/10.4043/17738-MS>
- Vaughan, N. D., Johnson, T. C., Mearns, D. L., Hine, A. C., Kirby-Smith, W. W., Ustach, J. F., & Riggs, S. R. (1987). The impact of Hurricane Diana on the North Carolina continental shelf. *Marine Geology*, 76, 169–176. <https://doi.org/10.4043/7859-MS>
- Wijesekera, H. W., Wang, D. W., Teague, W. J., & Jarosz, E. (2010). High sea-floor stress induced by extreme hurricane waves. *Geophysical Research Letters*, 37(11). <https://doi.org/10.1029/2010GL043124>
- World Bank National Accounts Data. (2021a). *GDP per capita—current USD* [Data set]. [https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?name\\_desc=false](https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?name_desc=false)
- World Bank National Accounts Data. (2021b). *Logistics performance index* [Data set]. [https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fpi.worldbank.org%2Fsites%2Fdefault%2Ffiles%2FInternational\\_LPI\\_from\\_2007\\_to\\_2018.xlsx&wdOrigin=BROWSELINK](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fpi.worldbank.org%2Fsites%2Fdefault%2Ffiles%2FInternational_LPI_from_2007_to_2018.xlsx&wdOrigin=BROWSELINK)

# Adaptive Detection and Policy Transformation for Insider Threats

Nicholas B. Harrell, Alexander Master, and J. Eric Dietz  
Center for Education and Research in Information Assurance and Security  
Purdue Homeland Security Institute  
Purdue University  
nharrel@purdue.edu, amaster@purdue.edu, jedietz@purdue.edu

**Abstract** Insider threats are among the most costly and prevalent cybersecurity incidents. Modern organizations lack an effective way to detect and deter insider threat events; traditional mitigation approaches that focus on recruitment processes and workplace behavior have proven insufficient. Current analytic detection tools do not map technical indicators to organizational policies. This limitation results in poor risk calculations, rendering inaccurate risk mitigation decisions regarding insider threats. This paper proposes a pragmatic, data-driven approach that uses policy-mapped technical indicators to assess insider threat risk. Our approach provides a quantitative insider threat risk score to facilitate informed decision-making by policymakers. Using computer simulation modeling and synthetic data to iterate common threat scenarios, we increase the probability of detecting an insider threat event. This novel approach provides quantitative analysis with distinct advantages over qualitative risk matrices commonly used in industry to forecast and assess organizational risk.

## INTRODUCTION

According to Verizon's most recent data breach investigation report, internal employees caused 19 percent of data breaches (Bassett et al., 2023). The report also noted that external actors likely took advantage of internal errors—more than 40 percent of breaches involved stolen credentials from a legitimate user. Verizon ranked ransomware and phishing among the top four actions contributing to breaches (Bassett et al., 2023). Note that most of these attacks required some action by an internal employee. The rise of remote work, accelerated by the global COVID-19 pandemic (Manokha, 2020), has further complicated detection of insider threats; data from the IT industry in the same year indicated a concerning trend of increased insider disruptions. Insider threats are defined as individuals, either current or former employees, who possess particular access to an organization's internal resources. Their actions, whether unintentional or intentional, cause harm or increase the risk of harm within the organization (Collins, 2016). Harm can be monetary loss from service downtime, loss of intellectual property, liability for disclosure of personally identifiable information, or reputational damage.

To study information environments in organizations, various researchers have emphasized the significance of the recruitment process, workplace behavior, and interpersonal interactions among colleagues to determine how psychometric traits can predict insider behavior. Most organizations employ internal mechanisms to flag behavioral indicators via background checks, which include past employment records, credit reports, credential verification, criminal convictions, and insights from

previous coworkers and supervisors who may reveal more intrinsic details about the candidate (Collins, 2016). Based on current industry statistics, we can see that despite these approaches, insider threats are still prevalent and on the rise (Bassett et al., 2023).

This paper proposes a pragmatic approach based on the premise that insider threats are inevitable due to human error. Rather than attempting to discern indicators from human behavior, we focus on the relationship between an organization's policy and its monitoring and auditing capabilities. Our primary contribution is to offer a tool and an approach that utilizes quantitatively measured technical indicators to provide policymakers with an insider threat risk score. Rather than relying solely on subject matter expert opinion, our model provides policymakers with a composite score that supports informed decision-making. We adopt a process known as dynamic adaptive management or dynamic adaptive policy pathways (DAPP), which has been employed in various industries (Haasnoot et al., 2013). We demonstrate how looking at insider threats as an event of uncertainty can assist decision-makers in making better risk management decisions regarding insider threat activity. We call this approach adaptive detection and policy transformation for insider threats (ADAPT-IT).

## PRIOR WORK

### *Analytic and Monitoring Capabilities*

Legg et al. (2015) demonstrated the mapping of technical indicators to user behavior in insider threat detection using log data, such as login attempts, removable media,

email, web, and file logs. This approach allowed for monitoring activities and incidents indicative of insider behavior, supporting the identification of insider threat activity through profiling.

Analytical strategies in insider threat detection have encompassed anomaly-based and heuristic-based approaches (Yamin et al., 2020; Collins, 2016; Eldardiry et al., 2013; Caputo et al., 2009). However, the mapping of features to policy violations remains underdeveloped.

Intrusion detection systems are commonly used to detect network threats. They can be either signature-based, relying on known attacks, or anomaly-based, relying on deviations from normal behavior. Anomaly-based systems require more time for setup and rely on establishing a baseline of normal behavior, making them susceptible to mimicry attacks.

Detection of insider threats depends on capturing logs documenting specific activities and associated features (Legg et al., 2015). Each feature contributes to the user's profile, providing insights into their behavior. Organizations can more effectively detect insider threats by classifying activities into risk categories based on user roles. They utilize various methods, including user activity monitoring, data loss prevention, security information and event management, analytics, and digital forensics (Spooner et al., 2018). Organizations can detect deviations from normal behavior and identify potential insider threats by leveraging technical indicators such as file transfers, database queries, and login activities. Monitoring specific actions (e.g., file transfers and logins) can effectively narrow the focus and increase the likelihood of insider threat detection.

### ***Effective Decision-Making***

Insider threats involve uncertainty, posing challenges for decision-makers who struggle with intangibles (Hubbard and Seiersen, 2023). Researchers have explored models addressing security policy compliance and noncompliance. The cause of uncertainty lies in the behaviors of employees regarding adherence to security policies (Warkentin and Willison, 2009).

Traditionally, policymakers in many industries assumed they could predict the future; they created a static "optimal" plan based on a single "most likely" future (Haasnoot et al., 2013). This strategy solved the short-term problems; however, when different results happen in the assumed future, a new "optimal" plan must be created. Collingridge (1980) suggested that when there is limited knowledge regarding the potential side effects of emerging technologies, it is crucial to prioritize decision correctness, thorough monitoring of effects, and adaptability. In the context of uncertainty, Rosenhead (1990) and Rosenhead et al. (1972) proposed that

evaluating the robustness of strategies can be done by considering the degree of flexibility, specifically by measuring the number of available options.

Adaptive policymaking, proposed by Haasnoot et al. (2013), presented a structured approach for designing dynamic and robust plans. It emphasized the importance of decision correctness, extensive monitoring, and flexibility in the face of limited knowledge about the potential side effects of emerging technologies. The approach consisted of five steps: (1) analyze existing system conditions and set objectives, (2) formulate a basic plan, (3) enhance plan resilience through mitigating, hedging, seizing, and shaping actions, (4) continuously monitor plan performance, and (5) implement triggered actions based on signpost information. Adaptive policymaking enabled data-driven decision-making and reduced uncertainty by establishing a bidirectional relationship between policy and monitored technical indicators.

The adaptation pathways approach, summarized by Haasnoot et al. (2011, 2012), offered a different perspective on planning for adaptation. This concept considered adaptation tipping points; these signify the conditions under which an action no longer aligns with specified objectives. After reaching a tipping point, the approach presented a sequence of possible actions through adaptation trees, similar to decision trees or road maps. It utilized computational scenario approaches to assess the timing of tipping points across different scenarios. The adaptation pathways map provided an overview of alternative routes to achieve desired future outcomes, considering different actions and their potential performance. By incorporating stakeholder perspectives, cultural mapping, and cost-benefit analyses, decision-makers could make informed choices about the pathways to follow. The adaptation pathways approach provided a framework to adapt to changing conditions and support decision-making in uncertain and dynamic environments.

Integrating adaptive policymaking and adaptation pathways into DAPP aligns with Hubbard's strategy of measuring data points based on observable events. As Hubbard emphasized, quantitative measurement reduces uncertainty by focusing on observable technical indicators rather than subjective human behavior. The integrated approach of DAPP incorporated a monitoring system that tracks signpost information, which represents observable events and triggers related to the plan's success (Haasnoot et al., 2013). This data-driven approach enabled decision-making based on real-time information and facilitated continuous adjustment of actions and strategies to ensure alignment with preferred pathways (Haasnoot et al., 2011, 2012).

### ***Objectives and Indicators***

Haasnoot et al. (2013) posited that understanding indicators within asset pathways is crucial. The authors explored adversarial modeling, identifying potential actions that deviate from standard pathways and pose threats to organizations. Looking at their approach from a cyber perspective, we can see pathways of data extraction within an organization's cyber infrastructure. For instance, an email could lead to the dissemination of sensitive information to unauthorized entities.

Haasnoot et al. (2013) also offered that it is vital to monitor system actions to collect signpost information related to triggers. Monitoring enhances quantitative assessment of risk posture, facilitating the mapping of actions to policies and their categorization based on selected methods. Our contribution suggests incorporating a prioritization mechanism using weights. Haasnoot et al. (2013) described an adaptive system that measures the actions' effectiveness after each iteration. The system allowed policymakers to adjust weights based on indicators' effectiveness in detecting threat-like behavior, enabling quick adaptation of risk mitigation techniques. Similar challenges exist in ecology and other fields, where adaptive strategies require streamlined decision-making to address knowledge gaps (Scarlett, 2013).

### ***Weights and Composite Indicators***

Composite indicators are used in many fields of study regarding human development sustainability, perceived corruption competitiveness, or other complex phenomena (Becker et al., 2017). Studies that perform uncertainty and sensitivity analysis on composite indicator assumptions rely on subjective choices (Saisana et al., 2005). It is important to realize the bias in these assumptions and choices made, which will deviate from the importance factor placed on the overall aggregated score. Optimization is generally effective in defining the impact and importance of weights on a composite indicator (Becker et al., 2017). Due to corollary relationships between features, weights can often have negative scores (Becker et al., 2017). Further investigation using correlation analysis is required to ensure that the weights do not contribute to the same variation in the outcome, effectively canceling each other out.

### ***Policy and Training***

Kweon et al. (2021) conducted a study on the impact of security training on organizations. Many factors were considered, including managerial knowledge, employee knowledge, security policies, time spent on training, firm size, and budget for training. An interesting finding in this study was that security policy programs were an indicator of having many security incidents. Kweon et al.

concluded that organizations with many security policies most likely have the policies in place due to numerous security incidents. The author found that the more the population is aware of security concerns, the fewer incidents occur. However, many security policies in an organization are due to previous security incidents. The author inferred that the security policy is usually a consequence of a prior incident (Kweon et al., 2021).

### ***AnyLogic Modeling***

AnyLogic is simulation software that provides mechanisms to simulate real-life scenarios. It allows policymakers to make informed decisions without having to allocate immense resources. This study will use the optimizer in AnyLogic to calibrate the weights we use to determine the appropriate importance for each weight. Several research groups have used simulations to inform risk management decisions (Master et al., 2022; Tzvetanov et al., 2022; Lerums et al., 2018).

## **THE ADAPT-IT MODEL**

### ***Methodology***

This paper offers an iterative approach to reduce policy infringements by increasing detection rates of malicious actors. Through exploratory data analysis, our model calculates a composite score for each user and ranks them based on deviations from their exponential moving averages (EMA) over short and long periods. We evaluate model success by measuring all malicious actors that rank within the top 40 of composite scores.

### ***Validity***

We used an open-source dataset from the United States Computer Emergency Readiness Team (US-CERT) to test and validate the model's effectiveness in identifying insider threat behavior.<sup>1</sup> Using publicly available data promotes transparency and ease of reproducibility of our work. We used the version 5.2 release from the US-CERT data repository in this study to offer an assortment of scenarios encapsulating various facets of network interaction. These included email reception events, the structure of directories on removable media, properties of email attachments such as size, user login attempts, and web content.

The data derived from these scenarios were systematically cataloged across four distinct csv files: file, http, email, and device. Each of these files comprised more than 800,000 entries and encompassed many features that facilitate the mapping and understanding of user behavior within the network context. Our work underscores the value of linking technical indicators with policy frameworks to evaluate insider threat risk.



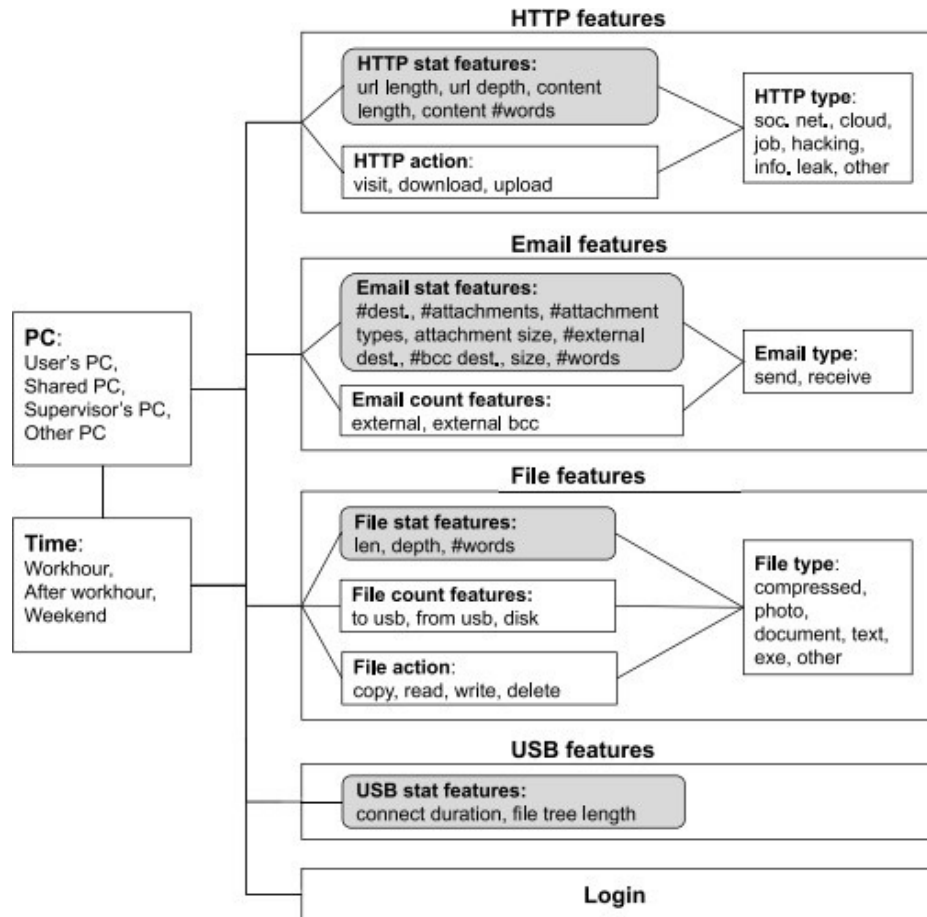


Figure 1. Example of feature extraction (Le et al., 2020)

Le et al. (2020) demonstrated the different elements within a cyber infrastructure that can be used to model a user's day-to-day work behavior, as seen in Figure 1. By relating the features on the right of Figure 1 with temporal and spatial elements, we extracted sequential features that indicated a higher probability of a malicious actor event. Our work did not focus on content filtering to simplify the results. However, we did use file names and URLs to flag suspicious behavior.

Our features reflect realistic scenarios that may enable us to use the model in production environments in future work. The dataset we used in this study is synthetic data, which alleviates privacy and ethical concerns in the conduct of our research (Glasser and Lindauer, 2013; US Department of Homeland Security, 2012).

#### **Limitations and Delineations**

Given the synthetic nature of the dataset we used in this study, our findings support the simulation model's feasibility and internal consistency. Due to hardware resource limitations, we evaluate only the users in scenarios 3 and

4. Interested readers may refer to the US-CERT dataset for these scenario definitions. We defined our general policies using scenarios 3 and 4.

The implemented model provides preliminary support for the detection of other events. To enhance the robustness of our findings and minimize sources of variation, we deliberately narrowed the focus of our experiment to two specific scenarios and a fixed group of forty identified malicious actors. Due to limited research showing the effectiveness of corrective measures on an employee population, we used a 5% reduction factor to simulate an organization implementing a corrective measure on its population (e.g., cyber awareness training).

We do not directly compare our model outputs to detection model effectiveness rates in the literature. Our experiment aims to simulate how an organization could leverage user event monitoring tools to formulate a composite score and reduce policy infringements. The model's success is demonstrated by its ability to increase the probability of flagging a malicious actor using an iterative approach.

**Table 1.** Policy to feature mapping

Policy	Feature/event	Trigger
No files, large emails, or attachments sent to external organizations without internal organization awareness	Monitor sent email	Employee sends a large email with no internal employee on the email to an organization outside of domain
No files, large emails, or attachments sent to self or personal email without internal organization awareness	Monitor sent email	Employee sends a large email with no internal employee on the email to own email or a personal email
Internet will be used for work-related activity; no browsing unauthorized content	Monitor web traffic URL	User browses unauthorized or non-work-related content
Users are prohibited from accessing files that are not related to their projects	Monitor file tree access	User access file not within normal file tree
Users are prohibited from copying proprietary information on to personal removable media or copying foreign files that can be executable on to organization devices	Monitor connect/disconnect and reading/writing of files to personal devices	User copies file outside of file tree or writes unauthorized file to file tree
Users are only authorized to perform work-related activities on the device assigned to them	Monitor logon attempts and PC names	User logs onto more than one device in set period
User event sequences will be monitored for suspicious activity	Monitor unusual sequences of activity	User performs activities outside of normal behavior

By concentrating on controlled parameters based on features derived from policy, we mitigated potential confounding factors, minimized the standard deviation, and attenuated the influence of outliers within the model’s detection capability.

**Preprocessing**

We imported each csv file and processed them using Python parsing techniques. We applied filtering techniques based on the appropriate policy. All files were aggregated into a main csv file with a heading of (date, user, pc, event, score, neg\_event). The score was binary, signifying whether the event was a policy infringement. The neg\_event was also binary and signified whether the event was part of a scenario that represented an incident inside the organization. We used the event and timestamp columns together to extract sequential features that rely on temporal data. Because the model does not directly align with the dataset’s intent, many more scores than neg\_events exist.

**Model Dynamics**

We collected a priority queue for each user, timestamp, and associated score. We applied a modified exponential moving average (MEMA) that calculated a score based on a set period and a second score based on a third of the previous set period. We applied a smoothing factor (SF) to the formula that gave more weight and influence on the nearer-term period. Using the changes in the user’s

EMA and distance from the standard deviation, we calculated each user’s z-score, which became larger when there was more disruption in the user’s composite score. Consider the following representation:

let SPS = short period score; LPS = long period score;  
 $SF = \frac{2}{(1 + (SPS))}$

$$MEMA = (SPS - LPS)(SF) + SPS$$

We created a distribution based on the user population z-scores. Users who demonstrated the largest z-scores (a larger deviation from their normal behavior compared to the population) within a certain period were moved to the top of an array. This distribution was consistently updated. A representation of the z-score is as follows:

Let z represent the z-score; x represents the MEMA;  $\mu$  = mean average of MEMA for a user;  $\sigma$  is the standard deviation of the population or sample.

$$z = \frac{x - \mu}{\sigma}$$

We measured where the forty malicious events occurred throughout the time window in which the incidents occurred and derived the average rank based on z-scores to determine how well the model successfully classifies the users associated with bad events. We sorted the z-scores from highest to lowest and ranked them in order. To

**Table 2.** Weights used in model

	<b>Weights</b>
personalP	User email's attachment or large email to self or personal email
emailP	User email's attachment or large email to external organization with no
webP	User browses unauthorized websites
logonP	Logon attempts outside of normal work hours
deviceP	Unauthorized copying of files or transferring files to a work device
fileP	Unauthorized file tree access
multiP	Accessing multiple computers within a set period of time
afP	Multiplier that is used to weigh events that happen after hours
evP	Tracks suspicious sequences of events (e.g., multiple unauthorized websites followed by unauthorized device)

minimize the error, we set checks throughout the model to ensure that the events were classified appropriately and aligned with the timestamps within the answer dataset. We also ensured that only malicious actors with

ground truth negative events were assessed during the evaluation period.

We used AnyLogic's optimization feature to calibrate the weights associated with each event within the dataset based on the collected features. Two types of features were considered: sequential features and frequency features. We scored frequency features according to their corresponding weight. We based weights in our study on email transactions, file tree access, web behavior, removable media behavior, and logons.

The sequential features relied on users being logged in to multiple PCs during a set period, or were judged based on access patterns. We purposely left the features generic to reflect simple, monitorable organizational policies.

Let weights be represented as  $\mathbf{W}$ , where  $W \in \{\mathbb{R}\}$  and  $\{w_1, \dots, w_n\} \setminus \{0\}$ .

We collected results by assessing how many malicious actors ( $n = 40$ ) out of the total population ( $N = \sim 2000$ ) were correctly classified by the model. We assessed all individuals that were ranked based on the absolute value of their z-scores, from highest to lowest. The short period was set to 15 days and the long period to

$$\text{user's z-score} \leftarrow F(\text{username}, \text{timestamp}, \text{weights}, \text{event}, \text{score}, \text{pc}, w_1, \dots, w_n)$$

```

1: Initialize User Priority Queue to PQ
2: Initialize ZScore HashMap to HM
3: for each entry in event log do
4:   if username exists in PQ then
5:     Load all username entries for set time-period in PQ
       into a temporary set
6:   end if
7:   if score = 1 then
8:     score *= (appropriate weight + 1)
9:   end if
10:  if user has been on another PC then
11:    score *= (multP + 1)
12:  end if
13:  if user was active after hours then
14:    score *= (afP + 1)
15:  end if
16:  if user falls in a suspicious sequence then
17:    score += (evP + 1)
18:  end if
19:  Calculate MEMA = (SPS - LPS) * SF + SPS
20:  if MEMA  $\neq$  0 then
21:    Update score with the  $MEMA_{i-1} - MEMA_i$ 
22:  else
23:    Update score with 0
24:  end if
25:  Update PQ with timestamp, username, event, score, pc
26:  Calculate z-score using the formula:  $z\text{-score} = \frac{\text{score} - \mu}{\sigma}$ 
27:  if HM has username and z score < current z score
       then
28:    Update HM with current username and z score
29:    Sort z score from highest to lowest
30:  end if
31:  return 100 Users with highest z scores
32: end for

```

**Figure 2.** Algorithm for composite scoring process

45 days. The MEMA used these two time frames throughout the experiment to calculate the user's scores. We chose these time periods because they allowed enough time for the model to correctly classify malicious actors over the variation of detection time windows throughout the experiment.

To demonstrate corrective measures, we performed the same experiment with a reduction factor applied. The reduction factor removes benign actor policy infringements to assess if the change improves the model's ability to detect insider threats. The reduction factor was set to .05, which is an estimation of an effective reduction factor when considering similarly sized organizations with adequate training versus those with a high amount of security incidents (Kweon et al., 2019). The experiment's purpose was exploratory analysis to determine if there was adequate support for using composite scores to classify potential insider threats. Our study also explored whether corrective measures could help improve detection rates with the ADAPT-IT framework, which implied an adaptive and iterative noise reduction approach.

## RESULTS AND ANALYSIS

The initial experiment without a reduction factor successfully classified 38 out of the 40 malicious actors, resulting in an error rate of 5 percent. The model flagged many of the bad actors with a rank of three or lower during their detection window. Three malicious actors were classified early, but their ranks remained below 40 during their detection window. As the events were classified, the ranks of the malicious actors shifted. At the end of the experiment, the 38 correctly classified malicious actors had a mean rank of 36.05, with a maximum rank

of 106 and a minimum rank of 1. The range of rankings spanned 105 positions.

In the second experiment, the model rankings significantly changed with the reduction factor applied. The composite scores for the bad actors in the first experiment ( $M = 43.30, SD = 12.65$ ) remained identical; however, the ranks changed noticeably. Two bad actors were not classified correctly in the second experiment, resulting in an error rate of 5 percent. Only two bad actors were classified earlier than their detection window. The range of ranks slightly improved to 100. To assess the significance of the results, we compared the composite scores of each correctly classified malicious actor divided by their respective rank at the end of the experiment using a two-tailed pairwise  $t$ -test. The second experiment with the reduction factor demonstrated a significantly higher ranking of malicious actors compared to the first experiment without the reduction factor,  $t(38) = 3.28, p < .02, r = .22$ .

## DISCUSSION AND FUTURE WORK

This paper demonstrates support for an alternative approach to mitigating cybersecurity risk built around adaptive policymaking informed by network monitoring. Following the iterative cycle illustrated in Figure 3, organizations will have an adaptive, quantifiable score to facilitate better-informed decision-making. As demonstrated by applying appropriate corrective measures and adjusting policy, malicious actors will become more detectable as the organization reduces overall policy infringements within its cyber infrastructure. This approach will assist organizations in improving the security of their information systems by giving them risk reduction measures to improve their security posture iteratively.

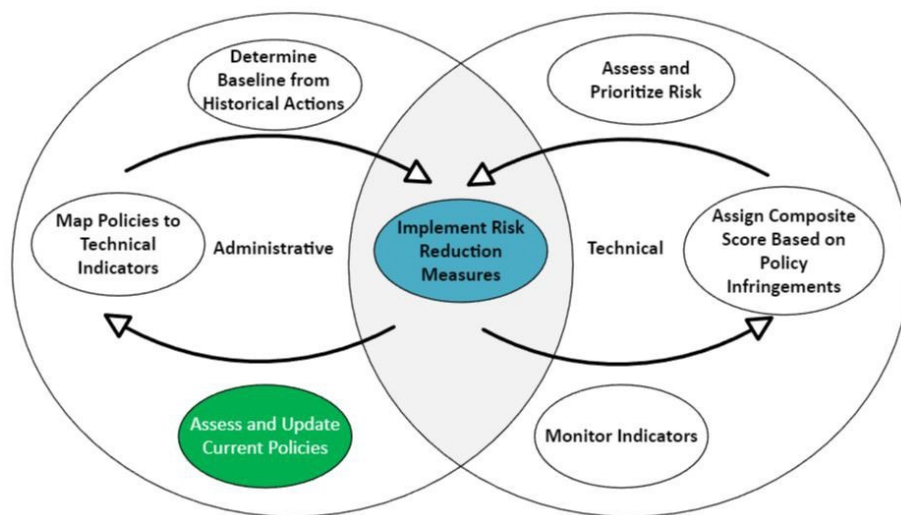


Figure 3. ADAPT-IT approach

For future work, researchers should assess more scenarios of the US-CERT dataset. These experiments would require widening the scope of the policies to capture policy infringements that relate to other malicious actor scenarios. Our model successfully identifies users that changed their behavior abruptly; however, persistent threats that lasted over two months were consistently classified at a higher rank, signifying that the malicious actor events were deviating very little from their normal behavior. This phenomenon is a known issue, described above as related to mimicry attacks. Our work illustrates how more analysis of convolution techniques that use windowing to create a more precise flagging signal is needed.

## NOTES

1. The US-CERT dataset is available at [https://kilthub.cmu.edu/articles/dataset/Insider\\_Threat\\_Test\\_Dataset/12841247/1](https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247/1)

## REFERENCES

- Balozian, P., & Leidner, D. (2017). Review of IS security policy compliance: Toward the building blocks of an IS security theory. *ACM SIGMIS Database*, 48(3), 11–43. doi:10.1145/3130515.3130518.
- Bassett, G., Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2023). *Verizon 2022 data breach investigations report*.
- Becker, W., Saisana, M., Paruolo, P., & Vandecasteele, I. (2017). Weights and importance in composite indicators: Closing the gap. *Ecological Indicators*, 80, 12–22. doi:10.1016/j.ecolind.2017.03.056.
- Caputo, D., Maloof, M., & Stephens, G. (2009). Detecting insider theft of trade secrets. *IEEE Security & Privacy Magazine*, 7(6), 14–21. doi:10.1109/MSP.2009.110.
- Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, 31(4), 49–87. doi:10.1080/07421222.2014.1001257.
- Collingridge, D. (1980), *The social control of technology*. St. Martin's Press, New York.
- Collins, M., Theis, M., Trzeciak, R., Strozer, J., Clark, J., Costa, D., & Moore, A. (2016). *Common sense guide to mitigating insider threats* (Technical report CMU/SEI-2015-TR-010). CERT Insider Threat Center.
- Couretas, J. M. (2018). *An introduction to cyber modeling and simulation*. John Wiley & Sons, Hoboken, NJ.
- Eldardiry, H., Bart, E., Liu, J., Hanley, J., Price, B., & Brdiczka, O. (2013). Multi-domain information fusion for insider threat detection. In *Proceedings of the Security and Privacy Workshops* (pp. 45–51). IEEE, San Francisco, CA. doi:10.1109/SPW.2013.14
- Glasser, J., & Lindauer, B. (2013). Bridging the gap: A pragmatic approach to generating insider threat data. In *Proceedings of the Security and Privacy Workshops* (pp. 98–104). IEEE, San Francisco, CA. doi:10.1109/SPW.2013.37
- Haasnoot, M., Middelkoop, H., Van Beek, E., & Van Deursen, W. P. A. (2011). A method to develop sustainable water management strategies for an uncertain future. *Sustainable Development*, 19(6), 369–381.
- Haasnoot, M., Van Deursen, W., Middelkoop, H., Beek, E. V., & Wijermans, N. (2012). *An integrated assessment metamodel for developing adaptation pathways for sustainable water management in the lower Rhine Delta* [Conference presentation]. Sixth International Congress on Environmental Modelling and Software.
- Haasnoot, M., Kwakkel, J. H., Walker, W. E., & Ter Maat, J. (2013). Dynamic adaptive policy pathways: A method for crafting robust decisions for a deeply uncertain world. *Global Environmental Change*, 23(2) 485–498. doi:10.1016/j.gloenvcha.2012.12.006.
- Hadlington, L. (2020). The ‘human factor’ in cybersecurity: Exploring the accidental insider.” In *Research anthology on artificial intelligence applications in security* (pp. 1960–1977). IGI Global. doi:10.4018/978-1-7998-7705-9.ch087.
- Hubbard, D. W., & Seiersen, R. (2023). *How to measure anything in cybersecurity risk* (2nd ed.). John Wiley & Sons, Hoboken, NJ.
- Khan, M. I., Foley, S. N., & O’Sullivan, B. (2022). Database intrusion detection systems (DIDs): Insider threat detection via behaviour-based anomaly detection systems—a brief survey of concepts and approaches. In W. Meng & S. K. Katsikas (Eds.), *Emerging information security and applications* (pp. 178–197). Springer, Cham. doi:10.1007/978-3-030-93956-4\_11
- Kim, J., Park, M., Kim, H., Cho, S., & Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Applied Sciences*, 9(19), 4018. doi:10.3390/app9194018
- Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*, 23(2), 361–373. doi:10.1007/s10796-019-09977-z
- Le, D. C., Zincir-Heywood, N., & Heywood, M. I. (2020). Analyzing data granularity levels for insider threat detection using machine learning. *IEEE Transactions on Network and Service Management*, 17(1), 30–44.
- Legg, P. A. (2015). Visualizing the insider threat: Challenges and tools for identifying malicious user activity. In *Proceedings of the IEEE Symposium on Visualization for Cyber Security (VizSec)* (pp. 1–7). Chicago. doi:10.1109/VIZSEC.2015.7312772
- Lerums, J. E., Poe, L. D., & Dietz, J. E. (2018). *Simulation modeling cyber threats, risks, and prevention costs* [Paper presentation]. IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI. doi:10.1109/EIT.2018.8500240
- Manokha, I. (2020). The implications of digital employee monitoring and people analytics for power relations in the workplace. *Surveillance and Society*, 18(4).
- Master, A., Hamilton, G., & Dietz, J. E. (2022). *Optimizing cybersecurity budgets with AttackSimulation* [Paper presentation]. IEEE International Symposium on

- Technologies for Homeland Security (HST), Boston, MA. doi:10.1109/HST56032.2022.10024984
- Mingers, J., & Rosenhead, J. (Eds.). (2001). *Rational analysis for a problematic world revisited: Problem structuring methods for complexity, uncertainty and conflict* (2nd ed.). John Wiley & Sons.
- Rosenhead, J., Elton, M., & Gupta, S. K. (1972). Robustness and optimality as criteria for strategic decisions. *Journal of the Operational Research Society*, 23(4). doi:10.1057/jors.1972.72.
- Rosenhead, J. (1990). Rational analysis: Keeping your options open. In *Rational analysis for a problematic world: Problem structuring methods for complexity, uncertainty and conflict*. John Wiley & Sons.
- Saisana, M., Saltelli, A., & Tarantola, S. (2005). Uncertainty and sensitivity analysis techniques as tools for the quality assessment of composite indicators. *Journal of the Royal Statistical Society Series A: Statistics in Society*, 168(2), 307–323. doi:10.1111/j.1467-985X.2005.00350.x
- Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6), 526–531. doi:10.1016/S0167-4048(02)01009-X
- Senator, T. E., Goldberg, H. G., Memory, A., Young, W. T., Rees, B., Pierce, R., Huang, D., et al. (2013). Detecting insider threats in a real corporate database of computer usage activity (pp. 1393–1401). In *Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. doi:10.1145/2487575.2488213.
- Shaw, E., Ruby, K., & Post, J. (1998). *The insider threat to information systems: The psychology of the dangerous insider*. Security Awareness Bulletin 2–98. Defense Security Service.
- Spooner, D., Silowash, G., Costa, D., & Albrethsen, M. (2018). Navigating the insider threat tool landscape: Low cost technical solutions to jump start an insider threat program (pp. 247–257). In *Proceedings of the IEEE Security and Privacy Workshops (SPW)*, San Francisco. doi:10.1109/SPW.2018.00040.
- Tzvetanov, K., Riegsecker, A., Frantz, B., Xiong, C., Bott, R., Cline, T., & Dietz, J. E. (2022). Agent-based modeling for theme park evacuation. *Journal of Emergency Management*, 20(2), 157–173.
- US Department of Homeland Security. (2012). *The Menlo report: Ethical principles guiding information and communication technology research*.
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18(2), 101–105. doi:10.1057/ejis.2009.12
- Yamin, M. M., Katt, B., Sattar, K., & Ahmad, M. B. (2020). Implementation of insider threat detection system using honeypot based sensors and threat analytics (pp. 801–829). In *Advances in information and communication: Proceedings of the 2019 future of information and communication conference (FICC)*, volume 2. Springer International.

# Information Communication Technology Support to Remote Work in Higher Education Institutes

**Craig Keith**

Purdue Polytechnic  
US Army Civil Schooling  
Craig.w.keith@gmail.com

**Chad Laux, PhD**

Department of Computer and Information Technology  
Purdue University

**Abstract** COVID-19 forced mass transitions to remote work in higher education institutes (HEIs), testing their ability to provide decentralized information communication technology (ICT) support. This research describes successful ICT support of remote work within HEIs during the pandemic. A systematic literature review was conducted to explore ICT support to remote work in HEIs and to inform data collection methods. Subject matter experts (SMEs) then participated in semistructured interviews. Qualitative content analysis of interview data was used to identify the most significant themes regarding ICT support to remote work during the pandemic. The analysis found the following themes as most significant: effective leadership qualities, customer emphasis, digital transformation and cloud tools, organizational factors, and digital inequity. Specific codes within each theme offer consideration of success factors for providing remote work ICT support in HEIs. These success factors suggest ways ahead for ICT leaders to improve their approach to emergency remote work support, with agility and resilience at the forefront of future remote work support efforts. Remote work practices and strategies vary by industry and organizational structure. This research focuses on HEIs, and thus generalizability may be limited.

## INTRODUCTION

The COVID-19 pandemic tested the resiliency and agility of most industries, including higher education institutes (HEIs), as they rapidly transitioned from brick and mortar to remote learning/work. How well organizations responded largely depended on the flexibility of information communication technology (ICT) systems, services, and processes (Tallon et al., 2019). In their timely 2019 review of information technology and organizational agility, Tallon et al. (2019) found that organizations increasingly rely on technology in the face of unanticipated and drastic change and that there is a trade-off between providing agile ICT services and strategically aligned, often robust, ICT solutions.

This challenge became apparent for HEI ICT leaders as they scrambled to support thousands of suddenly decentralized customers with ICT solutions and infrastructure intended for in-person use.

The literature on remote learning in HEIs focuses mostly on pedagogy with some mention of ICT challenges. Additionally, most research on ICT and remote work/learning considers sustained support, not emergency support like during the pandemic. As such, a gap

in the literature exists on how to provide ICT support to remote work/learning during emergencies.

The experience of HEI ICT professionals during the pandemic offers rich opportunities to explore this problem. This study aims to characterize successful ICT support to remote work/learning during emergencies. In so doing, this research identifies characteristics of ICT support to remote work during the pandemic while discussing success factors based on these results. The findings of this study offer real-world lessons learned for ICT professionals and potential paths forward for better resiliency and agility in HEIs.

Analysis of the data collected from ICT professionals offers insight into successful and unsuccessful practices based on themes and concepts within the data. In this case, content analysis is conducted from interview transcripts to identify trends related to ICT support to remote work/learning in HEIs.

Several limitations exist in this study. First, this study focuses on HEIs in North America and thus generalizability is limited to this context. Second, data was collected only from one side of the service and support relationship—the ICT leader instead of the customer. Further research could incorporate quantitative data analysis of

customer experience metrics to address related research questions. Third, industries outside of HEIs were not considered in this study.

## LITERATURE REVIEW

### *ICT, Remote Work, and COVID-19*

Remote work is an encompassing term describing work arrangements outside centralized locations, like office buildings. Generally, remote work has trended up with technological advancements like high-speed Internet or cloud services.

By spring 2020, the COVID-19 pandemic forced nearly four billion people across the planet into lockdowns (Sandford, 2020) with nearly half of all work going remote in the United States (Dalton & Groen, 2022). Financial pressures forced organizations to reduce their ICT budgets. Consequently, investments in cloud infrastructure increased as noncloud initiatives slowed (Columbus, 2020).

The following themes describing ICT remote work support during the pandemic are evident in the literature: (1) infrastructure and hardware, (2) cloud software and platforms, (3) ICT systems and processes, and (4) common challenges.

**Infrastructure and Hardware.** In some ways, national ICT infrastructure was “accidentally prepared” for a rapid increase in network traffic (Papagiannidis et al., 2020). High-speed Internet infrastructure greatly expanded in the decade before the pandemic. Nearly 75% of adults reported broadband connection at home in 2019; that number only increased through 2021 (Vogels et al., 2020). Additionally, 4G technology further increased the availability of high-speed Internet access. Although network latency increased during the lockdowns (Candela et al. 2020), the Internet proved reliable in nations with advanced infrastructure (Feldmann et al., 2020; OECD, 2020).

On a more granular scale, the pandemic stressed organizational abilities to provide hardware to remote workers. ICT divisions had to support the procurement, installation, and maintenance of laptops and peripherals. Nearly all companies had to acquire additional hardware and software solutions. In the early weeks of lockdowns, computer sales surged by 40%, while sales of keyboards, headsets, and cameras experienced even greater growth (Papagiannidis et al., 2020). The 2022 global supply chain crisis complicated these efforts late in the pandemic.

Some organizations employed “bring your own device” plans that saw remote workers relying on personal devices for connectivity (Papagiannidis et al., 2020; Sull et al., 2020). This approach presents challenges in information security, employee costs, and support for disparate ICT systems that may be unfamiliar to help desks

(Papagiannidis et al., 2020; Sull et al., 2020; Alashhab et al., 2021; Rachmawati et al., 2021).

**Cloud: Platforms and Software.** Cloud computing proved the “unsung hero of the pandemic” (Alashhab et al., 2021). Cloud resources allowed organizations to rapidly expand their remote software and data storage resources without procuring mass amounts of enterprise network equipment. Compared with traditional network infrastructures, cloud computing promised more rapid delivery of services and data, more agile responses to changing requirements, and increased information sharing efficiencies. Organizations understood that digital transformation to cloud services provided the most flexibility for the cost. For these reasons, cloud use increased significantly during the pandemic (Jacks, 2021; Maphosa & Maphosa, 2022)

Cloud computing environments offer flexibility and resiliency in pay-as-you-go service. According to the Synergy Research Group, spending on cloud services was up nearly 40% in the summer of 2020 (Alley, 2020) as cloud services replaced centralized infrastructure. Cloud also offers on-request surge capabilities (Alashhab et al., 2021; Papagiannidis et al., 2020).

Video-conference, messaging, portal, file share, and collaboration tools were in high demand as organizations were required to maintain workflow and emulate in-person work in a virtual environment. Companies were able to shop for the right tools for their individual needs and deploy them remotely. (Maphosa & Maphosa, 2022; Rachmawati et al., 2021).

**Systems and processes.** “[The] availability of technology by itself does not translate into good practice. It is an enabler but not necessarily the main driving force” (Papagiannidis, 2020). Organizations with high-quality ICT systems and processes fared better than others during the pandemic.

Successful ICT support often depends on ICT leaders’ integration with organizational operations and strategies. Quality ICT systems also include dynamic support structures that optimize flattened communications, establish manning cycles aligned with risk areas and priorities, and provide training tools for newly introduced capabilities. ICT leaders involved in organizational continuity planning were already considering how to expand or flex their service requirements as needed. Prior planning and reliance on decentralized cloud solutions allowed ICT leaders to deploy solutions to customers rapidly and consistently.

ICT professionals at the University of Washington highlighted their successes at streamlining incident response procedures and equipment deployment through prior preparation and operational prioritization (Grange et al., 2020). Their lessons reinforced the benefit of



implementing scalable and agile ICT systems. They reported strong integration between ICT and leadership, optimized communication, and updating policies as crucial to their transition to remote work. They successfully accelerated ICT support during the height of the pandemic by implementing quality systems that were aligned with their strategic guidance.

**Challenges.** Frequently reported challenges centered around the initial deployment of ICT hardware and tools, such as computers, monitors, and routers, and implementing new and unfamiliar software solutions. Change management and incident response processes were heavily strained as end users established office spaces at home. Inconsistencies in hardware and software implementation were also highlighted, causing confusion for end users and ICT support staff. Increased personal costs to remote workers was also highlighted as an obstacle for organizations to address (Maphosa & Maphosa, 2022; Rachmawati et al., 2021; Sull et al., 2020).

### ***Remote Learning/Work in HEIs***

Like remote work, remote learning has progressed along advancements in technology and culture (Kentnor, 2015). From correspondence education in the 1700s to advanced technology-driven education, remote methods have been practiced for some time (Harting & Erthal, 2005). The Internet changed the remote learning game by offering near-instant access and interaction with HEIs. The rate of students enrolled in online coursework increased fivefold from 2007 to 2012 and has continued to increase (Kentnor, 2015).

COVID-19 forced HEIs to discontinue in-person schooling seemingly overnight to varying degrees of success. Robust national Internet infrastructure (Favale et al., 2020; Papagiannidis et al., 2020), familiarity with online learning practices, and the availability of online education platforms encouraged successful transitions (Wahab & Ali, 2020). Many HEIs realized that traditional remote learning support differs from emergency remote learning/teaching (Hodges et al., 2020). In-person teaching material may need to be converted to remote formats like slide notes, lecture recordings, and other digital resources (Dwivedi et al., 2020). Emergency remote learning requires prior contingency planning that considers technology familiarity, required training, and expanded platform access (Dhawan, 2020; Mishra et al., 2020).

Many of the technologies discussed in general remote work ICT support were common in the literature on remote learning. Software and platforms to support online collaboration, instant messaging, video-teleconference, and VPNs were all commonly utilized (Dhawan, 2020; Favale et al., 2020; Lassoued et al., 2020). HEIs often relied on familiar, public-facing applications, reducing complications

from introducing new tools that may require more training and support (Almaiah et al., 2020). Dhawan (2020) emphasizes the importance of diversifying delivery methods to offer students various options for accessing instructional material. Options can range from providing different file formats for printable materials to more complex approaches.

Conversely, other HEIs relied heavily on locally supported platforms and technology. In one such example, an HEI in Italy hosted its own e-learning platform with collaboration tools, VPN access, and remote desktop support. ICT researchers monitored local traffic and reported success as network traffic changed but overall services remained constant (Favale et al., 2020).

The most common challenge found in the literature was digital inequity. Researchers frequently bemoaned the challenges of students in remote areas to maintain Internet connectivity (Almaiah et al., 2020; Dhawan, 2020; Lassoued et al., 2020; Mishra et al., 2020). Also explored were issues of access to adequate computing technologies, webcams, and antivirus security platforms. Recommendations to combat inequity include coordinating with Internet service providers for reduced costs, offering subsidies for low-income students, and offering offline asynchronous classes (Dhawan, 2020; Wahab and Ali, 2020).

Overall, research in remote learning ICT support has surged in the years following the pandemic and is mostly pedagogically focused, not focused on ICT service and support. Few delineate between steady-state and emergency remote learning support. There appears to be a gap in the research on providing ICT service and support to remote learning from the ICT perspective.

## **RESEARCH METHODOLOGY**

Themes identified in the literature review framed questions for semistructured interviews. Interviews were conducted with eight ICT leaders from North American universities and colleges of various sizes. Chief information officers (CIOs) and deputies who provided ICT support at HEIs during the pandemic were recruited as participants. Interviews were recorded and transcribed for data analysis.

Content analysis was conducted on the interview data as a viable method to identify success factors in qualitative datasets (Finney & Corbett, 2007; Nasir & Sahibuddin, 2011). This methodology is common in applied fields because it offers insights into application and practice through rich descriptions of events and experiences (Singh Hundal et al., 2021). It is particularly appropriate for investigating the experiences of ICT professionals within an HEI as they supported remote learning during COVID-19. Analysis of interview transcripts was conducted

in four steps: identify meaning units (open coding), recontextualize, group into themes, and compile/tally.

## RESULTS AND FINDINGS

A total of 21 naming units (codes) were identified during the coding process and were divided into five theme groups: (1) leadership qualities, (2) customer emphasis, (3) remote work ICT tools, (4) organizational factors, and (5) combating digital inequity. Each of these five themes was addressed in all eight of the interviews. The frequency of individual code references from the data is provided in Table 1.

### Leadership Qualities

Participants consistently offered effective leadership as an important factor in providing ICT support to remote learning during the pandemic. This theme was not surprising considering all participants were leaders in their departments. Nevertheless, certain leadership qualities

were consistently highlighted as important in the early days of the pandemic.

Trust and support from HEI senior leadership was a significant factor in successful ICT support. The ability to extend influence across the organization while driving ICT projects was often related to the level of trust CIOs felt from their leadership. CIOs who felt supported were able to make quick decisions, spend money more effectively, overcome hurdles, and influence organizational opposition to ICT changes. Conversely, a lack of trust from HEI leadership negatively affected preparedness and reaction times.

Within ICT departments, support team management also played a role in successful support to remote learning. Effective ICT leaders communicated transparently with their staff and teams on a continual basis. Daily and weekly virtual update meetings offered opportunities to synchronize internal priorities and efforts across ICT divisions. They also afforded autonomy to their teams to creatively find solutions to ICT issues

**Table 1.** Naming units (codes) and themes

	Interview 1	Interview 2	Interview 3	Interview 4	Interview 5	Interview 6	Interview 7	Interview 8
<b>Leadership Qualities</b>								
Trust	X	X	X	X	X	X	X	X
Transparency	X						X	
Institutional/operation knowledge	X	X				X		X
Horizontal and vertical influence		X	X	X		X	X	X
Communication (internal & external)	X	X	X	X	X	X	X	X
Support team management	X	X			X	X	X	
<b>Customer Emphasis</b>								
People over tech		X	X		X	X	X	
Customer requirement emphasis	X	X	X	X				X
Information literacy	X	X	X	X	X	X	X	
Training			X	X	X		X	
Initial surge	X	X		X	X	X	X	X
<b>Remote Work ICT Tools</b>								
Digital transformation/cloud reliance	X	X	X	X	X	X	X	X
Leveraging existing tools	X			X	X	X		X
Core remote work capabilities	X	X	X	X	X	X	X	X
<b>Organizational Factors</b>								
Policies	X	X		X		X	X	
Planning		X			X	X	X	X
Funding	X	X			X	X		X
Governance/decision making		X	X					X
<b>Combating Digital Inequity</b>								
Computer access challenges	X	X		X			X	
Internet access challenges	X	X	X	X			X	X
Solutions	X		X	X			X	

while ensuring the “right people were in the right positions.” ICT leaders ensured request lines were manned by experienced technicians who worked well with customers. One CIO described a particularly novel approach to supporting virtual classrooms where student support staff provided live ICT support to students and teachers during their classes. Another offered flexible work hours to support staff, which extended their help desk coverage hours significantly.

### ***Customer Emphasis***

“IT is a customer service organization; we just happen to support technology.” As HEIs made the difficult decision to transition to remote learning, ICT requirements changed and increased rapidly. CIOs and their staff who well understood their customer requirements were able to flex resources and tools to critical areas quickly as teachers and students scrambled to establish workspaces at home. This was not an easy task, as one CIO related it to “putting wheels on while you are driving the car.” Initial ICT support focused mostly on establishing the basics—workstations, peripherals, and connectivity—in remote locations, while later support became more nuanced and diversified.

CIOs also stressed that ICT support should focus on people rather than technology. “The technical challenges were not the most profound because we have all kinds of technical options.” “[The biggest challenge] is getting people over hurdles of changing their behaviors and their processes,” one CIO explained. Another mentioned, “the technology stuff is easy. It’s the people stuff that . . . can make you lose your mind.” ICT leaders understood that the people behind ICT solutions are the most important factor in ICT support.

One of the primary ways CIOs addressed customers was through information literacy campaigns that included informational bulletins on new technology, message boards addressing common issues, daily email distributions with updates, etc. One CIO described this as “evangelizing the tools we are using.” Additionally, training resources for students and teachers often accompanied these campaigns.

Another critical aspect of emphasizing customer requirements was seen in the initial surges of ICT support staff. Most CIOs described the days and weeks after going remote as hectic but crucial to ensure customers had functionality. These efforts included increased work hours for many staff members, unconventional methods to deploy capabilities, and redirecting of manning and resources to critical areas.

### ***Remote Work ICT Tools***

While ICT support is people focused rather than technology focused, the tools and resources employed

during the pandemic were inarguably central in supporting remote learning and work. Consistent with the literature, cloud reliance was crucial to providing remote support. HEIs were at various stages of digital transformation with some already relying mostly on cloud services while others were primarily using on-premises solutions. The degree to which organizations were already relying on cloud services appears to be associated with ease of initial transition to remote learning during the pandemic. Furthermore, CIOs consistently reported that the pandemic had an accelerating effect on their organizations’ digital transformation strategies. Cloud transition projects that were scheduled for ten months were accomplished in two. The most commonly reported core cloud solutions were teleconference applications, learning management systems, VPN services, remote support, and virtual desktop capabilities.

Multiple CIOs stressed the importance, and sometimes fortune, in leveraging existing tools and resources toward the initial transition to remote learning. Lab laptop carts were salvaged and issued out to remote employees. Limited licenses of Microsoft Teams were expanded to include entire colleges instead of single departments. One college even reported that they were already in the process of transitioning hard telephony to Teams and fortunately had webcams and headsets on hand. In any case, leveraging existing tools and resources afforded more prepared transitions and more effective support.

### ***Organizational Factors***

Organizational factors were also consistently reported as significant in providing ICT support to remote learning during the pandemic. Many of the HEIs already had remote work and/or emergency response policies and plans in place to address remote execution. Some policies included requirements to register remote workstations with CIO offices, remote training courses, and specific support practices. However, many lacked the detail and scope necessary to address such large-scale transitions to remote work. In these cases, policies had to be updated on the fly or later during the pandemic.

Remote work planning initiatives also played a role in an HEIs ability to support mass transitions to remote work/learning. Several HEIs mentioned previous event planning activities having a direct effect on their ability to rapidly transition to remote support. One university even conducted pandemic/health emergency planning less than a year before the pandemic. These efforts, while not exhaustive, helped CIOs predict, and prepare for, some of the challenges encountered during mass remote work/learning.

Organizational factors of funding and governance also played a crucial role in the ability to provide ICT

support to remote work/learning. Most CIOs reported that significant funding became available quickly after transitions, which allowed them to purchase critical capabilities and expand cloud resources accordingly. Others recounted funding as possibly the most difficult hurdle to overcome. Relatedly, HEIs with well-established governance processes enabled CIOs to navigate budget hurdles to fund critical ICT initiatives. The ability to vet resource requirements and execute ICT purchases afforded CIOs the means to address customer requirements as they materialized.

### **Combating Digital Inequity**

Consistent with the literature, digital inequity was a common theme when discussing ICT challenges during transitions to remote learning. Many students needed additional computer resources and/or lacked adequate Internet connectivity in their homes.

HEIs addressed digital inequity issues in different ways. Some issued spare and life-cycled laptops out to students and handed out peripherals (like webcams and headsets) where needed. Internet connectivity issues were addressed in multiple ways. Some HEIs invested heavily in internet hot spots to issue out to students and teachers. Others augmented the cost of internet for in-need customers via college and/or federal funding. A common response was to include information on internet service providers in their information literacy campaigns to help customers make informed decisions. A more granular option was to offer solutions that required minimal or intermittent connectivity (like asynchronous recorded lectures). There were no one-size-fits-all solutions to combating digital inequity. HEIs weighed their customer and business cases in their approach to these challenges to different conclusions.

### **DISCUSSION AND CONCLUSION**

The COVID-19 pandemic forced mass transitions to remote learning in HEIs testing their resiliency and agility. ICT service and support were critical to enabling HEIs to continue to function while decentralized. Decentralized operations often require significantly different ICT solutions than centralized. While most HEIs provided some remote learning capabilities before the pandemic, few were prepared to transition to remote learning at such a large scale. The breadth of research on HEIs and remote learning continues to expand but largely lacks investigation into factors critical to providing remote work ICT support during an emergency.

The literature review for this study found that cloud services played a crucial role in enabling remote work. It also found that ICT systems and processes, hardware and

infrastructure, and digital inequity were likely candidates for success factors of ICT support. This qualitative research reiterated the importance of cloud, ICT systems and processes, and combating digital inequity while also finding that leadership qualities, organizational factors, and customer requirements emphasis were forefront in CIO approaches to providing ICT support during the pandemic.

### **REFERENCES**

- Alashhab, Z. R., Anbar, M., Mahinderjit Singh, M., Leau, Y.-B., Al-Sai, Z. A., & Abu Alhayja'a, S. (2021). Impact of coronavirus pandemic crisis on technologies and cloud computing applications. *Journal of Electronic Science and Technology*, 19(1), 25–40. <https://doi.org/10.1016/j.jnlest.2020.100059>
- Almaiah, M. A., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. *Education and Information Technologies*, 25(6), 5261–5280. <https://doi.org/10.1007/s10639-020-10219-y>
- Candela, M., Luconi, V., & Vecchio, A. (2020). Impact of the COVID-19 pandemic on the Internet latency: A large-scale study. *Computer Networks*, 182. <https://doi.org/10.1016/J.COMNET.2020.107495>
- Dhawan, S. (2020). Online learning: A panacea in the time of COVID-19 crisis. *Journal of Educational Technology Systems*, 49(1), 5–22. <https://doi.org/10.1177/0047239520934018>
- Dwivedi, Y. K., et al. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, 55. <https://doi.org/10.1016/J.IJINFOMGT.2020.102211>
- Favale, T., Soro, F., Trevisan, M., Drago, I., & Mellia, M. (2020). Campus traffic and e-learning during COVID-19 pandemic. *Computer Networks*, 176. <https://doi.org/10.1016/J.COMNET.2020.107290>
- Feldmann, A., et al. (2020). The lockdown effect: Implications of the COVID-19 pandemic on Internet traffic. <https://doi.org/10.1145/3419394.3423658>.
- Finney, S., & Corbett, M. (2007). ERP implementation: A compilation and analysis of critical success factors. *Business Process Management Journal*, 13(3), 329–347. <https://doi.org/10.1108/14637150710752272>
- Harting, K., & Erthal, M. (2005). History of distance learning. *Information Technology, Learning, and Performance*, 23(1), 35–44.
- Hodges, C., More, S., Lockee, B., Trust, T., & Bond, A. (2020). *The difference between emergency remote teaching and online learning*. Retrieved March 11, 2023, from <https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning>
- Jacks, T. (2021). Research on remote work in the era of COVID-19. *Journal of Global Information Technology Management*, 24(2), 93–97. <https://doi.org/10.1080/1097198X.2021.1914500>
- Kentnor, H. (2015). *Distance education and the evolution of online learning in the distance education and the evolution*

- of online learning in the United States. [https://digitalcommons.du.edu/law\\_facpub](https://digitalcommons.du.edu/law_facpub)
- Lassoued, Z., Alhendawi, M., & Bashitialshaaer, R. (2020). An exploratory study of the obstacles for achieving quality in distance learning during the COVID-19 pandemic. *Education Sciences, 10*(9), 1–13. <https://doi.org/10.3390/educsci10090232>
- Maphosa, V., & Maphosa, M. (2022). Factors influencing the adoption of ICT for remote work among Zimbabwean SMEs: A case study of Bulawayo Metropolitan province. *International Journal of Advanced and Applied Sciences, 9*(3), 150–158. <https://doi.org/10.21833/ijaas.2022.03.017>
- Mishra, L., Gupta, T., & Shree, A. (2020). Online teaching-learning in higher education during lockdown period of COVID-19 pandemic. *International Journal of Educational Research Open, 1*. <https://doi.org/10.1016/J.IJEDRO.2020.100012>
- Nasir, M. H. N., & Sahibuddin, S. (2011). Critical success factors for software projects: A comparative study. *Scientific Research and Essays, 6*(10), 2174–2186. <https://doi.org/10.5897/sre10.1171>
- OECD. (2020). *Keeping the Internet up and running in times of crisis*. Retrieved March 18, 2023, from [https://read.oecd-ilibrary.org/view/?ref=130\\_130768-5vgoglwswy&title=Keeping-the-Internet-up-and-running-in\\_times-of-crisis](https://read.oecd-ilibrary.org/view/?ref=130_130768-5vgoglwswy&title=Keeping-the-Internet-up-and-running-in_times-of-crisis)
- Papagiannidis, S., Harris, J., & Morton, D. (2020). WHO led the digital transformation of your company? A reflection of IT related challenges during the pandemic. *International Journal of Information Management, 55*. <https://doi.org/10.1016/j.ijinfomgt.2020.102166>
- Rachmawati, R., Choirunnisa, U., Ayuningsih Pambagyo, Z., Atikah Syarafina, Y., & Adriadi Ghiffari, R. (2021). Work from home and the use of ICT during the COVID-19 pandemic in Indonesia and its impact on cities in the future. *Sustainability (Switzerland), 13*(12). <https://doi.org/10.3390/su13126760>
- Sandford, A. (2020). *Coronavirus: Half of humanity now on lockdown as 90 countries call for confinement*. EuroNews.
- Singh Hundal, G., Thiyagarajan, S., Alduraibi, M., Laux, C. M., Furterer, S. L., Cudney, E. A., & Antony, J. (2021). Lean Six Sigma as an organizational resilience mechanism in health care during the era of COVID-19. *International Journal of Lean Six Sigma, 12*(4), 762–783. <https://doi.org/10.1108/IJLSS-11-2020-0204>
- Sull, D., Sull, C., & Bersin, J. (2020). Five ways leaders can support remote work. *MIT Sloan Management Review*. <https://mitsmr.com/3cAECul>.
- Tallon, P. P., Queiroz, M., Coltman, T., & Sharma, R. (2019). Information technology and the search for organizational agility: A systematic review with future research possibilities. *Journal of Strategic Information Systems, 28*(2), 218–237. <https://doi.org/10.1016/j.jsis.2018.12.002>
- Vogels, E., et al. (2020). [www.pewresearch.org](http://www.pewresearch.org).
- Wahab, A., & Ali, W. (2020). Online and remote learning in higher education institutes: A necessity in light of COVID-19 pandemic. *Higher Education Studies, 10*(3). <https://doi.org/10.5539/hes.v10n3p16>

## **Hypersonics: A Case History of the Dynamic Soarer Project, and Questions to Consider with the Adoption of Exotic Technologies**

Nicholas Michael Sambaluk, PhD<sup>1</sup>

Hypersonic missiles stand among the exotic technologies unleashed during the current fighting in Ukraine, but their abrupt appearance belies a need to contextualize and reflect. Russian authorities first claimed to have used hypersonic missiles in March 2022, just one month into the escalation of a war that Russia had waged against Ukraine in much lower intensity since 2014 (Kirby, 2022). Given Russia’s early embarrassments and the prosaic initial target selection, the first use of hypersonic weapons seemed to fall flat against their futuristic sci-fi-style hype.

Some analysis, as that by the Brookings Institution, has dismissed the Russian Kinzhal or “Dagger” missile as a pseudohypersonic, characterizing it as “an air-launched ballistic missile” rather than a true hypersonic glide or cruise system. Furthermore, such analysts hasten to rebuff ideas that hypersonics are destabilizing or that Russian technology has surpassed US technology, or that even true hypersonic weapons are immune to interception (Montgomery & Nelson, 2023).

Meanwhile, as open-source media touted the Ukrainian claims of having downed Kinzhal missiles by using US-supplied Patriot missile defense batteries and scoffed at the Russian counterclaims (Garanich & Karazy, 2023), NORAD commander General Glen VanHerck simultaneously told a Senate Armed Services subcommittee that “Hypersonic weapons are extremely difficult to detect and counter given the weapons’ speed and maneuverability, low flight paths and unpredictable trajectories” (Vergun, 2023), and the Congressional Budget Office implied that hypersonics bear few mitigating near-term advantages relative to ballistic missiles, in view of their higher costs and ongoing technological hurdles and the remaining efficacy of ballistic systems (Congressional Budget Office, 2023).

In short, the jury is still out regarding hypersonic technology in warfare. And that should not be surprising, since the first combat use of even a pseudohypersonic is less than a year and a half old. But although the first combat use is fresh, the idea is older. And the time is right to acknowledge the early history of hypersonic weapons research and thought. Hypersonics were first recognized as a cutting-edge military-applicable technological area eight decades ago, and top-ranking US Air

Force figures advocated hypersonic weapons systems in the late 1950s. A grounding in the early history is a tool to use when reflecting on the role and future of hypersonic weapons, in the midst of the fog of war reports from an ongoing conflict.<sup>2</sup>

In the mid-1950s, when hypersonic speeds exceeding Mach 5<sup>3</sup> were the stuff of science fiction, the US Air Force was riding particularly high. It had experienced enormous growth during World War II, had achieved greater doctrinal autonomy by midwar, had performed a range of missions to contribute to Allied victory, and, after delivering the last heavy blows culminating in Japanese surrender, could argue that it had played a decisive role in winning World War II.

Service independence came in 1947, and concern about the potential for a Soviet surprise attack (and the potential for revolutionary enemy technologies in the future) implied to Air Force apologists a need for continually advancing Air Force technologies in turn. The service saw its most vital role as being the atomic strike mission that underpinned the massive retaliation approach to the US defense posture in the 1950s. Airpower advocates believed in the mid-1950s that President Dwight Eisenhower agreed with their vision, as the Air Force received half of the nation’s *total* contemporary defense budget.<sup>4</sup>

The “spiraling expansion of technology” demanded alertness to the advent of new tools that could achieve familiar missions on into the future. Thus, while the newly installed Strategic Air Command (SAC) head General Thomas Power indicated that it is “highly unlikely that there will ever be such a thing as an ‘ultimate’ strategic weapon,” the ongoing effort would never reach an end point (Power, 1959, p. 488).

The Air Force’s first interest in hypersonics grew, albeit slowly, in this context during the mid-1950s. Increasingly capable nuclear bombers with increased speed and range opened the door to performing the massive retaliation mission more comprehensively against anticipated Soviet targets; whereas the survivability of the B-36 had been the subject of intense and high-profile controversy (Curatola, 2002, p. 54–59), and the speedier B-47 had still not addressed the range requirements of round-trip missions, the B-52 had begun to deliver on US airpower chiefs’

expectations. The as yet nascent threat of future surface-to-air missile technology brought Air Force leaders to the realization that B-52s would eventually need to be supplemented by stand-off cruise missiles or supplanted by still faster and higher-flying bombers. So the futuristic sketches of an atmosphere-skimming plane of extreme speed and virtually limitless range was appealing, but it seemed far from urgent. The first notable hypersonics advocacy in the United States came with Bell Aircraft's hiring of Walter Dornberger, the ex-Nazi general who had been Wernher von Braun's superior at Peenemünde.

A limited study of a system boosted on a rocket and making an extended high-speed glide was codenamed Hywards and begun in 1954. Likewise, small-scale research into reconnaissance (Brass Bell, initiated in 1955) and bombardment (Bomber Missile BoMi, later rechristened Rocket Bomber RoBo as of the mid-1956) could proceed at a deliberate pace, assisted by the National Advisory Committee for Aeronautics (NACA) efforts to extend the state of the art in aviation. Established in 1915 as an entity to support US technical development regarding aviation, NACA was not unjustifiably interpreted by Air Force planners as a support in ambitious research efforts (Sambaluk, 2012, p. 36; Anderson, 1981, pp. 3–4). Indeed, NACA director Hugh Dryden told his employees that “no vehicle as important as the boost-glide research vehicle . . . could proceed without the active participation and cooperation of the NACA.” NACA's internal memos optimistically indicated that “the hypersonic glide rocket concept offers a breakthrough in weapon system capability in terms of obtaining speed, range, and altitude simultaneously,” and “this research system should be able to generally support the Air Force research and development effort in the development of superior weapon systems for many years to come.”<sup>5</sup>

The as yet back-burner interest was reflected in the Air Research and Development Command's missile boss Major General Bernard Schriever's February 1959 statement that “in the *long run* our safety as a nation may depend upon our having space superiority” (italics added) (Schriever, 1957; n.d.). NACA noted “many detail design problems,”<sup>6</sup> and in the middle of 1957, the Air Force contemplated merging the Hywards, Brass Bell, and RoBo study projects into a single effort, in order to pool the remaining project resources. What transformed the Air Force's sense of urgency was the advent of the space race with the launch of the Soviet Sputnik I satellite, the first artificial object to orbit the planet. The Soviet launch marked a notable milestone in a contest that both superpowers had embarked on in preparation for the International Geophysical Year (IGY), July 1957 through December 1958. An episodic scientific tradition intended to extend human knowledge and to divert competition away from strife,

the next IGY's inclusion of a space element carried strategic importance for superpower policymakers.

Soviet hostility, secrecy, and an acumen for eradicating Free World intelligence operatives heightened the US need for image and signal intelligence. By 1954, the Eisenhower administration had decided on the long-term need for a reconnaissance satellite, interim development of an extremely high-altitude reconnaissance plane, and the establishment of international norms insulating intelligence gathering from interception (Dockrill, 1996, pp. 49–59). Soviet rejection of Eisenhower's “Open Skies” proposal in 1955 (Smith, 2013, pp. 667–670) made a sanctuary status for space all the more crucial for US policymakers.

Sputnik I's launch meant that the USSR had itself established the prerequisite precedent that Eisenhower officials had quietly wanted since 1954 to cement. However, the high-profile Soviet technological feat simultaneously kicked US Air Force hunger for spacefaring defense technologies into much higher gear. Eisenhower's domestic political opponents, like Senate Majority Leader Lyndon Johnson, saw the high-tech Soviet achievement as a gap in the president's political armor on security issues. “Sputnik has finally killed the ‘Ike knows all about defense’ myth,” defense hawk and media commentator Stewart Alsop agreed to Johnson in the wake of the event (Frank, 2013, p. 160). In this environment defined by Soviet achievements, muted administration assurances, and shrill declarations from the media and Capitol Hill, space security issues were prone to become politicized.

In this new environment, space-minded Air Force leaders stepped up their efforts to explore and exploit the new domain. The Air Staff now not only approved the pending hypersonic research consolidation into a single Dynamic Soarer, or Dyna-Soar, project, but directed an acceleration of the ambitious program. Dyna-Soar I, II, and III embodied the old goals of Hywards, Brass Bell, and RoBo, and the proposed timelines of each were accelerated, so that a Dyna-Soar III space bomber was desired by 1968.<sup>7</sup> Space development seemed important because, particularly in the wake of the adversary's new space achievement, “the classic sustained flight air breathing engine approach to strategic mission accomplishment is very limited and has very little growth potential.”<sup>8</sup> The massive retaliation mission now demanded the expedited development of radical technology. There was “no division, per se, between air and space; [there is] only one indivisible field of operations above the surface of the Earth,” argued Air Force chief of staff General Thomas White, who popularized the term “aerospace” to make his point to Capitol Hill (Bowen, 1964, pp. 183–184; Sambaluk, 2015, pp. 71, 75).

But this perspective fundamentally clashed with the president's confidential need for space sanctuary and intelligence collection. Eisenhower's Air Force secretary quickly shut down a Directorate of Astronautics in December 1957, which had been initiated by space-minded generals. During 1958, the Advanced Research Projects Agency was established as a repository for space projects, so that the administration could at least temporarily remove them from military control. Months later, NACA was statutorily transformed from being the Air Force's research *helper* to being a potential *rival* in the space realm.

Frustrations continued to mount. In October 1958, as NASA was being officially established, White noted that "this [Dyna-Soar] program represents the first of a new generation of strategic weapons systems. It will enable the United States to maintain its military posture of major war deterrence by having in-being a known capacity to nullify air defense systems designed to combat air-breathing manned vehicles and predictable ICBM trajectories."<sup>9</sup> But precursor projects, such as a Man in Space demonstrator that was meant to show human capacity to survive (and work) in the space environment, risked being poached by ARPA or NASA, as occurred when the administration deleted Man in Space from Air Force authority before the announcement of NASA's Mercury program (Sambaluk, 2015, pp. 85, 127).<sup>10</sup> In this context, Air Force secretary James Douglas's October 1958 message that ARPA aimed to oversee "only projects which are designed to attain or exceed velocities necessary for stabilized orbits" prompted protective space advocates in the Air Force to conclude that Dyna-Soar I "should clearly be designated a military research vehicle programmed for *suborbital* velocities."<sup>11</sup>

This gambit succeeded in staving off the loss of the Dyna-Soar program to ARPA, but it inadvertently permitted a lengthy new program review to be ordered in April 1959 that dragged on for a year (Rosenberg, 1962).<sup>12</sup> Dyna-Soar emerged from review just weeks before the downing of a U-2 spy plane on May 1, 1960, and the secret first successful satellite mission in August. Not privy to these highly secret successes, Air Force deputy chief of staff for development Lieutenant General Roscoe Wilson in September 1960 declared the Dyna-Soar to be "the most important research and development project" that the Air Force had (Sambaluk, 2015, p. 111).

The dawn of the space race had thus opened a fissure between the Air Force's senior futurists and the Eisenhower administration, and this widened until his departure from office. Eisenhower's farewell address, which would later come to be celebrated and lauded, warned of the dangers both of a military-industrial complex and of the potential dominance of a scientific-technological elite. It met an initially mixed reception, and Air Force

analysts predicted shortly before the 1960 election that a victory by John F. Kennedy should lead to favorable changes in executive posture in relation to the Air Force and its space ambitions ("Maj. Abbott C. Greenleaf," n.d.)

Although candidate Kennedy had proven elusive about which "strategic concept he endorses," Air Force leaders were reassured by the apparent influence of former Air Force secretary (and contemporary Missouri Democratic senator) Stuart Symington, whose "views . . . appear to be very close—if not identical in most respects—to the USAF position" on defense matters ("Maj. Abbott C. Greenleaf," n.d.). Kennedy had called for investment in several areas, including the "missile-space" arena, and this encouraged Air Force planners.

Kennedy's administration got off to a shaky start. Just two weeks after inauguration his defense secretary's public disclosure that the "missile gap" that had helped define the presidential campaign had been a red herring (Raymond, 1961). Kennedy went before a joint session of Congress in March to announce defense adjustments timed to lessen the political damage; in this context Kennedy fine-tuned bomber and missile strengths and charted a \$100 million investment course for Dyna-Soar, between a begrudging \$70 million planned by Eisenhower and the Air Force's \$146 million request (Kennedy, 1961a). April saw further setbacks, in the Soviet's first human to orbit Earth and a US-backed debacle meant to topple communist forces in Cuba. Kennedy searched desperately for a space goal that would be simultaneously achievable and valuable enough to offer the United States national prestige, yet without being so close to possibility within the state of the art that the Soviet Union might again soon upstage the United States. The result was the human lunar landing and the Apollo program, ostensibly because "no single space project in this period will be more impressive to mankind, or more important for the long-range exploration of space" (Kennedy, 1961b).

Interestingly, some in the audience may have felt differently. The same month that Kennedy delivered his famous moon speech, the House Appropriations Committee expressed that "the Dyna-Soar concept provides the quickest and best means of obtaining . . . an operational, manned military space vehicle over which the pilot has the greatest possible control."<sup>13</sup> During the remainder of Kennedy's first year in office, the Dyna-Soar's supporters continued to work to accelerate the program. An accelerated development was in fact authorized in November, but analysis by the aviation trade journals noticed a change in the Dyna-Soar's apparent emphasis. It was "no longer being pushed as a potential offensive weapon system" ("Industry observer," 1961).

The administration supported the development of a new booster, derived from the Titan intercontinental



ballistic missile and ostensibly capable of boosting the Dyna-Soar craft (Finney, 1961). But officials of the new administration seemed more tentative in relation to the craft being boosted; Defense Secretary Robert McNamara said early in 1962 that “we cannot say categorically [that] it will yield an important weapon” but merited developmental activity (“This is Dyna-Soar,” 1962).

The Air Force moved forward even as the program’s direction continued to endure warping. The first half dozen Dyna-Soar pilots, including Purdue University alumnus Neil Armstrong, were selected in March 1962, but the *New York Times* noticed that “the actual training of the Dyna-Soar astronauts has not begun, partly because of the uncertainty and controversy still surrounding the project” (Matranga et al., 2003; Palmer, 1961; “50 airmen,” 1961).<sup>14</sup> In late September, the program was redesigned as an X-plane; this highlighted the experimental and research character, rather than the proto-operational intent, of the program. Undersecretary of the Air Force Victor Charyk, who had played a role in the Dyna-Soar’s year-long review phase from 1959 to 1960, told the Air Force Association convening in Las Vegas that, “The X-20 does not represent a vehicle for a specific military job, but neither did the Wright Brothers’ airplane nor Robert H. Goddard’s early rockets, and yet, without the pioneering effort, without the vision, without the search for new knowledge and without the determination to explore the unknown, the fruits of these efforts could never have been realized. And so it is, I believe, with the X-20.”<sup>15</sup>

It was a misleading comparison, since the Air Force had *always* viewed the Dyna-Soar as a craft to serve a military purpose, whereas neither Goddard nor the Wright Brothers had intended to weaponize the fruits of their flight research. But worse was in store. McNamara ruminated about Dyna-Soar integrating with NASA’s Gemini (a conical two-crew spin-off of the Mercury craft) as early as 1962. In 1963, he demanded comparison about four military missions: satellite inspection, satellite defense, reconnaissance, and orbiting an offensive weapon system.<sup>16</sup>

Analysts answered that neither system was postured for the identified tasks, that Gemini promised superior in-space maneuverability but a rigid (and vulnerable) vehicle recovery regimen, whereas Dyna-Soar’s maneuverability concentrated on atmospheric reentry.<sup>17</sup> This reinforced McNamara’s impression of the Dyna-Soar as being an ongoing *reentry research* platform rather than being the first phase of a military system with a specific mission set, and he was already on record being unenthused with a maneuverable reentry focus (Houchin, 1995, p. 333).

By October 1963, a preliminary bilateral renunciation of orbital weapons of mass destruction was in the

offing; apparent progress toward a repudiation of space-based orbital weapons of mass destruction seemed ready to negate the very concept of a spacefaring system executing the Air Force’s massive retaliation mission. Following Kennedy’s November assassination and Johnson’s accession to power, McNamara was charged with trimming the new president’s initial defense spending. Deleting Dyna-Soar was an easy decision for McNamara, who characterized the program as having lacked a focus or purpose (McNamara, 1963).

McNamara and his advisors may have been unaware of (or ignored) the Air Force’s *very* specific original purpose in the project; conceivably, the Air Force’s 1958 gambit to prevent the project’s transfer to NASA may have worked *too* well, obscuring (outside the Air Force) the intended mission of performing reconnaissance and bombing in an air defense/access denial environment unsurvivable by jet planes. Certainly, for the McNamara Defense Department, activity *in* space was more interesting than maneuver *from* space: simultaneous with cancellation of the Dyna-Soar, McNamara marked the beginning of a manned orbital laboratory (MOL) that would explore the ability of humans to operate in orbit for a relatively extended period of time. Ironically, the myopic and cost-conscious defense czar replaced the Dyna-Soar (which had cost almost \$500 million over six years) with MOL, which would consume three times as much funding during its equally brief and equally fruitless programmatic existence.

After the cancellation of the Dyna-Soar project, other work was done under the auspices of NASA, generally in relation to flight using lifting bodies wherein a high lift-to-drag ratio could be accomplished without a craft having differentiated wings. This work, commemorated by the presence of the M2-F3 lifting body in the National Air and Space Museum in Washington, D.C., interested NASA but had no immediate application matching Air Force priorities in the way that a spacefaring reconnaissance and bombing platform had done.

Several factors stand out when reflecting on the Cold War–era precedent and current hypersonic research and development.

First is the issue of doctrinal continuity and the expectation that advances in technology would themselves drive the direction of policy and strategy. Continuity personified Air Force intentions in the 1950s, as the framing of the “aerospace” thinking indicated. And the expectation that advancing technology would be met by other technologies was almost palpable in the trade press and among aerospace advocates of the era. Modern US interest in swift precision strikes carries a spiritual continuity with Air Force aspirations throughout the post–Cold

War period, and although arms control voices figure into modern conversation (Speier et al., 2017; Bugos and Reif, 2018), wars have a way of accelerating (some) weapons development and eroding reservations about weapons use. Recent investments—(\$8 billion by the US military from 2019 to 2022, and the Defense Department is requesting \$13 billion for the period running from 2023 to 2027) suggest a receptive policy landscape (Congressional Budget Office, 2023).

Second, it is worth acknowledging that formidable technological hurdles remain. Although US research flirted, in the X-43, with speeds on the cusp of Mach 10 two decades ago, the fielding of practical hypersonic weapons has remained a stubborn and thorny economic and engineering challenge (“NASA’s X-43A,” 2010).

Next, the form of hypersonic weapon system envisioned in the 1950s differed greatly from the fielded and conceptualized weapons of the 2020s. In the former case, space power advocates wanted a piloted vehicle; it was not yet practical to trust the reliability of ballistic missiles, and this seemed to demand a futuristic poststrike reconnaissance and follow-up bombardment requirement. Today, these are not concerns—but the defeat of air defense/area denial systems and the desire for highly effective nonnuclear strikes are. It is unsurprising, then, that the attention has shifted from vehicles to projectiles.

Finally, a related point. Whereas *modern* interest in hypersonics intrinsically derives from the air defense–defeating potential of Mach 5+ speeds as well as the potentially ferocious kinetic energy during a strike, it is worth noting that the hypersonic speeds were of comparatively incidental interest to advocates in the 1950s. Yes, there was keen faith that platforms flying “higher, faster, and farther” represented the future of aerospace power, but the hypersonically faster speeds were in large measure contingent on the higher and farther elements that were of at least equally great importance to Air Force leaders who had long striven to establish a retaliatory force with truly global range.

While current claims can be debated or disbelieved, and future predictions demand scrutiny and even skepticism, a reflection on history can lend the chance to gain perspective about a security topic that is again a seemingly imminent presence in warfare.

## NOTES

1. The views expressed in this study are those of the author, and they are not a reflection of the official position of the United States Air Force.
2. The Dyna-Soar’s history has been explored by a small number of researchers. For historians such as Richard Hallion (editor of the three-volume *The Hypersonic Revolution*, 1987–1988) and Roy Houchin (Houchin, 2007), the ultimate cancellation represented a lost opportunity. Sites such as *DefenseMediaNetwork* condemn the cancellation as an “uninformed decision” that was “one of the great missed opportunities of the 1960s” (Simonsen, 2013). In contrast, I offer a revised perspective (Sambaluk, 2013) that frames the project’s development, as well as its cancellation, in the context of the Dyna-Soar’s relationship to security policy and the contrasting perspectives of the executive branch and of the Air Force about whether reconnaissance would serve to provide stabilizing warning capabilities or alternatively pre/poststrike intelligence during combat.
3. Although a ballistic missile’s terminal velocity far exceeds Mach 5, and such speeds were first demonstrated in a weapon with the Nazi V-2 missile during World War II, such trajectory-derived terminal velocities are not conventionally deemed as meeting the definition of hypersonic flight.
4. In the middle of the decade, the Air Force received 47% of the DOD budget. The Navy and the Marine Corps combined got 29%, and the Army oversaw 22% (Wills, 2010, pp. 44–45; Leighton, 2001, p. 33).
5. Memo for Record, “Meeting of NACA Personnel at NACA Headquarters February 6, 1957 to Discuss Possible Hypersonic Research Airplane,” February 6, 1957. 11924 “Round Three’ Background Correspondence,” NASA HQ; “Project Research System: Hypersonic Glide Rocket Research System; Hypersonic Weapons Research & Development Supporting System,” December 28, 1956. 11924 “Round Three’ Background Correspondence,” NASA HQ.
6. Memo for NACA Director, “Meeting of NACA Personnel Held at NACA Headquarters February 6, 1957, to Discuss Possible Hypersonic Research Airplane,” February 6, 1957. 11924 “Round Three’ Background Correspondence,” NASA HQ.
7. The Dyna-Soar I target was accelerated from 1963 to 1962, and Dyna-Soar II from 1969 to 1967; Dyna-Soar III shifted up from an earlier development target date of 1974 (Bowen, 1964, p. 46). “Abbreviated System Development Plan,” August 23, 1957 (Godwin, 2003, pp. 40–51).
8. “Abbreviated System Development Plan.” August 23, 1957 (Godwin, 2003).
9. Memo from White to Air Force Secretary Douglas, “Priority Program Augmentations to Basic 1959 Budget Estimate,” October 3, 1958. Fldr Secretary of the Air Force #2, Box 18, White Papers, Library of Congress.
10. “DOD in Space,” NASA HQ. Lt. Gen. Putt, memo, January 31, 1958. 11130 “DOD in Space,” NASA HQ; White, “Memorandum for DCS/Development,” September 8, 1958; Fldr Chief of Staff Signed Memos Jan 58-Dec 58, Box 15, White Papers, Library of Congress.
11. Memo from Air Force Secretary Douglas to Chief of Staff White, October 13, 1958. Fldr Secretary of the Air Force #2, Box 18, White Papers, Library of Congress.
12. “Dyna-Soar Milestones,” 168.7127-38; “Information for Dr Charyk,” May 5, 1960 (Godwin, 2003, pp. 117–119).

13. Quoted in "Air Force Information Fact Sheet: X-20 Dyna Soar," January 1963, 11325 X-20 Dyna-Soar Documentation, NASA HQ.
14. Gene J. Matranga, William H. Dana, and Neil A. Armstrong, "Flight Simulated off the Pad Escape & Landing," March 1962 (Godwin, 2003, pp. 219–236).
15. Joseph V. Charyk, "DOD Press Release: Unveiling X-20," September 20, 1962 (Godwin, 2003, p. 254).
16. "Lectures in Aerospace Medicine," February 4-8, 1963, 168.7082-867, AFHRA.
17. Clarence J. Geiger, "History of the X-20A Dyna-Soar," October 1963 (Godwin, 2003, pp. 400–401).

## REFERENCES

- 50 airmen picked for space flights; Would fly military missions – projects still debated. (1961, July 23, p. 33). *The New York Times*.
- Anderson, F. W. (1981). *Orders of magnitude: A history of NACA and NASA, 1915–1980*. NASA Scientific and Technological Branch.
- Bowen, L. (1964). *Threshold of space: An Air Force history of space activities, 1945–1959*. USAF Historical Division Liaison Office.
- Bugos S., and Reif, K. (2018). *Understanding hypersonic weapons: Managing the allure and the risks*. Arms Control Association.
- Congressional Budget Office. (2023, January). *US hypersonic weapons and alternatives*. Retrieved June 13, 2023, from <https://www.cbo.gov/publication/58924>
- Curatola, J. M. (2022). *Autumn of our discontent: Fall 1949 and the crises in American national security*. Naval Institute.
- Dockrill, S. (1996). *Eisenhower's New-Look national security policy, 1953–*. Palgrave Macmillan.
- Dyna-soar pilots chosen. (1962, March 19). *Missiles and Rockets Magazine*.
- Finney, J. W. (1961, December 24). Clearance given for giant rocket; Advanced missile slated for big load-lifting job. *The New York Times*.
- Frank, J. (2013). *Ike and Dick: Portrait of a strange political marriage*. Simon and Schuster.
- Garanich, G., and Karazy, S. (2023, May 16). *Kyiv says it shoots down volley of Russian hypersonic missiles*. Reuters. Retrieved June 13, 2023, from <https://www.reuters.com/world/europe/air-defence-systems-repelling-attacks-ukraine-early-tuesday-officials-2023-05-16/>
- Godwin. R. (Ed.). (2003). *Dyna-Soar: Hypersonic strategic weapons system*. Apogee Books.
- Houchin, R. (1995). *The rise and fall of Dyna-Soar: A history of Air Force hypersonic R&D, 1944–1963* [PhD Dissertation, Auburn University].
- Industry observer. (1961, November 20). *Aviation Week*.
- Kennedy, J. F. (1961a). *Special message to Congress on defense spending, March 28, 1961*. Retrieved May 21, 2023, from <http://www.presidency.ucsb.edu/ws/index.php?pid=8554#axzz1crwqH0MG>
- Kennedy, J. F. (1961b). *Address to joint session of Congress, May 25, 1961*. John F. Kennedy Presidential Library and Museum. Retrieved May 21, 2023, from <https://www.jfklibrary.org/learn/about-jfk/historic-speeches/address-to-joint-session-of-congress-may-25-1961>
- Kirby, P. (2022, March 19). *Russia claims first use of hypersonic Kinzhal missile in Ukraine*. Accessed June 13, 2023, from <https://www.bbc.com/news/world-europe-60806151>
- Leighton, R. (2001). *Strategy, money, and the New Look, 1953–1956*. Historical Office of the Secretary of Defense.
- McNamara, R. S. (1963, December 10). *Cancellation of the X-20 Program* [News brief].
- Montgomery, A. H., and Nelson, A. J. (2023, May 23). *Ukraine and the Kinzhal: Don't believe the hypersonic hype*. Brookings. Accessed June 13, 2023, from <https://www.brookings.edu/blog/order-from-chaos/2023/05/23/ukraine-and-the-kinzhal-dont-believe-the-hypersonic-hype/>
- NASA's X-43A is a hypersonic, scramjet-powered research aircraft designed to fly at speeds up to Mach 10*. (2010, September 2). NASA. Retrieved May 10, 2023, from <https://www.nasa.gov/missions/research/x43-main.html>
- Palmer, C. B. (1961, June 25). Search for spacemen. *New York Times*, pSM28.
- Power, T. (1959). Strategic air command and the ballistic missile. In E. Emme (Ed.), *The impact of air power* (p. 488). Van Nostrand.
- Quoted in "Air Force Information Fact Sheet: X-20 Dyna Soar," January 1963, 11325 X-20 Dyna-Soar Documentation, NASA HQ.
- Raymond, J. (1961, February 7). Kennedy defense study finds no evidence of a "missile gap." *The New York Times*.
- Rosenberg, M. (1962). *The Air Force in space, 1959–1960*. USAF Historical Division Liaison Office.
- Sambaluk, N. M. (2015). *The other space race: Eisenhower and the quest for aerospace security*. Naval Institute Press.
- Schriever, B. A. (1957). *ICBM – A step toward space conquest*. <http://www.astronauticsnow.com/history/schriever/index.html>.
- Schriever, B. A. (n.d.) [Public statements on important military issues]. Air Force Historical Research Agency, Maxwell AFB (Roll 35253, IRIS 1040169)
- Simonsen, E. (2013, April 5). *Cancelled US aircraft programs: A look at what might have been*. DefenseMediaNetwork. Retrieved June 12, 2023, from <https://www.defensemedianetwork.com/stories/cancelled-u-s-aircraft-programs/2/#:~:text=10%2C%201963%2C%20Secretary%20of%20Defense,done%20enormous%20amounts%20of%20research>
- Smith, J. E. (2013). *Eisenhower in war and peace*. Random House.
- Speier, R. et al. (2017). *Hypersonic missile nonproliferation: Hindering the spread of a new class of weapons*. RAND Corporation.
- This is Dyna-Soar. (1962, January). *Boeing Company News*.
- US hypersonic weapons and alternatives*. (2023). Congressional Budget Office. Retrieved June 13, 2023, from <https://www.cbo.gov/publication/58924>.

Vergun, D. (2023, May 10). *General says countering hypersonic weapons is imperative*. US Department of Defense. Retrieved June 13, 2023, from <https://www.defense.gov/News/News-Stories/Article/Article/3391322/general-says-countering-hypersonic-weapons-is-imperative/#:~:text=>

Missile%20threats%20to%20the%20U.S.,North%20American%20Aerospace%20Defense%20Command  
Wills, G. (2010). *Bomb power: The modern presidency and the national security state*. Penguin.

# Outlining the Development of Instructional Resources for Cyberphysical Security Mitigation and Preparedness

**Rylee Lane**

Purdue Homeland Security Institute, Dept. of Computer and Information Technology  
Purdue University  
lane85@purdue.edu

**Shawn Ehlers, PhD**

Dept. of Agricultural and Biological Engineering  
Purdue University  
sehlers@purdue.edu

**Glaris Lancia Raja Arul**

Dept. of Computer and Information Technology  
Purdue University  
lanciaraja72@gmail.com

**J. Eric Dietz, PhD, PE**

Dept. of Computer and Information Technology  
Purdue University  
jedietz@purdue.edu

**Abstract** Attacks on cyber-physical systems (CPS) have continued to increase with the rapid adoption of technology across different facets of life, with attacks on critical infrastructure costing entities physical and financial losses. In turn, there is a growing need to address the weak points of CPS security, particularly with respect to educating and empowering the workforce to stay vigilant and respond appropriately to potential attacks. This study focuses on the development of instructional resources to address the key points that need to be incorporated in CPS training videos. The aim is to develop training videos that cover essential topics in an informative and engaging manner. The study outlines the design and formatting characteristics that need to be incorporated to construct effective instructional content with an emphasis on the development of just-in-time training. The study was developed as a project assignment in a graduate-level course titled Foundations of Homeland Security, which is used as an elective course at Purdue University for computer and information technology, cybersecurity, and agricultural security students. Future work would involve quantitative assessments of the training materials developed from guidance in this study.

## INTRODUCTION

Cyber-physical systems (CPS), as defined by the National Institute of Standards and Technology (NIST), refer to systems that consist of “interactive digital, analog, physical and human components engineered for function through integrated physics and logic” (Cyber-Physical, 2017). In contextual terms, CPS comprise a major portion of key infrastructure across a variety of industries. They also provide a foundation for various services and applications available through products that are in use in daily life. The aim of CPS is to improve the quality of life and contemporize traditional processes across different

areas. Given the extent to which CPS remain foundational to critical infrastructure, it is no surprise that the security of such systems is a vital focus area for ensuring homeland security, especially in the wake of increasing attacks against physical infrastructure (Department of Homeland Security, 2023).

In early 2020, the Texas Department of Transportation fell victim to a ransomware attack, just days after a ransomware attack on the state’s judicial agencies (Ropek, 2020; Coble, 2020). The attacks forced officials to shut down networks, with the agencies from the first attack losing access to key management systems and legal documents that were available only online. Perhaps the most

prominent attack on key infrastructure in recent times was the Colonial Pipeline ransomware incident, which led to the shutdown of the largest fuel pipeline system in the US and subsequently to fuel shortages in serviced areas (Turton and Mehrota, 2021). Subsequent investigations found that the cause of the incident was a compromised password. These are just examples of attacks with large consequences in recent times, and with the increased adoption of CPS across all aspects of life, systems continue to be vulnerable to various kinds of attacks.

In response to such attacks, there have been calls across government and other entities for bolstering defenses against threats to CPS, including debates on legislation surrounding cyber hygiene of federal employees (Peters, 2021). This is in line with academic research on general protective or mitigative actions in cybersecurity, one of which calls for changes in individual behaviors and responses to attacks (Yaacoub et al., 2020). The preventative actions that can be taken by people is vital for emergency preparedness as specific personnel who interact frequently with CPS are the first line of defense against attacks on the systems. However, they are not the only individuals who might have access to such systems. Any employee who is a part of the system essentially represents an access point to the system. Therefore, it is important for all personnel across organizations to be aware of the different threats to CPS and the different responses that need to be taken on identification of threats.

One of the ways in which this can be achieved is by training individuals to detect such attacks, not only in organizational settings but also across individuals and those preparing for careers across the gamut of cybersecurity applications. The objective of this study is to develop general guidance for security professionals in developing training related to CPS security. This material could be used as a continuing education preventative, for hardening of the CPS, or for rapid deployment as a just-in-time response to an event. The guidance will be developed in the form of instructional videos and guidelines to emphasize the known and necessary elements to defend against CPS attacks and the cognitive capabilities of individuals with respect to learning and application.

With advances in computing and development of embedded systems, CPS has been rapidly adopted to increase the efficiency and robustness of large-scale infrastructure and its processes. One of the hallmarks of CPS is that it encapsulates technologies and processes whose main aim is not merely providing computations (Shi et al., 2011). Examples of this can be seen in industries such as medical and health care, automotive, energy systems, smart applications, and industrial controls (Khaitan and McCalley, 2015). CPS have become ubiquitous across various areas of life owing to the benefits of

efficiency, scalability, and timeliness that are associated with these systems. However, ubiquity means that CPS present themselves as a unique target for attackers to seriously compromise large-scale systems, with devastating consequences. Considerable efforts in research are being made to identify the kinds of threats that can be posed to these systems and the defensive or mitigative actions that can be taken.

In their review of incidents involving CPS, researchers proposed a taxonomy of attacks on CPS based on the type of attack itself, the industrial target, the intention of the attacks, impacts, and incident categories in terms of classification as crimes (Al-Mhiqani et al., 2018). They also identified 18 unique incidents of attacks on CPS of countries in the Middle East–North Africa region. The targets largely tended to be military or government agencies, and attacks were generally launched with the intention of disrupting operations and procuring sensitive data. Attackers in the identified incidents tended to use targeted phishing emails to launch viruses and hijack accounts to gain access to systems.

Another classification of CPS threats considered the categories related to the integrity of data and access to the systems, such as information disclosure and denial of service (Alguliyev, 2018).

Other threats to CPS include lack of comprehension or identification of the threats and limited security considerations applicable to CPS. Examples of threats to CPS include man-in-the-middle attacks, spoofing in the system, and compromised keys (Ashibani and Mahmoud, 2017).

These threats are largely generic, and the variety of technical attacks differ based on the layer of CPS that is being targeted. Some of the detection strategies discussed in the research include algorithm detection techniques, robustness checks, and fault detection and isolation techniques (Alguliyev, 2018). Researchers also suggested that threat and vulnerability identifications are important aspects of defense strategies (Ashibani and Mahmoud, 2017).

It is worth noting that academic studies largely emphasize the development and bolstering of computational and technical countermeasures (Li et al., 2020). The deployment of countermeasures can be automated to some extent, but it largely falls on the individuals that regularly maintain and interact with CPS components to ensure the proper functioning of the measures. Attacks can be executed by insiders, who would already have extensive or adequate knowledge about the systems to execute attacks with relative ease (Ashibani and Mahmoud, 2017). Not only are employees capable of launching attacks on CPS, but they can be victims of such attacks by being unwitting accessories. Employees

are also susceptible to physical threats such as infected devices and social engineering attacks, wherein attackers take advantage of common behaviors and attitudes of individuals to manipulate them into divulging sensitive information or performing a specific behavior (Resolver, 2021). Human errors accounted for more than 100 incidents that affected around 130 million people in 2020 alone (Insurance Information Institute, 2021). With close to 80 percent of senior IT security leaders expressing concerns about protection against cyberattacks, it is crucial for individuals across all levels of the workforce to be aware and be prepared to handle cases of attacks against CPS (Brooks, 2021).

An approach to awareness and preparedness for CPS security can be adapted from cybersecurity training. The development of the National Initiative for Cybersecurity Education framework demonstrates a strong example of entities like the government, academia, and industrial organizations working together to bolster security training of the workforce (Newhouse et al., 2017). Among the work roles in the training framework are those focused on the development of training materials based on instructional needs. In their study on instructional method preferences for security education, researchers found that most participants preferred video-based materials for learning (Abawajy, 2012). The use of video materials for software training was also found to increase the learning motivation of individuals, proficiency, and retention of skills (van der Meij and van der Meij, 2013).

## METHODS

The scope of development for this study was restricted to developing a mixed-materials guide for CPS instructional resources. A mixed-materials guide involves a video and supplementary information documents to provide viewers with guidance in an accessible manner. While the guidance provided in this study is intended for security professionals, there are also foreseeable benefits to employers and first responders. The development of educational videos could be used to consolidate in-depth training materials into understandable and segmented videos highlighting core training competencies (CTC). Additionally, it could be utilized to develop more in-depth education about CTC directed toward specific personnel, or to develop a refresher course of CTC as needed. In general, CTC are the skills, attributes, information, or behaviors needed to accomplish a specific task or job. Further applications for educational videos would be as just-in-time training tailored to address a particular emergency or attack situation.

The methodology followed for video development was structured from literature focused on effective security

education and training. Based on evidence from research about the most effective learning techniques among professionals in the workplace, the scope of the audience, and the time frame of the development of resources, two complementary components were identified as the foundation of the instructional materials. An instructional video and a supplementary information document would provide similar, if not more in-depth, details as the video (Le et al., 2018). Narrator scripts for a video were developed based on CTC and how much content could be delivered in two to three minutes (He et al., 2019). The narrator scripts also serve as subtitle documents to make the video content more accessible. In conjunction with the narrative script development, a supplementary information document would be developed to summarize the content, provide additional information, and give instruction for the viewer to access the full training content when applicable. The guidelines for video development comprise the actual content and formatting considerations. The content guidance is adapted from a comprehensive article that provides an in-depth procedure for different types of CPS attacks based on response efforts, recovery phases, and available resources (Ayala, 2016).

As a part of the developed framework for creating effective CPS security training videos, deliverables were created to serve as a sample presentation and to double as training material to accompany this study. Final deliverables consist of a video addressing content material, a video addressing formatting considerations, video transcripts, and a supplementary information document. The guidelines for content and formatting considerations were developed to be generic so that the deliverables could be used to develop training for different types of CPS attacks or just-in-time training.

## RESULTS

The proper procedures to be followed when responding to a CPS attack were developed as content components that would need to be addressed in the video (Ayala, 2016). The steps are outlined as follows as key attributes of the content.

1. *Introduction.* Introduce the specific threat to CPS security. Present a brief overview of what attack they are discussing, how it is launched, and the consequences that can arise as a result of a successful attack or an emergency event.
2. *Overview of response plan.* Present an overview of the response plan that will be implemented to address the specific threat. The response plan can be developed based on existing guidelines, or steps can be added based on further

considerations and solutions to specific aspects of a problem.

3. *Identify resources needed for response components.* Identify the resources needed to achieve the steps directed in the response plan. Developers list the resources or personnel needed to defend or mitigate against the specific type of CPS threat that is being discussed.
4. *Detection, mitigation, and recovery discussion.* Outline the specific strategies and processes that will be followed based on the previously identified available resources. The strategy should incorporate elements of detection, mitigation, and recovery in order to provide a comprehensive overview of procedures that address the threat from start to finish.
5. *Strategies for response and application processes of available resources.* Discuss the specific steps that viewers can take given what is available to them, within their capabilities, and feasible to accomplish in a timely manner.
6. *Conclusion.* Provide a summary of all points discussed toward the end of the video, and end the video with the appropriate credits for production and external resources used.

A study in the journal *Technical Communications* provided eight guidelines catering to design specifications and requirements for software training (van der Meij and van der Meij, 2013). For the scope of this study, six guidelines were developed with an additional optional guideline to incorporate depending on individual design choices. The steps are outlined below as key attributes of video production and design considerations

1. *Keep videos short.* Shorter videos are more effective for learning and retention, with the most effective videos falling between two and three minutes in length. If developers cannot shorten the video to this length, reduce content or split it into multiple videos.
2. *Present content in a clear and concise manner.* Developers should refrain from using large blocks of texts in their videos, instead opting for short sentences or simple phrases to support the narration. Text should include only vital information, such as CTC, and all other essential information for background and application should rely on spoken narration. Utilize text fonts that are easy to read and chose a large text size.
3. *Rely on visual material.* Adding visuals such as graphics and video demonstrations will enrich the quality of the video. Highly rated videos rely on visuals; therefore, it is strongly recommended for the narration to begin just before the visual demonstration or graphic is presented, rather than a visual being presented late or never. Additionally, introducing vital information by demonstrating the application, in context, helps develop concreteness of the material for viewers and aids with comprehension. One way this can be achieved is by adding B-roll or background footage, demonstrating the concept being carried out in the specific setting, or a comparable one, where it would take place.
4. *Use consistent formatting standards.* This is dependent on who the video is being developed for, but developers should be mindful of design and formatting choices. The same types of information (such as titles, body text, and tables) should be presented in the same manner and in the same position on screen. This allows the viewer to develop a schema of how information is presented, enhancing viewer engagement. Developers should use the provided or professional templates, if accessible, that do not distract the viewer from the content.
5. *Use a real person and a fitting pace for narration.* Narration should be used instead of onscreen text to inform viewers of the story (such as the background or purpose) of what they are visually seeing. Using people to narrate content (as opposed to automated narration) can help viewers retain information. Additionally, how the content is delivered matters. Refrain from giving instructions too quickly, and instead speak at a slightly faster rate, or a conversational tempo, and extend natural breaks in speaking by adding a two- to five- second pause while the viewer is processing key information and between segments of information. The video narrator should also be attentive to incorporating voice inflection throughout the video.
6. *Pace the content and make it cohesive.* Developers should refrain from providing too much information in a single video, even if the video meets the recommended running time. Developers should instead make sure the content of the video has a single, achievable process. If the training has multiple steps that each have multiple subsequent steps, consider making multiple videos for each step of the process to keep the viewer from being overwhelmed. Additionally, the video should follow the natural order the viewer would carry out the process to help with comprehension of information. A generic order of a



process being carried out would be as follows: viewer action → software/physical response of system → viewer action → software/physical response of system → viewer action, etc. It is recommended that training videos have no more than three to five action steps to be completed to aid in retention and not overwhelm the viewer. The use of transitions is highly recommended as they can provide cohesion between the various aspects being presented.

7. (Optional) Add background music. Music can bolster emotions and help viewers recall portions of content. This is an optional step in the guidelines due to the nature of the videos being presented. Developers should be mindful of the type of music being used and the source.

## CONCLUSION

The emphasis on CPS security has been increasing with the uptick in attacks on critical infrastructure. To promote awareness of the issue among individuals, especially those in the cybersecurity workforce, the development of education and training materials has become paramount to ensuring security and distributing responsibilities across all people in an organization. To that end, this study discusses the development of training materials that would be used in an array of career fields to learn more about contemporary issues in CPS security, and to teach workforce and security personnel how to create simple but comprehensive training for preparation and response to these issues.

There are some limitations that need to be addressed with this study. Future work could involve quantitative evaluations of learning by utilizing pretests and posttests. Also, based on developed criteria and qualitative testing techniques, the effectiveness of materials can be tested based on the quality of works produced using these guidelines. A limitation worth noting is that the final deliverables only account for major considerations with respect to developing training videos and do not reflect all characteristics of training to the full content. Nonetheless, a combined audio and visual delivery has been proven to be effective for retention of knowledge (He et al., 2019). Additionally, the use of combined instructional materials is most effective for cognitive learning and retention (Cherrett et al., 2009).

It should be noted that the guidance provided in this study has been applied in a project with a graduate-level homeland security/agrisecurity class, Foundations of Homeland Security.

Based on the application and the project, a brief reflection summary was developed. The overall production

of educational videos was found to be relatively simple in that it does not take a video production professional or extensive manpower to develop quality training videos. Additionally, it was found that quality production can be achieved with little to no cost and little time commitment. Developers in the class were partnered in groups of two or three and were able to use their own phones and laptops in conjunction with a free online video editing software to create quality training videos in less than a day's time. Another cost-effective route that could be pursued is purchasing video equipment. Equipment such as lapel microphones, a GoPro or other professional camera, a gimbal or tripod, and a light panel can be purchased for about \$600 or less. It was found that the use of video equipment in conjunction with video editing software can be used to create more professional-looking instructional videos. Finally, it was found that projects developed with demonstration or background videos to accompany the video dialogue were more engaging to viewers than projects that heavily relied on presentation slides with images and text to accompany the video dialogue.

With the growing emphasis on CPS education, particularly with respect to ensuring the security of all types of systems, this study provides a general approach to discussing threats and responses to security in a manner that is accessible and comprehensible to entry-level employees and professionals of the security field and beyond. Adapting this study into projects can further highlight avenues for improvement pertaining to the development of the instructions themselves. Moving from the reliance on traditional, text-based content delivery strategies to audiovisual materials can help viewers to develop and retain the procedural knowledge required to ensure CPS security.

## REFERENCES

- Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237–248. doi:10.1080/0144929x.2012.708787
- Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, 100, 212–223. doi:10.1016/j.compind.2018.04.017
- Al-Mhiqani, M. N., Ahmad, R., Yassin, W., et al. (2018). Cyber-security incidents: A review cases in cyber-physical systems. *International Journal of Advanced Computer Science and Applications*, 9(1), 499–508.
- Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68, 81–97. doi:10.1016/j.cose.2017.04.005
- Ayala, L. (2016). Cyber-physical attack recovery procedures. In *Cyber-Physical Attack Recovery Procedures* (pp. 1–14). Springer. doi:10.1007/978-1-4842-2065-8\_1.

- Brooks, C. (2021). Alarming cybersecurity stats: What you need to know for 2021. *Forbes*. <https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-what-you-need-to-know-for-2021/>
- Cherrett, T., Wills, G., Price, J., Maynard, S. & Dror, I. E. (2009). Making training more cognitively effective: Making videos interactive. *British Journal of Educational Technology*, 40(6), 1124–1134. doi:10.1111/j.1467-8535.2009.00985.x
- Coble, S. (2020, May 18). Texas takes second ransomware hit. *Infosecurity Magazine*. <https://www.infosecurity-magazine.com/news/texas-takes-second-ransomware-hit/>
- Cyber-Physical Systems Public Working Group. (2017). Framework for cyber-physical systems: Volume 1, overview. Smart Grid and Cyber-Physical Systems Program Office, Engineering Laboratory, US Department of Commerce. <https://doi.org/10.6028/NIST.SP.1500-201>
- Department of Homeland Security. (2023). *Cyber-physical systems security*. US Department of Homeland Security. <https://www.dhs.gov/science-and-technology/cpssec>
- He, W., Ash, I., Anwar, M., Li, L., Yuan, X., L. Xu, & X. Tian. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training, *Journal of Intellectual Capital*, 21(2), 203–213. doi:10.1108/jic-05-2019-0112
- Insurance Information Institute. (2021), *Facts + statistics: Identity theft and cybercrime*. <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>
- Khaitan, S. K., & McCalley, J. D. (2015). Design techniques and applications of cyberphysical systems: A survey. *IEEE Systems Journal*, 9(2), 350–365. doi:10.1109/jsyst.2014.2322503
- Le, H.-T., Johri, A., & Malik, A. (2018). Situated information seeking for learning: A case study of engineering workplace cognition among cybersecurity professionals. In *Proceedings of the ASEE Annual Conference & Exposition Proceedings*. doi:10.18260/1-2—30966
- Li, J., Liu, Y., Chen, T., Xiao, Z., Li, Z. & Wang, J. (2020). Adversarial attacks and defenses on cyber-physical systems: A survey. *IEEE Internet of Things Journal*, 7(6), 5103–5115. doi:10.1109/jiot.2020.2975654
- Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce framework*. National Institute of Standards and Technology. doi:10.6028/nist.sp.800-181r1
- Peters, G. (2021). *Peters and Johnson introduce bipartisan bill to help secure federal information technology supply chains against threats*. <https://www.peters.senate.gov/newsroom/press-releases/peters-and-johnson-introduce-bipartisan-bill-to-help-secure-federal-information-technology-supply-chains-against-threats>
- Resolver. (2021). *Physical & cybersecurity defense: Hybrid attacks*. <https://www.resolver.com/blog/physical-and-cyber-security-defense-hybrid-attacks/>
- Ropek, L. (2020). *Cyberattack disrupts Texas Department of Transportation*. Government Technology. <https://www.govtech.com/security/cyberattack-disrupts-texas-department-of-transportation.html>
- Shi, J., Wan, J., Yan, H., & Suo, H. (2011). A survey of cyber-physical systems. In *Proceedings of the International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–6. doi:10.1109/wcsp.2011.6096958
- Turton, W., and Mehrotra, K. (2021). *Hackers breached Colonial Pipeline using compromised password*. <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>
- van der Meij, H., and van der Meij, J. (2013). Eight guidelines for the design of instructional videos for software training. *Technical Communication*, 60(3), 205–228.
- Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., and Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends, *Microprocessors and Microsystems*, 77. doi:10.1016/j.micpro.2020.103201

## Appendix A: Outline for CPS Instructional Resources

Below is an example of these guidelines summarized as instructions for the project conducted in the Foundations of Homeland Security course.

### **Cyber-Physical Security Instructional Project**

The main aims of the CPS security video development project are (1) to gain transferrable skills in video editing, (2) to develop research abilities about contemporary CPS security issues, and (3) to create effective training materials based on acquired knowledge.

#### *Key Deliverables*

1. CPS Security Video
2. Video Transcript
3. Supplementary Information Document (Fact Sheet)

### *Deliverable 1: CPS Security Video*

#### Instructions for Content:

- The first part of your video should introduce the specific issue or threat to CPS security. Provide a definition of the problem, how it can affect CPS, and the consequences of the attack or emergency (physical, financial, damages to reputation, or otherwise).
- The next part of your video should discuss the specific action(s) that should be taken to combat the issue. To achieve the action(s), you must present the response plan or procedure.
  - For example: If your identified CPS threat is insider threat, after identifying and discussing insider threat, the next section of your video will present an overview of the plan that needs to be implemented to combat insider threats
- Next, provide an overview of the different components that will be a part of the response plan. These include “identifying the necessary resources” and “developing the response strategy”. You can present these components in bulleted points or in a graphical format.
- The next part of your video should discuss the resources that are necessary for incident response. Resources can be any asset that is required to maintain the operations of a business. Based on your developed response plan, list out the personnel, devices, safeguards, and other types of resources that would be needed to respond to the threat.
- The next part of your video should discuss the steps that would be taken as a part of the response strategy. There are three steps to discuss here – detection, mitigation and recovery. Present a brief overview of different techniques that can be used for each of the three steps.
- The final part of your video will consist of the conclusion and ending credits. The conclusion must have a short summary of the video content. This can also be presented graphically. The end of the video should provide credits for all externally sourced images and graphics, references for information, and production credits.

#### Instructions for Formatting:

- Keep your video short; it must be no longer than 3-4 minutes. If you have a video over this duration, consider trimming content or splitting your video into multiple videos.
- Present all the content in a clear and concise manner. Refrain from adding large paragraphs of text; use short phrases or sentences instead.
- You must use visuals in your presentation. You can choose graphics, images or demonstrations to explain key concepts. It is highly recommended to use demonstrations for explanations about how to execute certain actions.
- Make sure that your formatting is consistent throughout the presentation. For the purposes of this assignment, you can use templates provided from Purdue or follow the Purdue color-scheme when making design choices. The use of transitions throughout the presentation is highly encouraged but be mindful of design choices as to not distract from the content.
- If you are developing only one video, designate one individual from the project group as the narrator of the video. If you have multiple videos, assign one individual to each video for narration. Be mindful of delivery, pace, and voice modulation when recording audio.
- (Optional) You can use the music as long as it does not distract from the content being presented in the video.

### *Deliverable 2: Video Transcript*

For accessibility purposes, please provide a transcript of all narration in the video. The format for writing out narration dialogues is as follows:

[SECTION TITLE/SLIDE TITLE] Transcript content

### *Deliverable 3: Supplementary Information Document*

Provide a supplementary information document that goes along with the video(s) to provide more details about response plans that were not discussed in the video(s). Depending on the extent of content presented in the video(s), you might not be able to provide detailed overviews of all the different steps that can be taken in response to a CPS threat or issue. This supplementary information document should follow the same format and reflect the content of the instructional video, but it should also contain additional information as needed.

# Evacuation Situational Manual Guidance for Long-Term Care Facilities

**Rylee Lane**

Purdue Homeland Security Institute, Dept. of Computer and Information Technology  
Purdue University  
lane85@purdue.edu

**Brock Warner**

Cengage Group  
Infosec Institute  
brock.warner@pm.me

**Dylan John**

Federal Bureau of Investigation

**William Field, PhD**

Department of Agricultural and Biological Engineering  
Purdue University

**Abstract** Facilities that care for populations that require personal assistance for each of their patrons in a disaster event are immediately at a disadvantage in being able to have a quick, effective disaster response (Aaby, 2005, pp. 1–8). These environments range from nursing homes with elderly populations to other medical care facilities with a wide range of disabled patrons and patrons with other special needs. For simplicity, “long-term care” (LTC) encompasses these types of vulnerable environments. This study is structured as a situational manual (SITMAN) using FEMA’s National Incident Management System guidelines for LTC facilities. The purpose of the study is to provide LTC staff with tabletop exercises to evaluate their emergency plans and procedures. The study design was further structured by a case study of a rural medical facility called Milner Community to emphasize the increasing challenges in disaster response for LTC facilities in rural environments. The four tabletop exercises are set up for chemical exposure, fire evacuation, active shooter, and shelter-in-place events. This study could benefit the US military, which evacuates thousands of service members and allies in disaster events each year, in further understanding the evacuation considerations of LTC facilities. Future work would include evaluation of the developed exercises and could also include the development of exercises with specified applications for US military personnel and LTC populations abroad.

## INTRODUCTION

LTC facilities must incorporate and expand their knowledge of emergency management methodologies that are in line with their external partners, with whom they may be required to work in conjunction during an emergency event. To strengthen emergency preparedness, similar to the overall mission of homeland security, LTC facilities must develop their capabilities to prevent, protect, respond, and recover (FEMA, 2023b).

LTC facilities, just like any other medical facility, are subject to emergency events that can bring harm to the facilities’ residents and infrastructure. The specific LTC facility that this SITMAN is designed for is Milner

Community Health Care, Inc., in Rossville, Indiana. The four SITMAN tabletop exercises focus on chemical exposures, fire evacuations, active shooters, and shelter-in-place. These exercises serve as tangible evidence of a commitment to ensure the safety of LTC facilities, staff, and visitors through education and the development of collaborative partnerships that will help them to respond to natural or manmade emergencies. The purpose of this SITMAN is to provide participants guidance to evaluate their facility’s current capabilities in response to emergencies. These exercises focus on the implementation and coordination of the current internal emergency management plans, policies, and risk communication and on the importance of integration

**Table 1.** Exercise objectives and associated core capabilities

Objective	Core capability
Assess participants' knowledge, skills, and abilities to effectively support all-hazards emergency response	Planning Public information and warning
Allow participating locations to share real-time related preparation, response, and recovery solutions with all participants	Operational coordination
Enable participants to better coordinate response operations with counterparts at federal, state, and local levels	Public health Healthcare and emergency management services

within the community regarding emergency management (FEMA, 2023b).

The focus of homeland security has been steered toward a capabilities-based approach by the National Planning Scenarios and the establishment of the National Preparedness Priorities (FEMA, 2023a). Capabilities-based planning focuses on planning under uncertainty because the next disaster or threat can never be predicted with complete certainty. Capabilities-based planning takes an all-hazards approach to preparation and planning that builds skills that can be applied to a wide variety of incidents (FEMA, 2023a). The core capabilities listed in Table 1 have been selected because they provide the foundation for the SITMAN design objectives and scenario. The goal is to measure and validate the performance of these capabilities and their associated critical tasks for LTC facilities. The exercise objectives in Table 1 describe the expected outcomes for the four modules in this SITMAN and are linked to corresponding core capabilities.

These exercises are structured to be group discussion based and mediator facilitated. The participants will include players, observers, and facilitators. Players respond to the presented situation, based on expert knowledge of response procedures, current plans and procedures, and insights derived from training. Observers support the group in developing responses to the situation during the discussion; they are not participants in the moderated discussion period. Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Players will participate in the following four modules:

- Module 1: Chemical exposure
- Module 2: Fire evacuation
- Module 3: Active shooter
- Module 4: Shelter-in-place

**Table 2.** Exercise guideline and assumptions

Guidelines	Assumptions
No-fault, low-stress, open environment	The scenario is plausible, and events occur as they are presented
Respect the opinions, perspectives, and observations of others	There is no "hidden agenda," nor any trick questions
Treat the scenario incidents as real	All players receive information at the same time
Respond based only on your knowledge of current plans and capabilities and insights derived from training	When possible, discussions and decision-making should be informed by active plans, policies, and procedures
Problem-solving efforts should be the focus, not issue identification	If necessary, discussions and decision-making can be hypothetical and based on group consensus
Keep time constraints in mind and comments focused	

Each module begins with a situation explanation that summarizes key events occurring within a time period. After the initial explanation, participants will review the situation and engage in functional group discussions of appropriate response issues. The functional groups are facility administration, nursing management, and support management. After these group discussions, the participants may be updated on the situation with additional information and engage in additional functional group discussions. After the functional group discussions, participants will engage in a caucus-style discussion in which a representative from each group presents a synopsis of the group's actions based on the scenario. The exercise guidelines and assumptions for conducting a module are listed in Table 2 (FEMA, 2023b).

When engaging in the discussion, participants should focus on identifying any additional requirements, decisions, critical issues, or questions that should be addressed at this time (Montgomery & Connorton, 2015). The questions provided with the modules are suggested subjects participants may wish to address as the discussion progresses, but they are not a definitive list of concerns.

## MODULE 1: CHEMICAL EXPOSURE

Objectives:

- Evaluate current procedures and policies in LTC facility.

- Evaluate communication methods within LTC.
- Evaluate initial response process.
- Identify how to effectively communicate information to affected groups.
- Determine deficiencies regarding resources and when to request additional resources.

Milner Community is located near crop fields that are behind and next to the facility. These fields are sprayed with pesticides and herbicides, which put patrons at risk of exposure to toxic substances. Routes of exposure are inhalation, ingestion, and eye or skin contact (Carson, 2015, p. 23). When exposure occurs, the toxic substances can penetrate the internal organs and bloodstream and can cause systemic effects (Department of Labor, n.d.). The liver, kidneys, heart, reproductive system, and nervous system are the organs that are usually affected by systemic effects (Department of Labor, n.d.). For this exercise, the chemical that people in Milner have risk of exposure to is sodium arsenite. Sodium arsenite is used to kill weeds (Carson, 2015, p. 47). When inhaled, it will cause cough, labored breathing, and headaches. If exposure occurs via skin or eyes, the person will experience pain and redness. If ingested it will cause burning in the throat and chest, vomiting, and potentially shock or collapse (NIOSH, 2015). Long-term exposure leads to cancer and infertility (Carson, 2015, p. 47).

At approximately 9:00 a.m., a farmer hits and damages a 5,000-gallon container of sodium arsenite. The chemical container was weak due to age and was easily punctured by the farmer's equipment. Sodium arsenite begins to leak from the container. The farmer does not immediately notify the fire department, believing they can repair the tank before losing all the chemical. At 9:30 a.m. the farmer realizes that they are not able to contain the spill and notifies the fire department. The fire department then notifies the LTC so that they can begin to take necessary measures. Firefighters are unable to determine the exact amount of chemical that was leaked and are worried that it may be picked up by either wind or water. The nearest available hazmat team is called to the scene. At 10:00 a.m. the fire department notifies the LTC that a hazmat team has been called to the scene and it may be in the best interest of the facility to evacuate.

Based on the provided information, participate in the discussion concerning key issues raised in Module 1.

1. What preparations have been made to prepare for chemical exposure?
2. Would any ICS be activated at this point? If so, what would the process be to activate it?
3. What agencies would respond to this event? How long would it take for these agencies to respond?

4. How would you handle requests for information from individuals' family members?
5. What resources would you need to evacuate the facility?
6. What safety concerns are there for staff and residents?
7. Would any internal policies or procedures be activated?
8. Would you take any other action at this point?

At 10:20 a.m. the staff and residents begin to evacuate the LTC facility. Local hospitals and other facilities with existing agreements in your facilities emergency plan have begun to accept members of your facility. The toxic cloud is spreading, and locals are requesting information.

Based on the provided information, participate in further discussion concerning key issues raised in Module 1.

1. Would the ICS be changed in any way because of the new information?
2. How would the public be notified about the incident?
3. What additional resources are needed to complete the evacuation?
4. Would any other internal procedures or policies be activated?
5. Would you take any other action at this point?

## MODULE 2: FIRE EVACUATION

Objectives:

- Evaluate current procedures and policies in LTC facility.
- Evaluate communication methods within LTC.
- Evaluate initial response process.
- Identify how to effectively communicate information to affected groups.
- Determine deficiencies regarding resources and when to request additional resources.

Milner Community is home to an elderly population. The special needs of the elderly make it complicated to evacuate so many with a limited staff. According to the United States Fire Administration, 2,700 nursing homes had facility fires between 2012 and 2014 (NFIRS, 2016). These fires largely took place in the morning, between 8:00 and 9:00 a.m. The next most common time is between 4:00 and 6:00 p.m. (NFIRS, 2016). In nursing homes, fires that happen in a confined area are much less dangerous than those that occur in nonconfined area (NFIRS, 2016). The three leading causes of fires in confined areas in nursing homes are cooking, appliances, and heating. The three

leading causes of fires in nonconfined areas are appliances, electrical malfunction, and heating (NFIRS, 2016).

At 9:00 a.m., temperatures are hovering around 62°F and the entire staff is happy to enjoy a break from a long Indiana winter. The morning shift of employees has recently arrived at the LTC facility and is beginning their day. At 9:05 a.m. a nurse detects the smell of smoke in the east side of the facility. The nurse asks one of her coworkers if they too smell the smoke. The coworker agrees, and inside one of the main electrical rooms, a fire grows. At 9:06 a.m. the automated fire alarm system is activated, and the local fire department has been notified. The smell of smoke spreads and a haze of smoke covers the first floor. Electrical power has been lost throughout the LTC facility. At 9:07 a.m. fire department units and local law enforcement have arrived and established a command post in the parking lot outside the LTC facility. Firefighters enter the building with their equipment. None of the staff or residents have seen a fire, but the smoke has caused some residents to feel stressed.

Based on the provided information, participate in the discussion concerning key issues raised in Module 2.

1. Who is in charge until the fire department and local law enforcement arrive?
2. Based on your current emergency management plan, what actions are a priority at this time?
3. Are there any safety concerns for residents?
4. Would any ICS be activated at this point? If so, what would the process be to activate it?
5. Who needs to be informed about the incident? How would this be done?

At 9:20 a.m. the fire department locates the fire and extinguishes it. All of the LTC facility is filled with smoke and without power. The incident commander (IC) is debating about evacuating or sheltering in place. The fire department chief is advising that residents be evacuated due to the smoke condition and lack of electrical utilities. The IC has made the request to evacuate the LTC facility. At 9:30 a.m. some residents have moderate to severe smoke inhalation along with existing health issues. It is critical that all residents and staff be evacuated in a timely manner.

Based on the provided information, participate in further discussion concerning key issues raised in Module 2.

1. Who oversees requesting an evacuation/shelter-in-place in the facility? Is this a group decision or an individual decision? Who will direct the evacuation?
2. Does your current emergency management plan sufficiently address evacuation procedures? Have

the staff exercised and trained in these evacuation procedures?

3. Would you notify family members of residents of the plan to evacuate? What information would you provide?
4. Does your emergency management plan contain updated transfer agreements for other facilities?
5. Would you take any other action at this point?

### MODULE 3: ACTIVE SHOOTER

#### Objectives

- Evaluate current procedures and policies in LTC facility.
- Evaluate communication methods within LTC.
- Evaluate initial response process.
- Identify how to effectively communicate information to affected groups.
- Determine deficiencies regarding resources and when to request additional resources.

Milner Community is home to elderly patients who require various medications daily. The facility has an automated machine that dispenses these medications based on patient information within its database. The presence of medications could be the target of armed individuals, whose presence has the potential to lead to an active shooter situation. Now is the best time to be prepared for an active shooter due to the opioid crisis in the United States. Indiana ranks second in the United States for armed pharmacy robberies (Fagerman, 2017).

At 2:00 p.m., an armed individual enters the front of the building and opens fire. Several residents are shot in the first few seconds of the incident. Employees who were present begin to scatter as residents panic. The armed individual continues through the lobby, shooting those who were not able to flee. At 2:05 p.m. residents and employees begin to call 911 to report an active shooter in the building. Patrol units are several minutes away; however, EMS and a local fire department are being advised and dispatched. Shots can be heard and the assailant continues down a hallway. Employees begin an effort to evacuate the opposite wing of the building. Police units arrive and begin addressing the situation. Police units call for additional officers and EMS/Fire is directed to begin triage at the opposite end of the building. At 2:10 p.m. police officers have neutralized the suspect and confirm he is no longer a threat. Officers begin to report that many victims need immediate medical attention. Television and radio stations have begun to report that there was a shooting. As reports spread, the

staff are inundated with calls from family members asking for status reports. Further family members also begin to arrive on the scene.

Based on the provided information, participate in the discussion concerning key issues raised in Module 3.

1. What measures have been taken to prepare for an active shooter?
2. Would any ICS be activated at this point? If so, what would the process be to activate it?
3. What security improvements could be put in place?
4. How would you handle requests for information from individuals' family members?
5. Would any internal policies or procedures be activated?
6. Would you take any other action at this point?

#### **MODULE 4: SHELTER-IN-PLACE**

Objectives:

- Evaluate current procedures and policies in LTC facility.
- Evaluate communication methods within LTC.
- Evaluate initial response process.
- Identify how to effectively communicate information to affected groups.
- Determine deficiencies regarding resources and when to request additional resources.

The weather in Indiana is constantly changing, often with dramatic temperatures swings. This results in perfect tornado weather. The peak tornado months are April, May, and June (National Weather Service, 2022). Indiana averaged around twenty-five tornadoes a year between 2010 and 2015 (National Weather Service, 2022). Strong winds that come from tornadoes are what cause damage and create danger ("Tornado FAQ," n.d.). If wind speeds are high enough, they will break windows, tear off building roofs, turn structures to piles of rubble, and pick up cars. This causes a major threat to buildings and people may be hit by debris thrown by winds ("Tornado FAQ," n.d.).

At 5:00 p.m. Indiana news channels have been advising that severe storms are heading through the region. Heavy rains are falling, and high winds are causing damage to powerlines. Tornado warnings are issued until 8:30 p.m., but none have been reported. Many employees have gotten off from their shift and have decided to wait for the storm to pass because of the severity and influx of traffic in the area from a festival the previous day. The LTC facility has full power and is monitoring the news via radio and TV.

At 5:45 p.m. emergency weather reports a tornado has touched down 12 miles west of the LTC facility, with another having touched down 2 miles north of the first. Both are moving east at 5 miles per hour. Residents are moved into the hallways by staff, away from the threat of shattering glass. At 6:30 p.m. airborne debris hits the west side of the LTC facility, shattering windows. The electricity goes out throughout the LTC facility and returns only to the east side of the LTC facility. Emergency power is switched on, but flashlights are necessary for some areas of the facility. At 7:10 p.m. an assessment of the LTC facility has been made now that the storm has passed. Windows on the west side of the facility are not intact. The emergency generator has a physical defect that is causing lack of power in some areas of the LTC facility. A replacement part or generator could take up to 36 hours to arrive, with an optimistic delivery time of 24 hours. The residents' family members are calling and requesting more information about the damage and the state of their loved ones.

Based on the provided information, participate in the discussion concerning key issues raised in Module 4.

1. Would the LTC facility consider sheltering in place? Who would make this decision?
2. Would any ICS be activated at this point? If so, what would the process be to activate it?
3. What notifications would you make? Would you make any external announcements?
4. Would you request additional resources? What would you request and from whom?
5. How would you handle the requests for additional information from residents' family members?
6. Would any other internal procedures or policies be activated?
7. Would you take any other action at this point?

At 8:30 p.m. the IC has decided to evacuate residents in the assisted living section because their rooms are the most damaged and it will take anywhere between 24 and 36 hours for the replacement generator/part to arrive and power to be restored. A request for support for the partial evacuation has been sent. At 9:00 p.m. the LTC facility IC hears back regarding support for the partial evacuation. The IC has been informed through the local emergency management agency that transportation will be unavailable for the evacuation due to damaged roads and recommends the LTC facility continue to shelter in place until resources become available.

Based on the provided information, participate in further discussion concerning key issues raised in Module 4.

1. Would the ICS be changed in any way because of the new information?



2. Would there be any security issues at this point?
3. What activities would need to occur for a full shelter-in-place?
4. Would you continue to prepare for an eventual evacuation? If so, what actions would you take?
5. Would any other internal procedures or policies be activated?
6. Would you take any other action at this point?

## CONCLUSION

The implementation of the emergency management plan of a facility and the true validation of the plan through the exercise and improvement planning process will only strengthen LTC facilities capabilities. These exercises stress the importance of including LTC facilities in the emergency management process by ensuring that current emergency management plans are practiced, evaluated, and validated. Future research would involve assessing the effectiveness of the created tabletop exercises through application.

## REFERENCES

- Aaby, K. (2005). *Emergency preparedness checklist for nursing homes, assisted living facilities, and group homes*. Montgomery County Advanced Practice Center for Public Health Emergency Preparedness and Response.
- Carson, R. (2015). *Silent spring*. Penguin Classics.
- Department of Labor and Industries (n.d.). *Understanding toxic substances: An introduction to chemical hazards in the workplace*. Purdue University. [www.purdue.edu/research/docs/pdf/Introduction to Chemical Hazards in the Workplace.pdf](http://www.purdue.edu/research/docs/pdf/Introduction%20to%20Chemical%20Hazards%20in%20the%20Workplace.pdf)
- Fagerman, K. (2017, April 21). Recent pharmacy robbery statistics. *Pharmacy Times*. [www.pharmacytimes.com/news/recent-pharmacy-robbery-statistics](http://www.pharmacytimes.com/news/recent-pharmacy-robbery-statistics)
- FEMA. (2023a). *National preparedness goal*. US Department of Homeland Security. [https://www.fema.gov/emergency-managers/national-preparedness/goal#:~:text=The %20National%20Preparedness%20Goal%20describes ,greatest%20risks%20to%20the%20nation](https://www.fema.gov/emergency-managers/national-preparedness/goal#:~:text=The%20National%20Preparedness%20Goal%20describes,greatest%20risks%20to%20the%20nation)
- FEMA. (2023b). *Exercise and preparedness tools*. US Department of Homeland Security. <https://www.fema.gov/emergency-managers/national-preparedness/exercises/tools>
- Health Care Association of New Jersey. (2010). *Ready – Set – GetOut tabletop exercise*. Homeland Security Exercise and Evaluation Program.
- Montgomery, J., & Connorton P. (2015). *Shelter in place: Planning resource guide for nursing homes*. AHCA/NCAL Emergency Preparedness Committee.
- National Weather Service. (2022). *Central Indiana tornado statistics*. [www.weather.gov/ind/tornadostats](http://www.weather.gov/ind/tornadostats)
- NFIRS. (2016). *Data snapshot: Nursing home fires*. FEMA. [www.usfa.fema.gov/statistics/reports/where-fires-occur/snapshot-nursing-home.html](http://www.usfa.fema.gov/statistics/reports/where-fires-occur/snapshot-nursing-home.html)
- NIOSH. (2015). *Sodium arsenite—international chemical safety cards*. Centers for Disease Control and Prevention. <http://med.iab.me/modules/en-cdc/www.cdc.gov/niosh/ipcsneng/neng1603.html>
- Tornado FAQ. (n.d.). NOAA National Severe Storms Laboratory. [www.nssl.noaa.gov/education/svrwx101/tornadoes/faq/](http://www.nssl.noaa.gov/education/svrwx101/tornadoes/faq/)

**Appendix A: Participant Feedback Form**

Please enter your responses in the form field or check-box after the appropriate selection.

**Participant Name:**

**Title:**

**Role (please place a checkmark in one of the boxes below):**

Player

Observer

Facilitator

Evaluator

**Part 1 - Recommendations and Action Steps**

Based on discussions today and the tasks identified, list the top 3 issues and/or areas that need improvement.

---

---

---

Identify the action steps that should be taken to address the issues identified above. For each action step, indicate if it is a high, medium, or low priority.

---

---

---

Describe the action steps that should be taken in your area of responsibility. Who should be assigned responsibility for each item?

---

---

---

List the policies, plans, and procedures that should be reviewed, revised, or developed. Indicate the priority level for each.

---

---

---

Is there anything you saw in the exercise that the evaluator(s) might not have been able to experience, observe and/or record?

---

---

---

## Part 2: Exercise Design and Conduct

What is your assessment of today's exercise?

Please rate, on a scale of 1 to 5, the assessment factors listed below, with 1 indicating strong disagreement with the statement and 5 indicating strong agreement.

Assessment Factor	Rating of Satisfaction with Exercise				
	Strongly Disagree				Strongly Agree
The exercise was well structured and organized.	1	2	3	4	5
The exercise scenario was plausible and realistic.	1	2	3	4	5
The Situation Manual was useful.	1	2	3	4	5
Participation in the exercise was appropriate for someone in my position.	1	2	3	4	5
The participants included the right people at the right level and a mix of disciplines.	1	2	3	4	5

What changes would you make to improve this exercise?

---

---

---

What additional training or experience would you like to have?

---

---

---

*Participant feedback form adapted from Health Care Association of New Jersey (2010).*

# Performance Analysis of HiFive Unmatched RISC-V Processor Versus x86 Processor Running Microsoft SEAL Homomorphic Encryption Library

Zachary Legg, James Dean, and Leleia Hsia

Air Force Institute of Technology, Department of Electrical and Computer Engineering  
Zachary.Legg.1@us.af.mil

**Abstract** Fully homomorphic encryption (FHE) is an encryption technique that allows an arbitrary amount of computations to be done on encrypted data without needing to decrypt. Once the computations are complete, the resulting decrypted plaintext is equivalent to the result of computations done on unencrypted data. This technique is a promising option for securing Department of Defense cloud computing and information storage in a zero trust environment. However, the computational load has largely relegated FHE to datacenter-scale computing. Such a scale is not feasible for edge computing devices that require an architecture prioritizing power and thermal efficiency, which the RISC-V architecture lends itself well to. If we are to support moving FHE capabilities to edge computing devices, then we will need to find ways to close the performance gap. To emphasize the present computing gap and provide an experimental baseline for future work, this article presents and compares a performance analysis of the HiFive Unmatched RISC-V processor versus an x86 processor running the Microsoft SEAL Homomorphic Encryption Library.

## INTRODUCTION

With security a major focus across the Department of Defense, new strategies for securing our cyberspace are continuously evolving. One such method is the use of fully homomorphic encryption (FHE) to secure the critical technology needed for advanced computing in areas such as cloud computing and information storage, as required by the Office of the Under Secretary of Defense for Research and Engineering (USD(R&E); <https://www.cto.mil/usdre-strat-vision-critical-tech-areas/>). FHE is a valuable tool as it allows a user to encrypt data and send it to a third-party service provider for storage or processing. After third-party computations are complete, the resulting ciphertext is returned to the user and then decrypted to reveal a value equal to the result of computations done on unencrypted data. This entire process occurs without the third party ever decrypting the data and thus preserves the user's privacy. Despite its benefits, the limitation of a prohibitively large computational load has thus far kept FHE from widespread adoption.

Currently, FHE requires the use of datacenter-scale computers to obtain adequate throughput for most applications. Such a scale cannot be achieved by today's edge computing devices, which prioritize power and thermal efficiency so that they may be used en masse for collecting and processing data closer to the source and, possibly, in very remote locations (such as satellites).

Moving FHE capabilities to edge computing devices will require finding ways to close the performance gap so that these devices can produce results in an acceptable amount of time. One method for achieving FHE speedup is through specialized hardware that exploits data-level parallelism (Su et al., 2020). Hardware acceleration has already shown promising results and can be combined with the RISC-V processor architecture to speed up FHE while maintaining the power and thermal performance innate to RISC-V (Paludo and Sousa, 2022). To emphasize the present computing gap and provide an experimental baseline for future work, this article presents and compares a performance analysis of the HiFive Unmatched RISC-V processor versus an x86 processor running the Microsoft SEAL Homomorphic Encryption Library.

## BACKGROUND

### *Fully Homomorphic Encryption*

While the topic of homomorphic encryption had been researched for decades, the first fully homomorphic scheme was constructed by Craig Gentry in 2009 (Gentry, 2009). Gentry's FHE scheme was a breakthrough as it allowed for multiple types of computations (such as addition and multiplication) to be done an arbitrary number of times on encrypted data. Previously, encryption schemes allowed for only one or two types of computations, as was the case with RSA, which, by the power of a

product rule, allows for multiplication to be done on data encrypted with the same key (Rivest et al., 1978, p. 122). Since Gentry, numerous other FHE schemes have been proposed and have resulted in the four most commonly used schemes: TFHE (Chillotti et al., 2018), BGV (Brakerski et al., 2011), BFV (Fan and Vercauteren, 2012), and CKKS encryption schemes (Cheon et al., 2016).

### **TFHE, BGV, BFV, and CKKS Encryption Schemes**

FHE schemes can generally be classified under one of three computational models and often share characteristics with other schemes of the same model type. The first is the boolean model in which the plaintext is represented as bits. The most common boolean scheme is TFHE, which benefits from fast number comparisons and fast bootstrapping operations (Chillotti et al., 2018). The second is the modular arithmetic model in which the plaintext is represented as integers with a modulus. The most common modular arithmetic schemes are BGV and BFV, which are closely related to each other (Brakerski et al., 2011; Fan and Vercauteren, 2012). Both BGV and BFV have the advantage of increasing performance using single-instruction multiple-data (SIMD) computations over integers, conducting scalar multiplication, and optionally operating as a leveled design where the use of bootstrapping is not required. The third is the floating point arithmetic model in which the plaintext is represented as real or complex numbers. The most common floating point arithmetic scheme is CKKS encryption (Cheon et al., 2016). CKKS benefits from SIMD computations and a leveled design as well as polynomial approximations, deep approximate computations, and fast multiplicative inverses. However, since CKKS produces approximate real numbers, it is not suited for tasks that need exact answers. All schemes discussed here rely on the security of the ring learning with errors problem, which is assumed to be as hard as classic ideal lattice problems. Table 1 shows a summary of these scheme’s characteristics.

These four schemes are implemented in various software libraries such as Microsoft SEAL ([https://github.com](https://github.com/microsoft/SEAL/releases/tag/v4.1.1)

[/microsoft/SEAL/releases/tag/v4.1.1](https://github.com/microsoft/SEAL/releases/tag/v4.1.1)), OpenFHE (<https://github.com/openfheorg/openfhe-development>), and Helib (<https://github.com/homenc/HElib>) that allow developers to experiment with FHE. This paper uses the Microsoft SEAL homomorphic encryption library due to its ease of use and support for BFV, BGV, and CKKS encryption schemes. BFV functions are chosen for analysis and will be the focus of future research into accelerating FHE with hardware. Despite having a slower runtime compared to its BGV counterpart and its inability to compute real numbers like CKKS, BFV offers simplicity of implementation and the option to use it as a leveled scheme to avoid the computational cost of bootstrapping (a process that is out of the scope of this paper).

### **RISC-V Instruction Set Architecture**

RISC-V (Waterman and Asanović, 2019) is an open-source modular instruction set architecture that is designed for research, education, and industrial uses. The instruction set is simple as the base specification (RV32-I) has only 47 instructions, fixed at 32 bits in length. The base specification RV32-I specifies control flow, register/memory addressing, and logic/integer manipulation. A compressed instruction set can also be used to enhance power efficiency. The modularity of RISC-V enables the use of fully developed extensions to add features such as multiplication, floating point, and vector operations as well as allowing the base specification to be extended to 64-bit and 128-bit versions. For these reasons, RISC-V is well-suited for edge computing devices that can be customized for specific use cases.

## **METHODOLOGY**

The purpose of this paper is to provide an analysis of the performance gap between high-performance devices and smaller edge computing devices as well as baseline data for future work. The methodology is to benchmark Microsoft SEAL’s BFV functions on an x86 chipset and a RISC-V chip to determine average runtimes. The average

**Table 1.** Characteristics of common FHE schemes

Scheme	Data type	Advantages
TFHE	Binary	Fast number comparison and bootstrapping
BFV	Modular integers	Simple/intuitive for users, SIMD operations over integers, scalar multiplication, leveled design
BGV	Modular integers	SIMD operations over integers, scalar multiplication, leveled design, bootstrapping as an optimization
CKKS	Real/complex numbers	SIMD operations over real numbers, polynomial approximation, deep approximate computations, fast multiplicative inverse & DFT

runtimes demonstrate the performance gap between the x86 chipsets and the RISC-V chip and provide a baseline dataset for future hardware acceleration research.

The hardware setup for this baseline experiment includes two test computers. The first is an Ubuntu workstation using a 16-core AMD Ryzen Threadripper 3955wx with 512 GB of DDR4 RAM. The second is the HiFive Unmatched board, which boots into an Ubuntu OS from an NVMe drive and uses a quad-core 64-bit RISC-V (RV64-GC) processor with 16 GB of DDR4 RAM. An SSH connection controls the HiFive board from the workstation.

The software setup for this experiment involves building Microsoft SEAL on both machines using Clang++ since it provides a ~5% runtime speedup compared to the alternative of using GNU G++ (<https://github.com/microsoft/SEAL/releases/tag/v4.1.1>). SEAL's built-in benchmark program is then executed three times on each machine and the results are averaged.

## RESULTS

Comparing the results of the AMD processor to those of the RISC-V processor shows that the AMD processor generally increases from being 33x to 50x faster than the RISC-V processor as the polynomial ring size  $n$  increases from 1024 to 32k. An exponential decrease in performance is observable for both the AMD processor and the

RISC-V processor as  $n$  increases. Figure 1 shows the runtime for BFV functions for the AMD and RISC-V processors for  $n = 1024$  and  $n = 2048$ . The most time-consuming process for these values of  $n$  is EvaluateMultCt (multiplying ciphertexts) (Figure 1). To speed up the operation of squaring a value, Microsoft added the function EvaluateSquare; however, it is still the second slowest function overall. Following in third and fourth places are the encrypt public key and encrypt secret key functions.

To mitigate potential confusion as to why evaluating plaintext (Pt) values can take longer than ciphertext values, it is worth noting that the "Evaluate . . . Pt" functions are adding/multiplying/subtracting an unencrypted plaintext operand with a ciphertext operand and returning the encrypted result. Microsoft includes these functions as they provide better runtime for evaluating plaintext than the alternative of encrypting the plaintext before doing computations. Furthermore, while EvaluateAddPt and EvaluateSubPt are two of the faster functions in terms of runtime, they take significantly longer to complete on RISC-V than on AMD. This result is evident in the speedup for EvaluateAddPt and EvaluateSubPt, which are ~67x and ~118x faster on AMD, respectively, for  $n = 1024$ , while the average speedup for all other functions is 22x.

Table 2 shows the speedups for EvaluateSubPt and EvaluateAddPt, the average speedup for all BFV

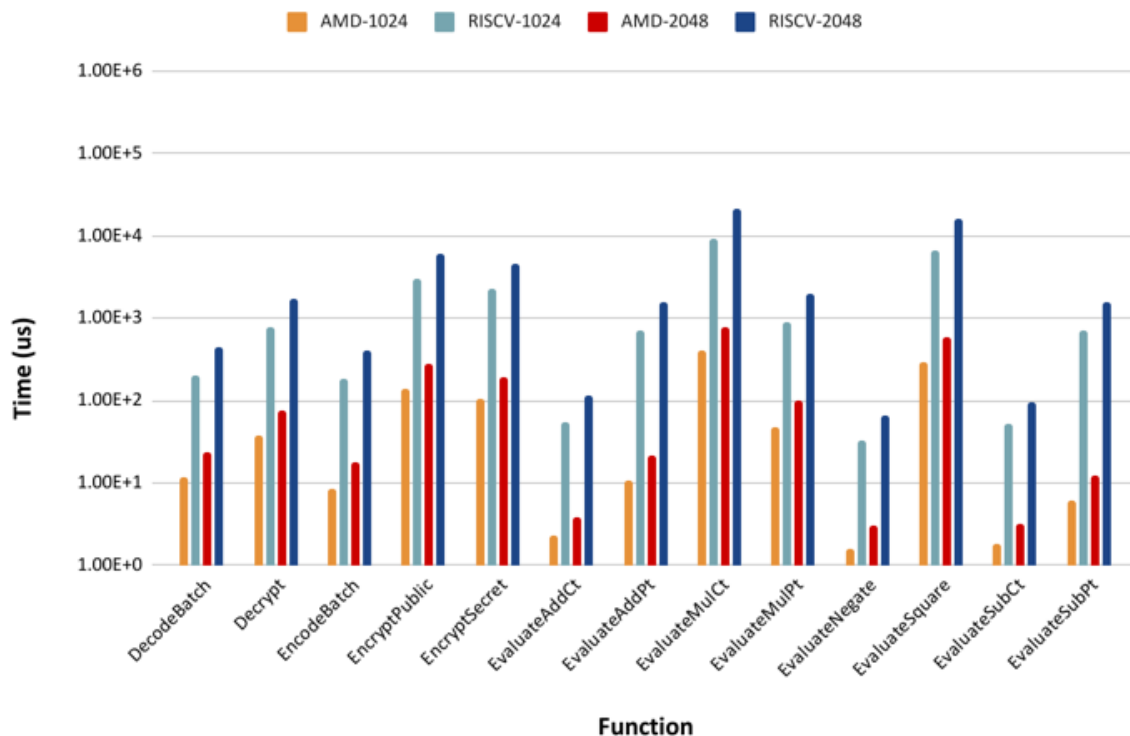


Figure 1. BFV function runtime for  $n = 1024$  and  $2048$  (log scale)

Table 2. Average AMD/RISC-V speedup for EvaluateSub/AddPt and for BFV overall

AMD/RISC-V speedup (x)	Polynomial ring size $n$					
	1024	2048	4096	8192	16384	32768
EvalSubPt	117.52	126.66	111.30	80.60	75.62	38.12
EvalAddPt	67.26	75.08	49.88	35.98	36.37	30.66
BFV Avg.	32.95	36.01	32.12	34.35	49.68	49.24
BFV w/o +/-	22.14	24.22	25.65	31.16	48.84	51.22

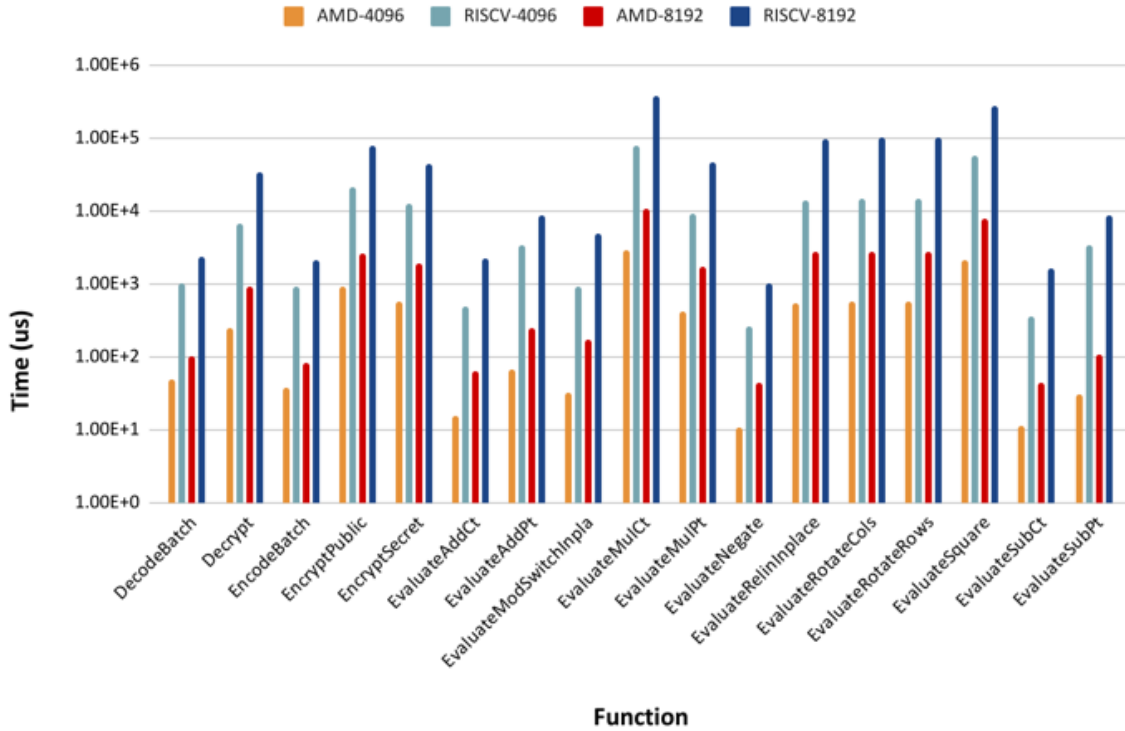


Figure. 2. BFV function runtime for  $n = 4096$  and  $8192$  (log scale)

functions, and the average speedup for BFV functions other than EvaluateSubPt and EvaluateAddPt. In the table, EvaluateAddPt swaps from being above the average of all other functions to being below the average a little after  $n = 8192$ ; however, EvaluateSubPt continues to be one of the more exaggerated gaps until  $n = 32768$ , where it has a sudden drop in speedup.

For  $n > 2048$ , the SEAL benchmark includes runtimes for four new functions: EvaluateModSwitchInplace, EvaluateRelinInplace, EvaluateRotateRows, and EvaluateRotateCols. While the in-place modulus switching function is comparable in speed to plaintext addition, the other three functions replace the encryption functions as the third slowest overall.

Figure 4 shows the runtime for generating public and secret keys with different values of  $n$ . Compared to the previous figures, this graph more clearly shows how

the runtime exponentially grows with  $n$ . For  $n = 1024$ , it seems that the key generating functions start to hit a lower bound for runtime since the power-of-two reduction from  $n = 2048$  to  $n = 1024$  does not result in the same speed improvement as the power-of-two reductions for other values of  $n$ .

## DISCUSSION

These results indicate that the HiFive Unmatched board with the RISC-V processor is significantly slower than the workstation PC with the AMD processor. Such a gap is expected, considering that the workstation PC has superior hardware. While the AMD processor is fast enough for edge computing applications, the power required for the processor is prohibitive for edge computing applications. Although the RISC-V processor can meet power

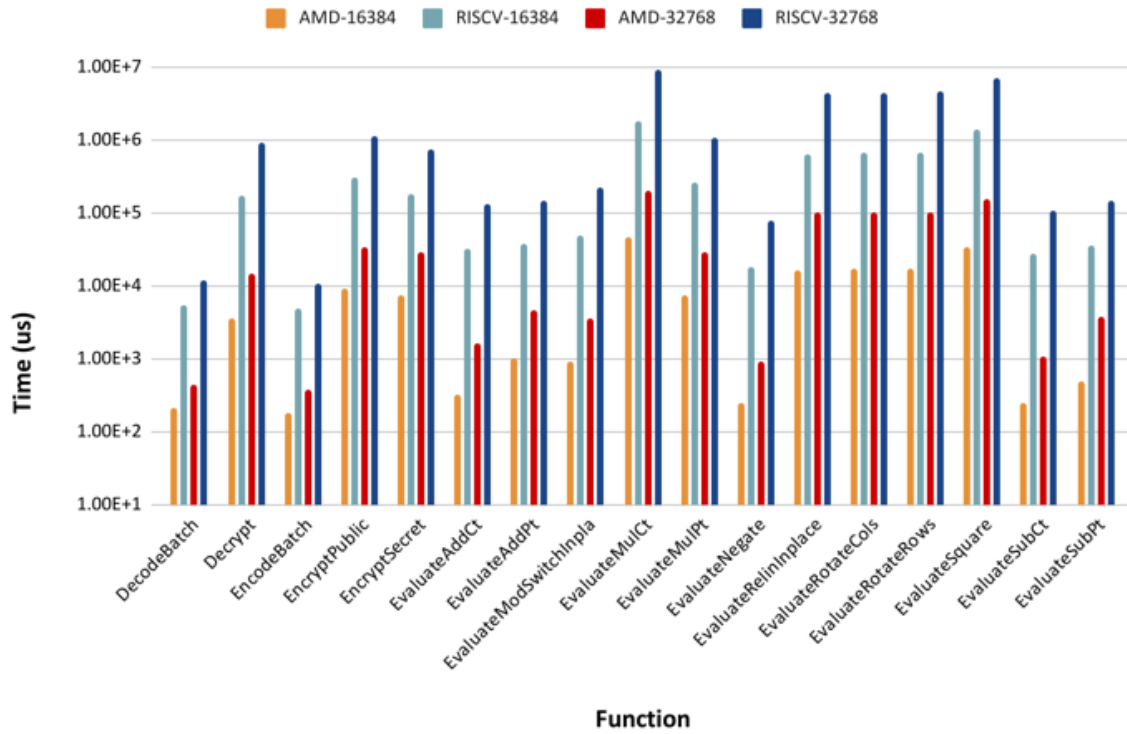


Figure 3. BFV function runtime for  $n = 16384$  and  $32768$  (log scale)

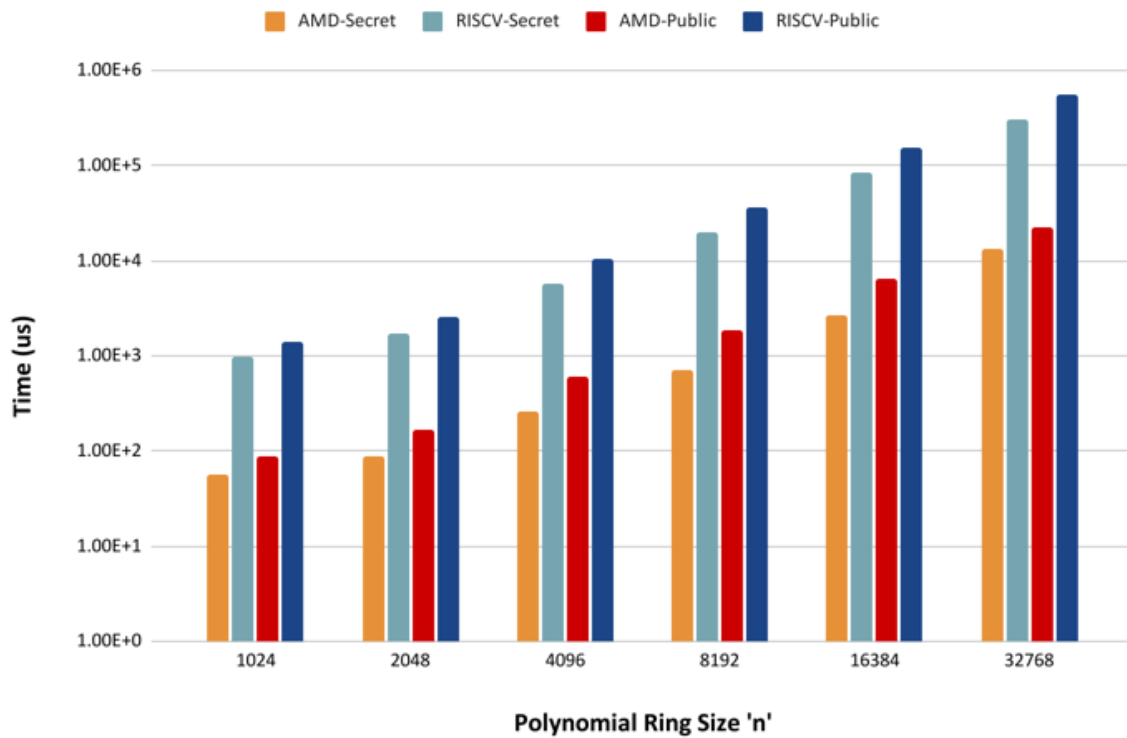


Figure 4. Public and secret key generation time for increasing polynomial ring size  $n$



requirements, the sheer amount of time required for HiFive Unmatched to evaluate these functions, especially for large values of  $n$ , is unacceptable for edge computing applications. Considering that the HiFive Unmatched board is one of the fastest RISC-V SoCs at the time of writing, FHE will not be practical to implement in edge computing devices until significant speedup can be achieved through specialized hardware optimizations.

One method for tailoring an edge computing device for FHE is to implement the number theoretic transform (NTT) to accelerate polynomial multiplication (Liang and Zhao, 2022). Microsoft SEAL implements this method in software; however, hardware has the potential to implement NTT units more efficiently. For example, Mert et al. (2019) implemented an NTT unit with an FPGA that could intercept encryption, decryption, and polynomial multiplication functions from the main PC running Microsoft SEAL and return the result. Not including transmission time from CPU to FPGA, their setup led to a 108x speedup for encryption, 53x for decryption, and 30x for polynomial multiplication. With I/O time, these values were lowered to 12x and 7x speedup for encryption and decryption, respectively. If implemented into a device as a RISC-V co-processor, like Google's Titan M2 security chip (<https://www.androidauthority.com/titan-m2-google-3261547/>), setups like this one could help make FHE computations practical for edge computing devices.

The data collected also provides a baseline for future research into accelerating FHE operations. Currently, future work includes adding an NTT unit to an FPGA-based RISC-V soft-core processor. This work in improving the speed of one component could assist with more accurately estimating how much speedup could be achieved across the processor as a whole.

## CONCLUSION

This paper presented and compared the Microsoft SEAL benchmark program runtime results for a workstation-scale PC using an AMD Ryzen Threadripper Pro 3955wx processor with the results for a HiFive Unmatched board with a RISC-V processor. A large performance gap was both expected and observed; however, this paper provided

upper and lower bounds that can be used to compare improvements made by future hardware optimizations.

## REFERENCES

- Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2011). *Fully homomorphic encryption without bootstrapping*. Retrieved May 29, 2023, from <https://eprint.iacr.org/2011/277>
- Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2016). *Homomorphic encryption for arithmetic of approximate numbers*. Retrieved May 29, 2023, from <https://eprint.iacr.org/2016/421>
- Chillotti, I., Gama, N., Georgieva, M., & Izabachène, M. (2018). *TFHE: Fast fully homomorphic encryption over the torus*. Retrieved May 29, 2023, from <https://eprint.iacr.org/2018/421>
- Fan, J., & Vercauteren, F. (2012). *Somewhat practical fully homomorphic encryption*. Retrieved May 29, 2023, from <https://eprint.iacr.org/2012/144?ref=blog.sunscreen.tech>
- Gentry, C. (2009). *A fully homomorphic encryption scheme* [PhD diss., Stanford University]. Retrieved May 29, 2023, from <https://crypto.stanford.edu/craig/craig-thesis.pdf>
- Liang, Z., & Zhao, Y. (2022). *Number theoretic transform and its applications in lattice-based cryptosystems: A survey*. Retrieved from [https://arxiv.org/abs/2211.13546#:~:text=Number%20theoretic%20transform%20\(NTT\)%20is%20the%20most,fundamental%20in%20the%20practical%20implementations%20of%20lattice%2Dbased](https://arxiv.org/abs/2211.13546#:~:text=Number%20theoretic%20transform%20(NTT)%20is%20the%20most,fundamental%20in%20the%20practical%20implementations%20of%20lattice%2Dbased)
- Mert, A. C., Öztürk, E., & Savaş, E. (2019). Design and implementation of encryption/decryption architectures for BFV homomorphic encryption scheme. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 28(2), 353–362. doi:10.1109/TVLSI.2019.2943127
- Paludo, R., & Sousa, L. (2022). NTT architecture for a Linux-ready RISC-V fully-homomorphic encryption accelerator. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 69(7), 2669–2682. doi:10.1109/TCSI.2022.3166550
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126. doi:10.1145/359340.359342
- Su, Y., Yang, B., Yang, C., & Tian, L. (2020). FPGA-based hardware accelerator for leveled Ring-LWE fully homomorphic encryption. *IEEE Access*, 8, 168008–168025. doi:10.1109/ACCESS.2020.3023255
- Waterman, A., & Asanović, K. (2019). *The RISC-V instruction set manual, Volume I: User-level ISA, document version 20191213*. RISC-V Foundation.

# The Need for Higher Fidelity Active Shooter Simulation

K. Tzvetanov<sup>1</sup> and J. Eric Dietz, PhD, PE

**Abstract** Simulation modeling has proven beneficial in gathering insights that may aid safety policy considerations for schools, offices, and outdoor events. This is especially true when conducting a drill that is not practical or possible, such as a response to active shooter events. However, current research models treat the victims as “killed” or “unaffected.” This binary approach is suitable for many simulations when the timeliness of interventions is of no concern, but it does not allow for high-fidelity simulation, which may be beneficial when developing response and safety protocols for a specific event or specific facilities. Simulating physiological decline is beneficial to improving realism and will lead to response protocol improvement. Furthermore, increased fidelity can help assess the effects of volunteer medical first response, critical care transport, and other first-responder interventions. This paper presents the implementation of a high-fidelity model for the simulation of exsanguination caused by gunshot wounds and possible mitigations, such as wound packing and tourniquet, and the model’s implementation as a reusable software component.

## INTRODUCTION

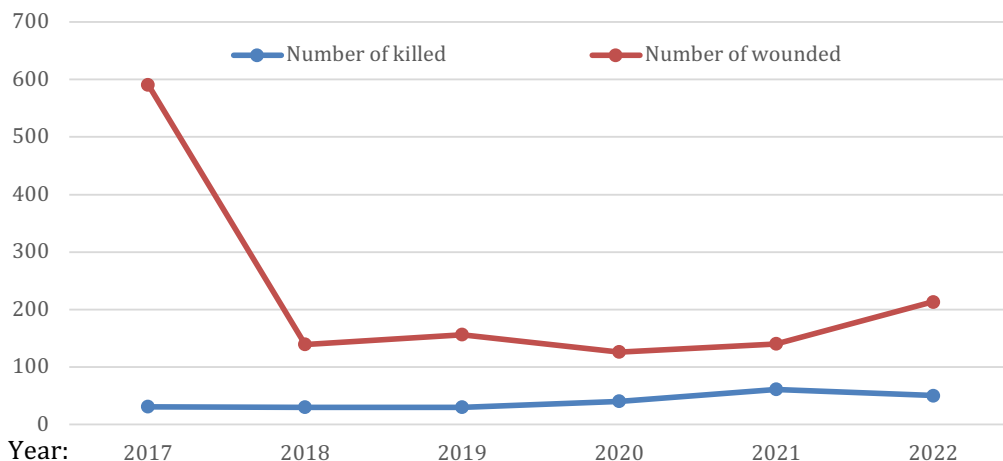
Over the past five years, active shooter events have significantly increased. Although in 2022 the trend in killings reversed and we saw an 18% decrease, just the previous year there was a 53% increase, and this upward trend has been observed for a long time (Figure 1). This increase led to research and examination of the events that unfolded during those incidents to better prepare responders. This need was further highlighted by the unreasonably long time it took the police to act in the Robb Elementary School shooting (Diaz, 2022; Kriel et al., 2022). Despite the need, an in-person reenactment and testing of those policies is not trivial and can be cost-prohibitive. To compensate for that, simulation modeling can be used to develop a response policy with a minimal cost while providing a rapid assessment of interventions. In the past, those simulations have primarily focused on the ability to thwart the active shooter’s actions through the use of door locks, the presence of additional police officers and security guards, allowing a percentage of concealed carry personnel within a venue, and testing behaviors such as “run, hide, fight” (Anklam et al., 2015; Kirby, 2016; Kirby et al., 2016; Lee et al., 2018; Harrell, Weston, Alteri, et al., 2023).

However, there is a significant drawback, which is the lack of injury and mitigation simulation. The number of injured has steadily increased for the past five years. Just in 2022, it jumped by 52%, and 11% the year prior (Table 1). Furthermore, between 2000 and 2010, 445 school shootings occurred that resulted in a victim surviving but with life-threatening wounds, which proves that the timing of medical response is material to the casualty outcome of the event (Bonanno and Levenson, 2014).

The data reveals two interesting facts. For the last two periods, deaths have decreased by 11%, while the number of wounded survivors has increased by 52%. While we may already be seeing an improvement in response procedures, we cannot conclude that. However, the number of injured has certainly increased even more. In an outlier case, the 2017 Route 91 Harvest Music Festival shooting in Las Vegas, a gunman wounded more than 800 and killed 58 people. In this case, the wounded casualties outnumbered the fatalities by more than 12 times. Fortunately, due to consistent training efforts for mass casualty events, the city was able to activate more than 160 firefighters, who could integrate with police efforts and emergency medical personnel (Apgar and Shoro, 2017), and more than 200 patients were transported to nearby hospitals for treatment by first responders.

To account for victims and medical response, we need a higher level of fidelity in simulations and to stop representing victims by a binary (“dead” or “healthy”) state. A study covering a cohort of 1,226 gunshot wound patients in a trauma center in Saint Louis, Missouri, showed that 93% of victims brought to the emergency department survived (de Anda et al., 2018). Another vivid example is the outcome of the Pulse Nightclub shooting, where 49 people died. A study revealed that 16, or 32%, of the fatalities could have been prevented given a timely response (Smith et al. 2018; Smith et al., 2020).

The studies above demonstrate that the outcomes will be positive given a timely medical intervention. If the “binary outcome” simulation were used and the wounded were considered “dead,” timely mitigation and transport could not have been evaluated.



**Figure 1.** Incident statistics, 2017–2022. (Federal Bureau of Investigation, 2022, 2023).

**Table 1.** Incident statistics, 2017–2022 (Federal Bureau of Investigation, 2022, 2023).

	2017	2018	2019	2020	2021	2022
Killed	31	30	30	40	61	50
Wounded	591*	139	156	126	140	213

\* Caused by an outlier event—the Route 66 Music Festival shooting in Las Vegas, NV

## THE GOAL

This current work introduces a *uniform model for computer simulations* of injuries and their treatment, which can be used across multiple research teams, allowing the results from those studies to be compared. It builds on previous work by Tzvetanov (2021). This model is not designed to predict outcomes for a specific victim in a clinical setting. An additional design goal of the model is easy integration into currently available simulations.

## MODELING BLOOD LOSS

To successfully model the pathophysiological decline of a victim, we have collected data from several studies, some of which pertain to gunshot injuries in civilian settings, the rest based on animal testing. Military studies were avoided because of the difference in wounding patterns heavily influenced by body armor worn in that setting.

### *Differences in Military and Civilian Wounding Patterns*

Extremity hemorrhage control was the primary and most preventable of death causes. A comprehensive study using autopsy reports from US-based mass shooting events showed that approximately 7% of the injuries

might have been survivable with appropriate and timely medical intervention (Smith et al., 2016). The study found significant differences between military and civilian fatality wound placement, noting that 72% of civilian fatalities had injuries to the head and torso, compared to 48% of combat-related fatalities. This difference is likely due to the additional protection of ballistic helmets and vests in military setting coupled with shooters being much closer to victims in civilian settings. Overall, in civilian settings, extremity hemorrhage accounted for a small percentage of preventable deaths, but wounds to the chest made up most of the preventable civilian deaths (Smith et al., 2016).

### *Initial Blood Amount*

A number of studies were reviewed to establish the starting amount of blood for the victim; however, since most numbers converge with Nadler’s numbers and he was the first to publish, the model uses those numbers, namely 75 ml of blood per kilogram for males and 65 ml/kg for females. To establish the initial blood amount based on weight, we use a 2012 study (Walpole et al., 2012), where the average person’s weight in North America is 80.7 kg, resulting in an estimated 5.25 to 6 liters. The numbers proposed for the model are summarized in Table 2.

**Table 2.** Proposed simulation values for blood volume and weight

Variable	Simulation value
Blood per kilogram for males	75 ml/kg
Blood per kilogram for females	65 ml/kg
Compensation for ages over 65	–5 ml/kg
Default person weight	80.7 kg

**Table 3.** Subset of values provided by Tjardes and Luecking (2018).

Injury compartment	Flow			
	mL/30 sec	mL/1 min	mL/2 min	mL/3 min
Abdominal aorta	468	936	1,872	2,808
Common iliac artery	234	468	936	1,404
Internal iliac artery	57	114	228	456
External iliac artery	177	354	702	1,062
Femoral artery	87	174	348	522

**Blood Loss Rate**

There is very little data on blood loss resulting from gunshot injuries, because of their relatively rare occurrence and the impracticability of taking field measurements, so most of the studies relevant to the topic measure blood flow based on the Doppler effect, use animals for testing, or use a mathematical model to describe the flow.

A 1995 study (Johnson et al., 1995) used transcutaneous ultrasound to measure the blood flow in the tibial and humeral arteries in a cohort of five female and sixteen male subjects. The study revealed blood flow between approximately 250 ml/min (at rest) and 1,500 ml/min (at maximal effort).

Osada et al. took a similar approach, but the measurements were using pulsed Doppler ultrasounds with spectral analysis at the aorta (above the celiac artery bifurcation for incoming flow) and femoral arteries (bilaterally on the femoral arteries of both legs for the outgoing flow), capturing the blood flow to all abdominal organs (Osada et al., 2011). The measurements were made in sitting and supine positions, and it was established that there was an approximate 550 ml/min flow difference between supine and sitting positions and a reduction of ~20% in the inspiration phase. And while this study appears to provide high-resolution data, it does not cover people standing or running, which is the case in an active shooter situation, and it has a small sample size.

In both of those studies, backpressure slows the bleeding since there is no wound. And in the case of a gunshot injury, the blood flow may be relatively unobstructed.

Alternatively, the blood flow can be expressed analytically (Tjardes and Luecking, 2018). The analytic model represents the circulatory system as a series of three arterial and two venous compartments, representing organs with similar properties and the heart. In this model, the output blood pressure of a compartment is the input pressure of the next one. In this model, they account for baroreflex and also assume early stages of hemorrhage, so the hemodynamics is solely determined by the cardiac function and the vascular system's passive physical properties. This model does not account for the humoral compensatory mechanisms, which take time, and for

**Table 4.** Summary of flow rates for different compartments used in the simulation

Injury compartment vessel	Flow, mL/sec
Abdominal aorta	15.6
Common iliac artery	7.8
Internal iliac artery	1.9
External iliac artery	5.9
Femoral artery	2.9
Brachial (proportional)	1.28

intestinal volume shift, chemoreceptors, and cardiopulmonary low-pressure receptors. While this decreases accuracy in prolonged blood loss situations, it is well-tuned for short-term, high-speed hemorrhage, which is consistent with our scenario. While their model is not validated clinically, it has substantial similarity with the data collected in other studies during the last six months of the Second World War (Beecher, 1960) and is summarized in Table 3. For the reasons outlined above, the author suggests the use of the Tjardes study as a reference for the model.

One shortcoming of this model is the lack of data on the upper extremities. For simulation purposes, we can use the diameter proportion for the femoral and brachial arteries. This ratio can be informed by a couple of studies (Tomiyama et al., 2015; Lorbeer et al., 2018). According to the former study, the brachial artery is 3.93 mm, and according to the latter one, the distal and proximal femoral diameters are 7.7 mm and 10.3 mm, correspondingly with an average of 9 mm. This gives us a proportional blood flow close to 38 mL/30 sec, or 1.28 mL/sec, which we recommend for use in simulation. (See Table 4.)

**Injury Area**

To establish the probability of injury in different areas, the author reviewed the studies presented in Table 5. Unfortunately, some of those studies focus on fatal wounding statistics, use nonsurviving victims, and do not provide detailed statistics on the particular injury. At the same time, for the simulation model, we need a statistic

**Table 5.** Studies on the injury area

Study	Scope (deceased/ surviving/both)	Statistics					Study size	
		Head	Face/neck	Chest/ upper back	Abdomen/ lower back	Lower extremity		Upper extremity
E. R. Smith et al., 2016	Deceased; fatal and nonfatal wounds	29%	9%	29%	14%	20%	12 events; 139 fatalities; 371 wounds	
Sarani et al., 2019	Deceased; overlap of statistics						23 events; 232 victims;	
Karaca et al., 2015	Both	31%		25%	11%	48%	29%	142 patients
C. P. Smith et al., 2020	Both; single event	9%	3%	25%	16%	46%	1 event; 49 fatalities; 53 injured; 336 wounds	
Knickerbocker et al., 2019	Both; 2 events	17.2% (head/face)	3.4% (neck only)	10.3%	13.8%	55.2%	2 events; 22 fatalities; 40 injured	

**Table 6.** Recommended values for injury probabilities used for simulation

Body area	Wounding probability
Head/face/neck	38%
Chest/upper back	29%
Abdomen/lower back	14%
Lower and upper extremity	20%

representative of the probability of injury to a particular area regardless of the outcome.

Of the studies presented in Table 5, only two (Karaca et al., 2015; Smith et al., 2020) satisfy the requirement to have data about survivors’ injuries, in addition to the deceased, and the injury grouping somewhat overlaps with the theoretical compartments from the mathematical model presented above (Tjardes and Luecking, 2018), which makes them suitable candidates. The former does not account for double injuries and injuries affecting two areas, so the percentages add up to more than 100%. Table 6 presents the data points recommended for the simulation.

**Hemorrhage, Physiological State, and Death**

The last three components of the blood loss simulation are determining the victim’s state of mind, their ability to ambulate, and the point at which they lose sufficient blood such that it would be impossible to recover them. All of those components depend strongly on how much

blood they have lost. A hemorrhage is classified into four categories (Gutierrez, 2004; Cannon, 2018).

Class I occurs when the patient loses less than 15% of blood (Cannon, 2018), which is the equivalent of a patient donating blood. This usually takes approximately 10 minutes, allowing the body ample time to adjust. Without preexisting conditions, like anemia or a severe heart problem, there is no decrease in blood pressure or increase in respiratory response and pulse, and no physical or mental impairment (Gutierrez, 2004).

Class II blood loss is accompanied by decreased blood pressure and increased pulse and respiratory rate to compensate for the blood loss, which is between 15% and 30% (Cannon, 2018). The victim would be in an excited mental state but able to move independently, although toward the high end of the range they may not be very coherent (Cannon, 2018). Similarly, their ambulatory state would vary greatly, but they would be likely to stop moving on their own during this state.

Hemorrhagic (hypovolemic) shock occurs when the patient goes into shock due to blood loss. Unfortunately, none of the reviewed literature provides information on whether the patients were in hemorrhagic shock. However, in most cases, the victim will go into shock during this category.

Class III occurs when the loss is 30% to 40% of total blood volume and is accompanied by lower blood pressure and increased pulse and respiratory rates (Cannon, 2018). The victim’s mental state will be impaired, and some cells will switch to anaerobic metabolism, as

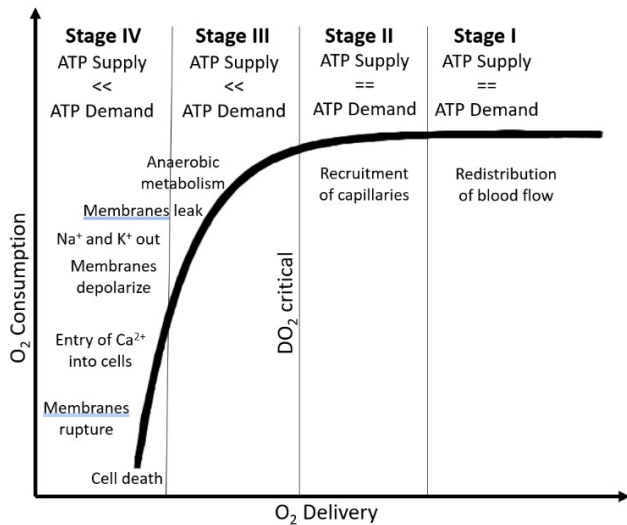


Figure 2. Stages of hemorrhage (Gutierrez, 2004)

shown in Figure 2 (Gutierrez, 2004; Cannon, 2018). At this point, the victim is in critical condition, and advanced medical intervention is necessary.

Class IV occurs when more than 40% blood loss is experienced, and victims are lethargic with a rapid pulse and respiratory rate (Cannon, 2018). At this point, cell death occurs (Figure 2), and the victim enters the “bloody vicious cycle,” elaborated by Moore (1996). At this point, lack of immediate ER intervention equates to death. So, for modeling purposes, we’ll use 40% as the death threshold.

The above paragraphs are summarized in Table 7. Note that blood volume losses are approximate and will differ in practice as individuals have different amounts of blood.

As we discussed, the ambulatory state and hypovolemic shock onset have high variability between patients, and for simulation purposes we need consistency to decrease variability between experiments. Toward this end, we will assume that certain injury areas and blood

Table 8. Proposed simulation ambulatory and nonambulatory states

Injured Area	Ambulatory
Head	No
Neck/face	No
Chest/upper back	Yes
Abdomen/lower back	Yes
Lower extremity	No
Upper extremity	Yes
Over 20% blood loss regardless of injury	No

Table 9. Proposed simulation values and color codes for different blood loss states

Victim simulation state	Blood loss, %	Color
No blood loss	0	natural avatar or white
Class I hemorrhage	<15	green
Class II hemorrhage	<30	yellow
Class III hemorrhage	<40	red
Class IV hemorrhage	>=40	black
Hemorrhagic shock	20%	n/a
Ambulatory threshold	25	n/a
Death	40	black

loss levels will always produce nonambulatory patients. A mechanical impairment will consist of an injury to the upper chest, the pelvis, and the thighs, but not below the knee, and nonambulatory blood loss will be 25%. Table 8 summarizes those conditions.

Regarding hypovolemic shock, the reviewed studies did not track the threshold, but all agree this will happen in Class II hemorrhage. To be conservative, we suggest using 20% as the threshold, which is consistent with the conservative nature of the model, so a victim will have a lower probability of surviving; thus, if there is a bias introduced due to this assumption, it will be toward lower survivability.

We summarize the recommended values in Table 9.

Table 7. Classification of hemorrhage (Gutierrez et al., 2004)

Parameter	Class			
	Class I	Class II	Class III	Class IV
Blood loss (ml)	<750	750–1500	1,500–2,000	>2,000
Blood loss (%)	<15	15–30	30–40	>40
Pulse rate (beats per minute)	<100	>100	>120	>140
Blood pressure	Normal	Decreased	Decreased	Decreased
Respiratory rate (breaths per minute)	14–20	20–30	30–40	>35
Urine output (ml/hour)	>30	20–30	5–15	Negligible
CNS symptoms	Normal	Anxious	Confused	Lethargic

## THE NEED FOR HIGHER FIDELITY SIMULATION

Based on an FBI study of active shooter incidents (Federal Bureau of Investigation, 2013), 69.8% of incidents end in 5 minutes, of which slightly over half end in under 2 minutes. In addition, 66.9% of those incidents ended before the police arrived. This raises the question, What is the average police and EMS response time? According to an FBI statistic, the police response time to active shooter events is consistently under 6 minutes (Federal Bureau of Investigation, n.d.), although in another study (Bennett, 2018) spanning some 40 police agencies, the median response time for Priority 1 calls is 8.8 minutes, but this study is not specific to active shooter events. It is important to note that the time is measured to the scene but not to the actual close-to-the-officer victim. According to another study, the mean EMS arrival time is also 6 minutes for urban and suburban areas and 13 for rural.

This means that in most events, a couple of minutes pass before an officer can assist a victim, provided they have established that the scene is secure. Thus in the way we currently simulate these events, it does not matter if the police officer arrives 1 second after the event has concluded or in 2 hours, since the simulated victims die immediately, and the survivors' health does not decline.

Now let's consider the reality. Take, for example, a severe but easily treatable injury, such as a femoral bleed, which can be mitigated by applying a tourniquet. Statistically, according to the data presented in the model (Table 3), it will take more than 10 minutes for the victim to pass the point of no return. This means that even if the victim was injured at the beginning of the incident, there is still a little time for the officer to intervene if they follow an optimized response protocol, including timely triage and critical care transport. However, in the current state of simulation, we could not discern that. Furthermore, if an active bystander responds by even direct pressure, they will slow the hemorrhage and extend the window of survivability, and if they use a tourniquet, with more than 90% probability this will increase that window by another 2 hours without a significant risk for the limb.

Figure 3 shows this timing of events, revealing the opportunity for response improvement, thus the need for higher simulation fidelity allowing those events to be simulated.

## CONCLUSION

It is clear that a higher level of simulation fidelity is necessary to provide benefits to response policy development aided by computer simulation. In this study, we present a baseline for the computer simulation of the impact of gunshot wounds during an active shooter simulation in

a broad set of cases. The data was collected from a wide variety of medical studies, and the output is easy to program into a computer simulation in any language. The components the model consists of are wounding patterns and injury area, initial blood volume and blood loss, and victim mobility and terminal state, and these are backed up by quantitative data.

The first task was reasonably easy to achieve due to a large number of retroactive studies, both military and civilian, although a bias was placed on the latter type, as this study intends to create a simulation model for civilian applications. The second task posed significant challenges caused by the lack of experimental data due to the rare occurrence of those injuries and the nature of dealing with them, making it impossible to conduct controlled experiments, and most of the data were gathered from retrospective studies.

An additional challenge was posed by the lack of a standard data collection structure, which made it difficult to combine and summarize them. Thus, the results were not averaged but were picked to be a specific study that represents the median. This enables future researchers to replace a study without changing the rest of the model structure. For example, determining the blood flow rate is based on the model of Tjardes and Luecking, which is mathematical in nature. While the study represents a very stable base with understood biases coming from the mathematical model and can be adjusted easily when new, higher fidelity data is available.

Due to the model's built-in conservative bias that victims have shorter expected life spans, it will yield less optimistic results and minimize the error when combined with larger-scale active shooter simulations, which makes it a reasonable basis for computer simulation.

## FUTURE WORK

This work is currently in active development and will continue in several directions. The immediate next steps are to expand the model and provide more details (Tzvetanov, 2023c), followed by a detailed model for the treatment and mitigation of those injuries by first responders or active bystanders (Tzvetanov, 2023b), and to provide a reference implementation in an AnyLogic library (Tzvetanov, 2023a), allowing its easy inclusion in active shooter computer simulations. Later, the model and library will be extended by containing other types of injuries and treatments.

In the next phase, this model will be used to simulate specific situations, helping to determine the effect of early medical intervention to inform public policy toward training the civilian population and providing hemorrhage control kits in programs like STOP THE BLEED.

Blunt trauma is prevalent in everyday life—from vehicular collisions, physical assaults, and falls; it is a significant cause for seeking emergency medical attention. When combined with the next direction of research, covering the golden hour, it can help drive policy development and the placement of emergency facilities statewide.

Each of these future directions has much to offer to improve public safety policy, ultimately leading to more saved lives.

The final lesson learned from this research is that we need a more uniform approach to testing and data collection to improve this type of simulation. An additional line of research would be to develop a consistent framework on what types of data need to be collected and documented in such studies.

## NOTE

1. OrcID: <https://orcid.org/0000-0001-6307-6625>

## REFERENCES

- Anklam, C., Kirby, A., Sharevski, F., & Dietz, J. E. (2015). Mitigating active shooter impact: Analysis for policy options based on agent/computer-based modeling. *Journal of Emergency Management*, 13(3), 201–216. <https://doi.org/10.5055/jem.2015.0234>
- Apgar, B., & Shoro, M. (2017, October 6). Las Vegas first responders trained extensively for mass casualty event. *Las Vegas Review-Journal*. Retrieved October 16, 2020, from <https://www.reviewjournal.com/local/the-strip/las-vegas-first-responders-trained-extensively-for-mass-casualty-event/>
- Beecher, H. K. (1960). The physiologic effects of wounds. *A.M.A. Archives of Surgery*, 80(3), 366–373. <https://doi.org/10.1001/archsurg.1960.01290200010002>
- Bennett, D. S. (2018). Police response times to calls for service: Fragmentation, community characteristics, and efficiency [Paper presentation]. Public and Environmental Economics Seminar, Stanford University, Stanford, CA.
- Bonanno, C. M., & Levenson, R. L. (2014). School shooters: History, current theoretical and empirical findings, and strategies for prevention. *SAGE Open*, 4(1), 215824401452542. <https://doi.org/10.1177/2158244014525425>
- Cannon, J. W. (2018). Hemorrhagic shock. *New England Journal of Medicine*, 378(4), 370–379. <https://doi.org/10.1056/NEJMr1705649>
- de Anda, H., Dibble, T., Schlaepfer, C., Foraker, R., & Mueller, K. (2018). A cross-sectional study of firearm injuries in emergency department patients. *Missouri Medicine*, 115(5), 456–462.
- Diaz, J. (2022, December 2). Uvalde survivors file a \$27 billion class-action lawsuit against police and others. NPR. Retrieved December 27, 2022, from <https://www.npr.org/2022/12/02/1140119739/uvalde-shooting-survivors-class-action-lawsuit>
- Federal Bureau of Investigation. (n.d.). *Police response time to active shooter attacks*. *Law Enforcement Bulletin*. Retrieved June 28, 2023, from <https://leb.fbi.gov/image-repository/police-response-time-to-active-shooter-attacks.jpg/view>
- Federal Bureau of Investigation. (2013). *A study of active shooter incidents in the United States between 2000 and 2013*. <https://www.fbi.gov/file-repository/active-shooter-study-2000-2013-1.pdf/view>
- Federal Bureau of Investigation. (2022). *Active shooter incidents in the United States in 2021*. <https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2021-052422.pdf/view>
- Federal Bureau of Investigation. (2023). *Active shooter incidents in the United States in 2022*. <https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2022-042623.pdf/view>
- Gutierrez, G., Reines, H. D., & Wulf-Gutierrez, M. E. (2004). Clinical review: Hemorrhagic shock. *Critical Care*, 8(5), 373–381. <https://doi.org/10.1186/cc2851>
- Harrell, N., Weston, R. E., Alteri, S. P., et al. (2023). Analyzing the impact of concealed carry weapons and school resource officers on school shootings: An agent-based modeling approach. *J Emer Mgmt*. In press. <https://doi.org/10.5055/jem.0818>
- Hughes, H. K., & Kahl, L. K. (2017). *The Harriet Lane Handbook* (21st ed.). Elsevier.
- Johnson, D., Bonnin, P., Perrault, H., Marchand, T., Vobecky, S. J., Fournier, A., & Davignon, A. (1995). Peripheral blood flow responses to exercise after successful correction of coarctation of the aorta. *Journal of the American College of Cardiology*, 26(7), 1719–1724. [https://doi.org/10.1016/0735-1097\(95\)00382-7](https://doi.org/10.1016/0735-1097(95)00382-7)
- Karaca, M. A., Kartal, N. D., Erbil, B., Öztürk, E., Kunt, M. M., Şahin, T. T., & Özmen, M. M. (2015). Evaluation of gunshot wounds in the emergency department. *Turkish Journal of Trauma & Emergency Surgery*, 21(4), 248–255. <https://doi.org/10.5505/tjtes.2015.64495>
- Kirby, A. M. (2016). *Comparing policy decisions for active shooters using simulation modeling*. Purdue University. <https://search.proquest.com/openview/15386d04c6ddd638949e94f179af04c6/1>
- Kirby, A., Anklam, C. E., & Dietz, J. E. (2016). Active shooter mitigation for gun-free zones. In *Proceedings of the IEEE Symposium on Technologies for Homeland Security (HST)* (pp. 1–6). <https://doi.org/10.1109/THS.2016.7568957>
- Knickerbocker, C., Gomez, M. F., Lozada, J., Zadeh, J., Costantini, E., & I Puente (2019). Wound patterns in survivors of modern firearm related civilian mass casualty incidents. *American Journal of Disaster Medicine*, 14(3), 175–180. <https://doi.org/10.5055/ajdm.2019.0329>
- Kriel, L., Despart, Z., Serrano, A., & Asgarian, R. (2022). “I’m so scared”: 911 recordings reveal fear and urgency of those trapped in Uvalde elementary school. *The Texas Tribune*. Retrieved December 27, 2022, from <https://www.texas>



- tribune.org/2022/11/01/uvalde-911-dispatch-recordings/
- Lee, J. Y., Dietz, E. J., & Ostrowski, K. (2018). Agent-based modeling for casualty rate assessment of large event active shooter incidents. In *Proceedings of the 2018 Winter Simulation Conference* (pp. 2737–2746). Available at: <https://doi.org/10.1109/WSC.2018.8632535>
- Lorbeer, R., Grotz, A., Dörr, M., Völzke, H., Lieb, W., Kühn, J.-P., & Minsel, B. (2018). Reference values of vessel diameters, stenosis prevalence, and arterial variations of the lower limb arteries in a male population sample using contrast-enhanced MR angiography. *PLOS ONE*, *13*(6), e0197559. <https://doi.org/10.1371/journal.pone.0197559>
- Moore, E. E. (1996). Staged laparotomy for the hypothermia, acidosis, and coagulopathy syndrome. *American Journal of Surgery*, *172*(5), 405–410. [https://doi.org/10.1016/S0002-9610\(96\)00216-4](https://doi.org/10.1016/S0002-9610(96)00216-4)
- Morgan, G. E., Mikhail, M. S., and Murray, M. J. (2002). *Clinical anesthesiology* (3rd ed.). McGraw-Hill.
- Muraki, R., Hiraoka, A., Nagata, K., Nakajima, K., Oshita, T., Arimichi, M., Chikazawa, G., Yoshitaka, H., & Sakaguchi, T. (2018). Novel method for estimating the total blood volume: The importance of adjustment using the ideal body weight and age for the accurate prediction of haemodilution during cardiopulmonary bypass. *Interactive Cardiovascular and Thoracic Surgery*, *27*(6), 802–807. <https://doi.org/10.1093/icvts/ivy173>.
- Nadler, S. B., Hidalgo, J. U., and Bloch, T. (1962). Prediction of blood volume in normal human adults. *Surgery*, *51*(2), 224–232. <https://doi.org/10.5555/uri:pii:0039606062901666>
- OpenAnesthesia. *Maximum allowable blood loss*. (n.d.). Retrieved May 21, 2021, from [https://www.openanesthesia.org/maximum\\_abl\\_calculation/](https://www.openanesthesia.org/maximum_abl_calculation/)
- Osada, T., Nagata, H., Murase, N., Kime, R., & Katsumura, T. (2011). Determination of comprehensive arterial blood inflow in abdominal-pelvic organs: Impact of respiration and posture on organ perfusion. *Medical Science Monitor: International Medical Journal of Experimental and Clinical Research*, *17*(2), CR57–CR66. <https://doi.org/10.12659/MSM.881388>
- Police response times* (n.d.). City of Oakland. Retrieved June 28, 2023, from <https://data.oaklandca.gov/Equity-Indicators/Police-Response-Times/wgvi-qsey>
- Riley, A. A., Arakawa, Y., Worley, S., Duncan, B. W., & Fukamachi, K. (2010). Circulating blood volumes: A review of measurement techniques and a meta-analysis in children. *ASAIO Journal*, *56*(3), 260–264. <https://doi.org/10.1097/MAT.0b013e3181d0c28d>
- Sarani, B., Hendrix, C., Matecki, M., Estroff, J., Amdur, R. L., Robinson, B. R. H., Shapiro, G., Gondek, S., Mitchell, R., & Smith, E. R. (2019). Wounding patterns based on firearm type in civilian public mass shootings in the United States. *Journal of the American College of Surgeons*, *228*(3), 228–234. <https://doi.org/10.1016/j.jamcollsurg.2018.11.014>
- Smith, C. P., Cheatham, M. L., Safcsak, K., Emrani, H., Ibrahim, J. A., Gregg, M., Eubanks, W. S., Lube, M. W., Havron, W. S., & Levy, M. S. (2020). Injury characteristics of the Pulse Nightclub shooting: Lessons for mass casualty incident preparation. *Journal of Trauma and Acute Care Surgery*, *88*(3), 372–378. <https://doi.org/10.1097/TA.00000000000002574>
- Smith, E. R., Shapiro, G., and Sarani, B. (2016). The profile of wounding in civilian public mass shooting fatalities. *Journal of Trauma and Acute Care Surgery*, *81*(1), 86–92. <https://doi.org/10.1097/TA.0000000000001031>
- Smith, E. R., Shapiro, G., & Sarani, B. (2018). Fatal wounding pattern and causes of potentially preventable death following the pulse night club shooting event. *Prehospital Emergency Care*, *22*(6), 662–668. <https://doi.org/10.1080/10903127.2018.1459980>
- Tjardes, T., and Luecking, M. (2018). The Platinum 5 min in TCCC: Analysis of junctional and extremity hemorrhage scenarios with a mathematical model. *Military Medicine*, *183*(5–6), e207–e215. <https://doi.org/10.1093/milmed/usx016>
- Tomiyama, Y., Yoshinaga, K., Fujii, S., Ochi, N., Inoue, M., Nishida, M., Aziki, K., Horie, T., Katoh, C., & Tamaki, N. (2015). Accurate quantitative measurements of brachial artery cross-sectional vascular area and vascular volume elastic modulus using automated oscillometric measurements: Comparison with brachial artery ultrasound. *Hypertension Research*, *38*(7), 478–484. <https://doi.org/10.1038/hr.2015.6>
- Tzvetanov, K. T. (2021). *Improving the fidelity of agent-based active shooter simulations through modelling bloodloss and injury management* [Master's thesis, Purdue University].
- Tzvetanov, K. (2023a). *AnyLogic implementation of injury and blood loss, and hemorrhage control models in the context of active shooter simulations* [Manuscript submitted for publication].
- Tzvetanov, K. (2023b). *Modelling hemorrhage control in the context of agent-based active shooter simulations* [Manuscript submitted for publication].
- Tzvetanov, K. (2023c). *Modelling injury and blood loss in the context of agent-based active shooter simulations* [Manuscript submitted for publication].
- University of Iowa Health Care. (n.d.). *Head and neck protocols. Maximum allowable blood loss*. Retrieved May 24, 2021 from <https://medicine.uiowa.edu/iowaprotocols/maximum-allowable-blood-loss>
- Walpole, S. C., Prieto-Merino, D., Edwards, P., Cleland, J., Stevens, G., & Roberts, I. (2012). The weight of nations: An estimation of adult human biomass. *BMC Public Health*, *12*(1), 439. <https://doi.org/10.1186/1471-2458-12-439>

# Optimizing Hemorrhage Control Kit Placement

K. Tzvetanov and J. Eric Dietz, PhD, PE

**Abstract** Simulation modeling has proven beneficial in gathering insights that may aid safety policy considerations for schools, offices, and outdoor events. Most current simulations focus on the actual act of violence but do not consider what happens when a victim is affected by being injured. In this presentation, the author proposes a methodology for the evaluation of the placement and number of first aid kits and how it can affect the outcome and, particularly, victim survivability in an active shooter situation.

## INTRODUCTION

Active shooter events have increased in frequency in recent years throughout the United States, with attacks occurring in schools, workplaces, concerts, festivals, religious locations, and the list continues. Although in 2022 the number of killed dropped by 18%, it is still dwarfed by the 53% increase in the previous year. Similar is the general trend (see Figure 1) for the wounded; however, there was a notable increase in 2022, accompanied by a decrease in mortality, leading us to suspect that this may be due to improved response that results in more victims surviving gunshot wounds (Federal Bureau of Investigation, 2020; 2021; 2022, p. 20; 2023).

The increased mortality has led many to examine the events that unfold during active shooter incidents, trying to understand them better as well as prepare the responding agencies. One of the most valuable tools toward that goal is simulation modeling, which is used to assess and develop active shooter response policies. While computer simulations allow for rapid prototyping and assessment at a lower cost, current work has not been comprehensive. So far, virtually all research assumes the victims are either dead or alive, which is beneficial when evaluating how to thwart the active shooter’s actions through the use of door locks, additional police officers, and security guards, allowing a percentage of concealed carry personnel within a venue, and testing behaviors such as “run, hide, fight”; however, it does not provide adequate detail for simulating medical processes where time is of the essence (Anklam et al., 2015; Kirby, 2016; Kirby et al., 2016; Lee et al. 2018; Lee, 2019). In recent work, Tzvetanov and Dietz (2023) proposed a model allowing for a higher level of detail during the simulation of the injury and pathophysiological trajectory of the victims, which further refines the previous model presented by Tzvetanov (2021) and in forthcoming work (Tzvetanov, 2023b, 2023c, 2023a). In this study, the authors make the case that there is a need for a higher level of detail in the timing of injury and death by showing the timeline

of police and EMS response versus the longevity of an injured individual (see Figure 2). In addition, they present an example from a study from a Saint Louis, Missouri, emergency department, where 93% of gunshot wound victims survived, showing how timely medical intervention can influence outcomes positively (de Anda et al., 2018).

## THE ROLE OF PREPAREDNESS

On October 1, 2017, during the Route 91 Harvest festival in Las Vegas, Nevada, a lone gunman opened fire on spectators, killing 60 and wounding more than 400. The festival was an unusually large event, and the sheer volume of victims would have overwhelmed most cities’ emergency response services. However, Clark County had been training to respond to mass casualty events and, in a short period, assembled a team of some 160 firefighters and triaged and transported the victims (Apgar and Shoro, 2017).

When discussing preparedness, we must consider equipment apart from response policies and training. In the case of smaller organizations such as schools, libraries, and other public buildings, equipment most commonly equates to first aid kits capable of hemorrhage control, which we call hemorrhage control kits (HCKs).

Generally, those kits are designed to be used by civilians. They can be used during the incident if the shooter is not present, but mainly they are used right after the incident has concluded and the police and EMS have not yet entered the premises. In addition, these kits work as a force multiplier for first responders who may not bring sufficient supplies to treat many victims, particularly tactical medics who enter with the SWAT team and are very lightly equipped.

## DETERMINING THE QUANTITY AND LOCATION OF THE HCKS

While human life is invaluable, and we cannot put a price on it, installing an unlimited number of HCKs is not

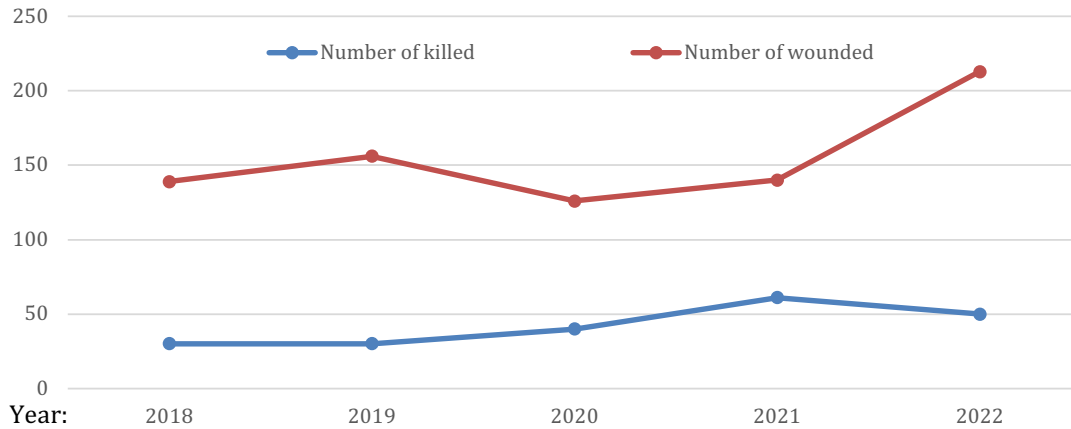


Figure 1. Incident statistics, 2018–2022

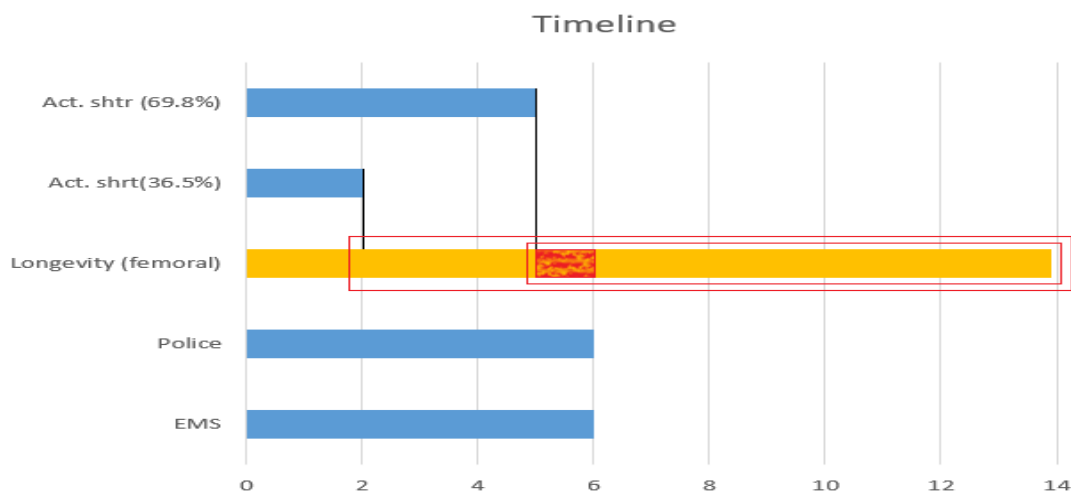


Figure 2. Window of opportunity for medical triage and improved computer simulation fidelity marked with a thin red line

practical. Besides logistics, cost is also a factor, which increases when replenishment of perishable items, such as hemostatic gauzes, is considered. Furthermore, our work shows that in specific configurations, having more HCKs may not notably change the outcome, while their placement is significant. This is why we devised a methodology for testing the effectiveness of the placement of those kits. In this paper, we focus on simulating placement in a primary or middle school environment where only the teachers can render first aid. To isolate the placement and number of kits as variables, we will control for the training component and assume all teachers are trained to respond. Furthermore, to control for the variability of injuries and the time it takes to treat them, we will measure only the time it takes to deliver a kit to a victim but will not account for the treatment time as different injury types would require different amounts of time.

To unambiguously and succinctly describe the placement of HCKs we will use a bit vector, where each bit represents a possible location for the HCKs. A bit is set to 1 if the HCK is present in that configuration and to 0 if it is not.

### CONTENTS OF THE HCK

There is a variety of first aid kits on the market. They differ not only in quality and price but also in the type of bandages and other supplies. On one end of the spectrum, they merely contain adhesive bandages and maybe gauze; on the other, they contain shearers, tourniquets, and bag valve masks. For this discussion, we consider only kits that can be used to manage severe trauma, so the kit must contain a tourniquet and hemostatic gauze. Furthermore, some jurisdictions legislate what types are acceptable for use and what their contents must be at

a minimum, such as Texas HB 496 ( 2019). The prevalent first aid kit providers are the Stop-the-Bleed campaign and the American Red Cross (ARC); of the two, Stop-the-Bleed appears to have the lead on setting standards, as even ARC offers Stop-the-Bleed kits. For this study, we are going to use the Stop-the-Bleed kits and, in particular, the wall-mounted Stop-the-Bleed basic, intermediate, and advanced stations.

**WHAT IS IN A STOP-THE-BLEED STATION?**

A wall-mount Stop-the-Bleed station type contains one portable bag containing eight kits of the station type: basic, intermediate, or advanced. Each of the kits contains a Stop-the-Bleed instructional booklet and the components listed in Table 1.

As discussed earlier, we are controlling for the type of injury and time to treat it, so for simulation purposes, it’s only necessary to simulate the delivery of one bag to the victim.

***Simulation Software Framework, Or Why We Chose AnyLogic***

For the simulation, the authors chose AnyLogic, which is excellent for agent-based computer simulations and is the de facto implementation standard within the Purdue Homeland Security Institute. The software allows the research scientist to use a wide range of primitives, implemented as libraries describing the behavior of pedestrian

agents, walls, escalators, and other components, allowing them to focus on the core logic of the simulation.

**SIMULATION METHODOLOGY**

Before we explain the simulation methodology, we’ll take a second to define the scope of the tasks clearly. Since some of the details were already covered, there may be a little overlap with previous sections.

***Simulation Methodology Scope***

This simulation models the deployment of HCKs in a building that is presumed to be a primary or middle school. As a result of those assumptions, only the teachers can provide first aid and acquire and deliver an HCK to a victim. In addition, the building has a particular layout consisting of large spaces connected through a common corridor. The test model replicated Robb Elementary School in Uvalde, Texas, but the layout can easily be swapped with any other school. As a part of the layout, the user can specify where it is feasible to mount an HCK. Those “allowed locations” are considered a constant within a simulation series; however, not all “allowed locations” will have an available HCK in different variations.

This model controls for the type of injury and treatment time, which are not factored in. The only variables introduced to a particular layout are the number of HCKs and their locations. In other words, the model will automatically try all combinations of placement of an HCK.

**Table 1.** Wall-mounted Stop-the-Bleed station types and their contents

Station type and price	Contents of single kit	Contents of station
Basic \$43.50/\$545.00	tourniquet marker 1 pair protective gloves compression bandage	8 tourniquets 8 markers 8 pairs protective gloves 8 compression bandages
Intermediate \$68.50/\$745.00	tourniquet QuikClot® bleeding control Dressing™ 3 in. x 4 yd. roll marker 1 pair of protective gloves compression bandage	8 tourniquets 8 QuikClot® bleeding control Dressing™ 3 in. x 4 yd. roll 8 markers 8 pairs protective gloves 8 compression bandages
Advanced \$83.50/\$895.00	tourniquet QuikClot® bleeding control Dressing™ 3 in. x 4 yd. roll marker 1 pair protective gloves compression bandage 1 pair 7 1/4” trauma shears 1 survival rescue blanket HALO vent chest seal, 2-pack	8 tourniquets 8 QuikClot® bleeding control Dressing™ 3 in. x 4 yd. roll 8 markers 8 pairs protective gloves 8 compression bandages 8 pairs 7 1/4” trauma shears 8 survival rescue blankets 8 HALO vent chest seals, 2-pack

### ***Simulating Walls***

The walls are implemented using the AnyLogic standard Wall primitive from the Pedestrian Library (*Pedestrian Library* | *AnyLogic Help*, 2023).

### ***Simulating Teachers***

The Teacher agent type is inherited from the AnyLogic Pedestrian agent type. The teachers can respond by finding the closest HCK and then delivering it to the closest victim. A teacher may carry a variable, predefined number of HCKs on them, which would allow for investigating the efficiency of bringing multiple kits against the possibility of depriving other responders access to them. In addition, if a responder has multiple kits on them, they will deliver the first one to the closest victim and then proceed to the next closest victim until they exhaust their HCK supply. At the beginning of the simulation, the teachers are spread around all rooms. The user controls their position using the Attractor AnyLogic primitive (*Attractor* | *AnyLogic Help*, 2023). The Teacher agent can be injured.

### ***Simulating Students***

The Student agent type is inherited from the Pedestrian AnyLogic agent type, and its instances are spread equally around different rooms. The researcher can control their position similarly to the Teacher agent type. Students do not respond to emergencies and are not a factor apart from being injured.

### ***Simulation of HCKs***

The HCK has two components to it. First is the location where it is feasible to mount one. For example, from a practical point of view, HCKs cannot be placed in the middle of a door, even though the computer may decide that this place is optimal. This is why the researcher can indicate the “allowed locations” for HCKs.

Furthermore, limiting those to a discrete set of possible locations is essential to decrease computational expenses. The experiments consist of multiple sets. Within each set, the HCK configuration does not change; however, the AnyLogic random number generator is reset, allowing for minor variability in the agent behavior. In some cases, software artifacts may cause the experiment to fail or reach the simulation limit, so we will use the median value from an experiment set to eliminate the influence of such bugs.

## **DISCUSSION**

The Stop-the-Bleed stations contain a large go-bag, which contains eight kits. In an earlier stage of this research, it was assumed that a responder would take the entire bag, but very quickly it became apparent that such

a scenario deprives other responders, who come from other directions, of the ability to take HCKs; thus, the implementation was changed to allow for a user-defined number of HCKs to be carried by a responder. Regardless, the implementation still allows for the simulation of the original behavior to allow researchers more freedom. It is speculated that taking the entire bag may benefit a relatively small number of responders; however, this will be established by future work using this model.

For this research, we simulated the deployment of three and four Stop-the-Bleed stations on the school’s first floor, assuming 10% of the population is injured. In addition, there are ten locations where a station may be mounted, and every responder would take up to three kits from each station and distribute them to victims before returning for replenishment.

There are many permutations of how HCKs can be positioned in the building. Each permutation was run (replicated) ten times to account for computer model bugs and artifacts, and the median result was chosen. In addition, the error rate was monitored; it was 5.25% for three kits, and for four kits, it was 5.29%. In addition, for each permutation, no more than one sample was discarded. Furthermore, to increase variability for each of those replications, the pseudorandom generator of the AnyLogic engine was reset with a cryptographically secure random number.

If using three kits, there are 120 possible permutations given the ten station installation locations. The time it took to distribute the kits varied between 2:09 and 4:49 minutes (see Figure 3), and most of the entries were under 3 minutes, clearly showing which configurations were not beneficial. Figure 4 shows the response times, top five and bottom five configurations.

For illustration purposes we have included a visual representation of the two worst-case scenarios (see Figure 5), known as configuration vectors 769 and 386, and contrasted them with the best ones (see Figure 6).

Looking at the examples above, it becomes apparent that better distribution of the kits creates a better outcome, which is also the intuitive conclusion. However, the power of the simulation model is that it can be applied to much more complicated layouts, including multistory buildings, and removes the human bias.

Using four kits, there are 210 permutations with similar time distributions (see Figure 7). The response time ranges between 1:30 and 4:02 minutes, and it’s interesting to note that the fastest times are significantly shorter, by 30%, while the slowest response times have decreased only by 16%. This statistic shows that merely adding an HCK is not sufficient but it also has to be optimally placed.

Apart from the numbers, the conclusions are the same. Figure 8 shows the best and worst configurations

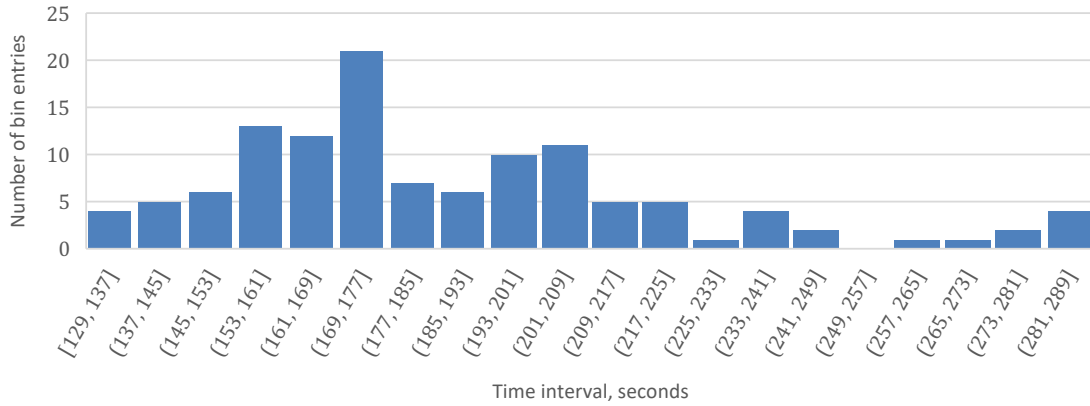


Figure 3. Response distribution time for three kits

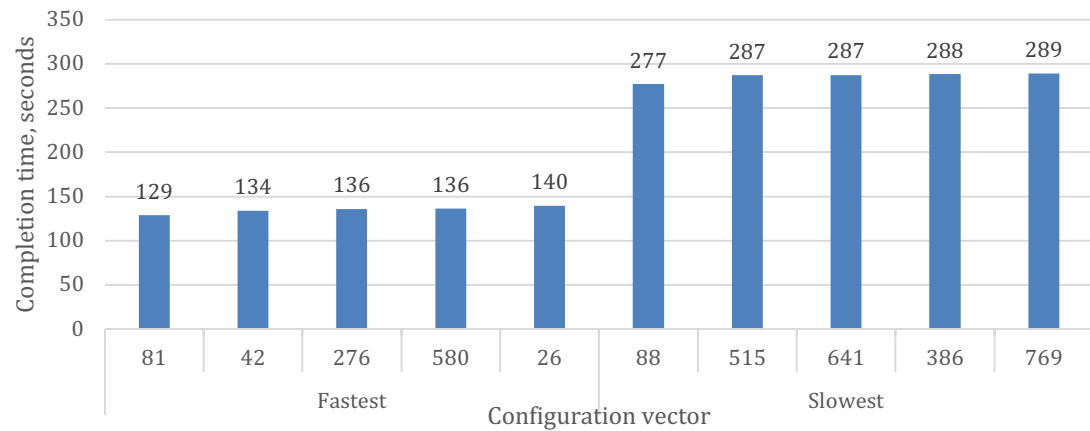


Figure 4. Top and bottom five response times by configuration vector (three kits)

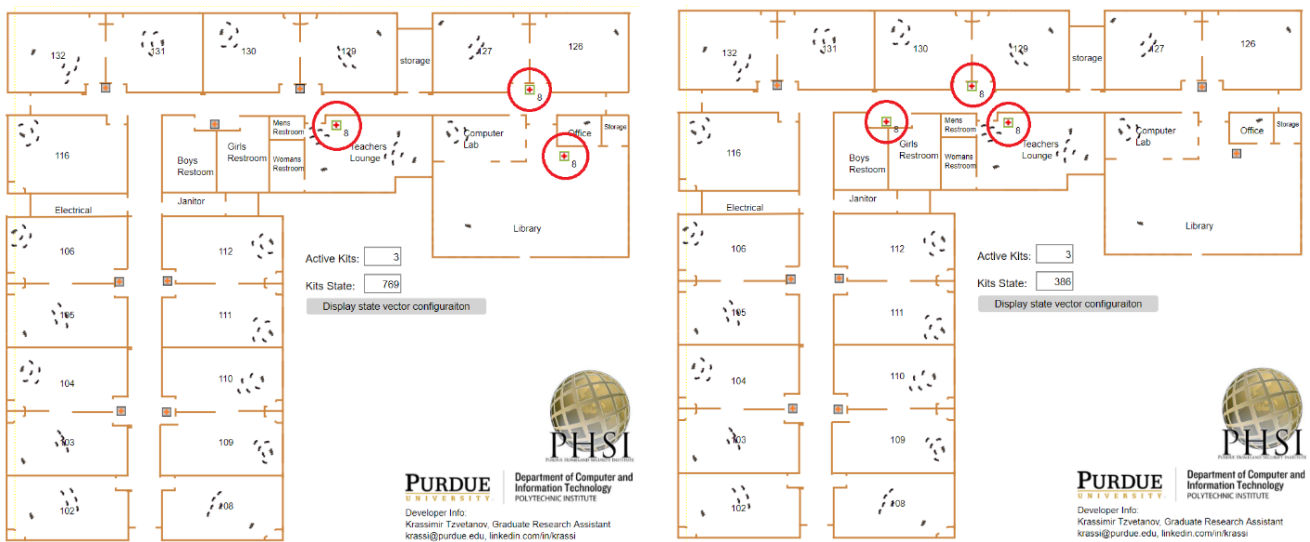


Figure 5. Least favorable configurations for three kits: configuration vectors 769 and 386

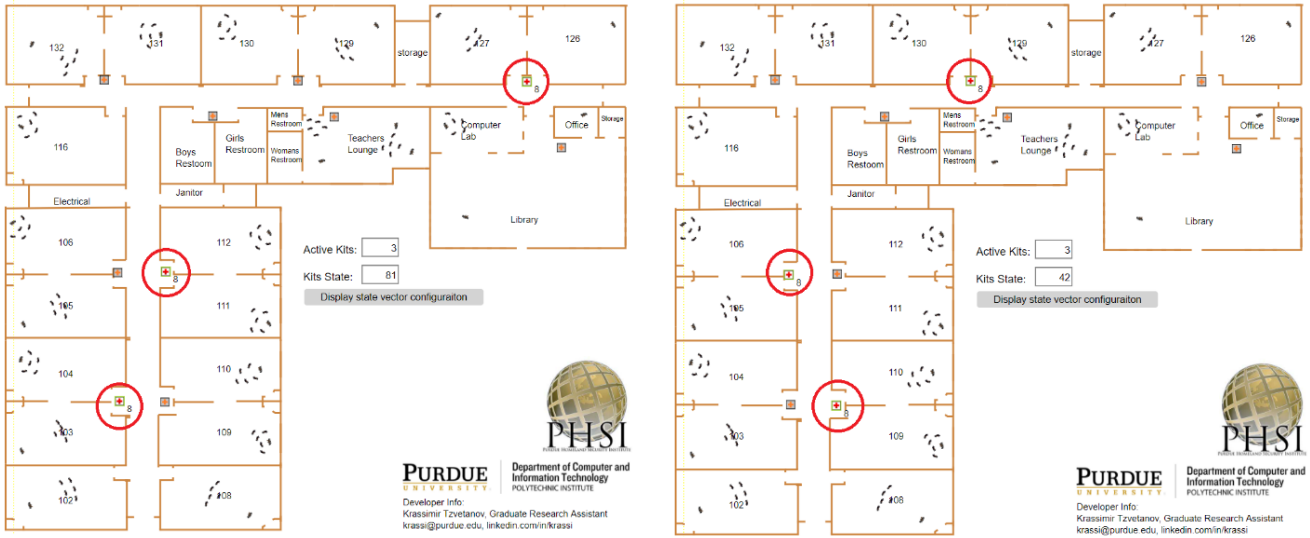


Figure 6. Most favorable configurations for three kits: configuration vectors 81 and 42

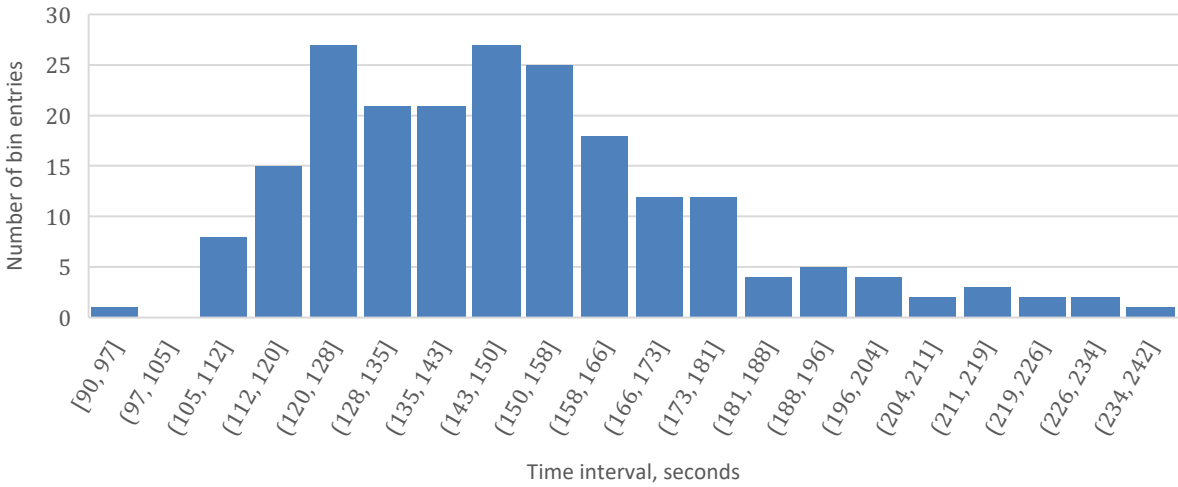


Figure 7. Response distribution time for four kits

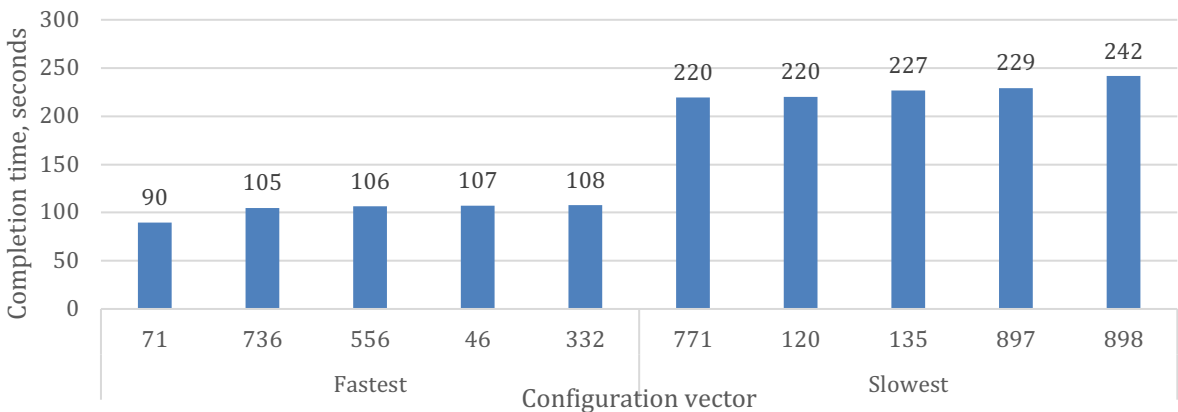


Figure 8. Top five and bottom five response times by configuration vector (four kits)

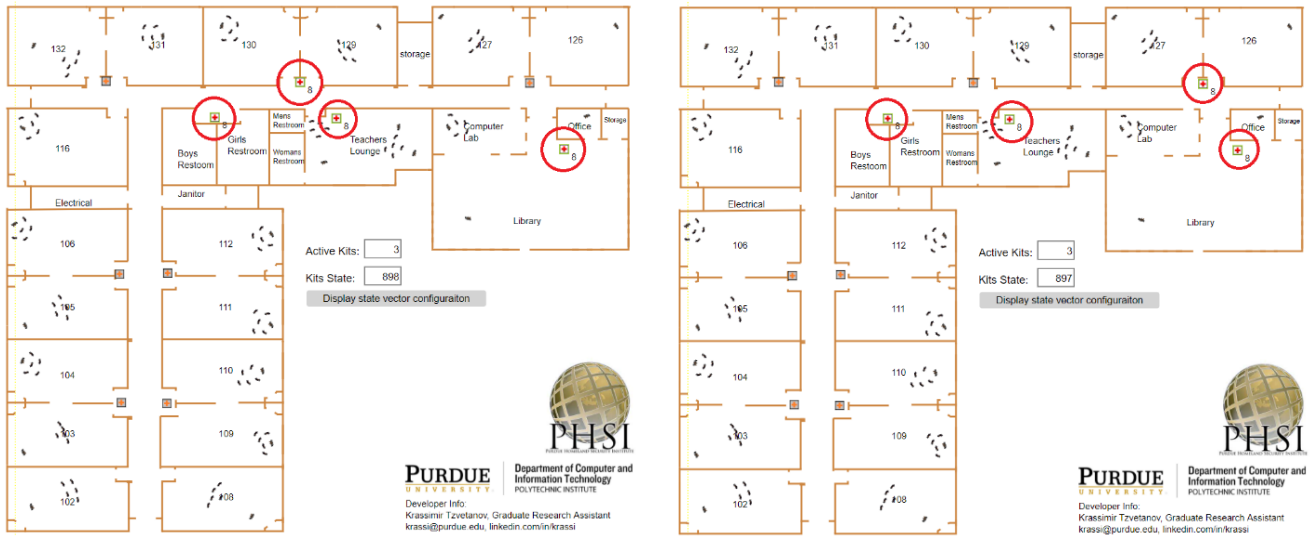


Figure 9. Least favorable configurations for three kits, configuration vectors 769 and 386

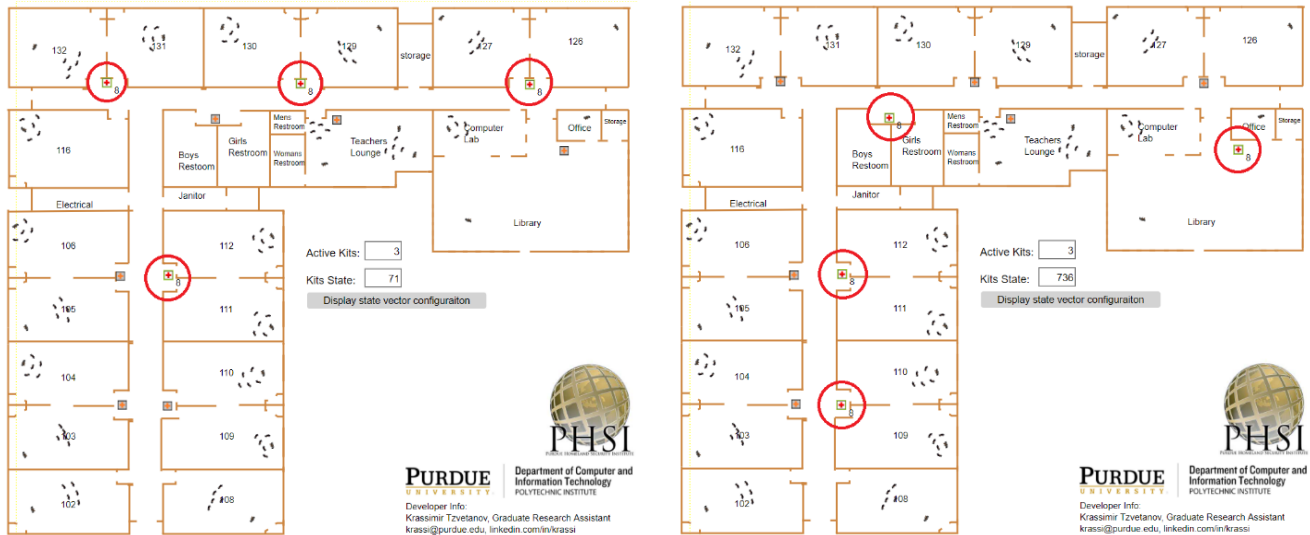


Figure 10. Most favorable configurations for three kits, configuration vectors 71 and 736

and their respective visualization (see Figure 9 and Figure 10).

### CONCLUSIONS

In this study, we demonstrated how to model the access to HCKs in a public setting, particularly in a middle school where only teachers are likely to respond to a medical emergency.

We evaluated the effects of deploying three and four HCKs and compared the results for each group and between them; the results are summarized in Table 2. The simulation reveals that regardless of the number of HCKs

deployed, there is a significant variance in the time it takes to complete their distribution to the victims, solely based on the overall deployment configuration and their optimal placement. When the kits are placed optimally, the addition of one HCK improves the performance by 30%. And when the kits are placed suboptimally, in the worst case, adding one more kit still provides 16% improvement, which confirms the obvious—having more kits improves performance. However, it appears that optimal placement has a far greater effect compared to sheer count. For this particular school layout, placing three kits optimally can cut the time in half compared to placing four kits suboptimally.



**Table 2.** Wall-mounted Stop-the-Bleed station types and their contents

Number of HCKs	Best time, min	Worst time, min
3 HCKs	2:09	4:49
4 HCKs	1:30	4:02
Improvement (one additional kit)	30%	16%

Last but not least, this model is programmed in such a way that even a person with basic AnyLogic knowledge can implement a new floor layout. Furthermore, it is possible to export the model to run independently of the AnyLogic product, allowing it to easily be used in the field.

### FUTURE WORK

While this study answers an essential question, namely quantity of HCKs versus quality of placement, it prompted a larger number of questions that can be studied using the same computer model.

One of the future research areas is to determine the effect of the percentage of qualified responders and how this percentage relates to the number of stations. Similarly, we will look at how the number of injured relates to the number of stations and responders, and will perform optimization analysis providing optimal placement and the optimal number of HCKs, as well as trained active bystanders. Similarly, it is interesting to investigate when it is more effective for a responder to take the entire go-bag with all kits in it and when it is better to take a smaller number.

While this model is portable and can be exported from AnyLogic to be used in the field, it will be good to figure out general rules for HCK placement based on the general floor layout.

Finally, we can evaluate the financial side of deploying those stations and analyze where and how it is best to allocate funds to stay within budget.

### SOURCE CODE

The simulation is published at <https://github.com/krassi/PHSI/HCK>.

### REFERENCES

Anklam, C., Kirby, A., Sharevski, F., & Dietz, J. E. (2015). Mitigating active shooter impact: Analysis for policy options based on agent/computer-based modeling. *Journal of*

*Emergency Management*, 13(3), 201–216. <https://doi.org/10.5055/jem.2015.0234>

Apgar, B., & Shoro, M. (2017, October 6). Las Vegas first responders trained extensively for mass casualty event. *Las Vegas Review-Journal*. Retrieved October 16, 2020, from <https://www.reviewjournal.com/local/the-strip/las-vegas-first-responders-trained-extensively-for-mass-casualty-event/>

Attractor | AnyLogic Help. (2023). Retrieved July 5, 2023, from <https://anylogic.help/markup/attractor.html>

Federal Bureau of Investigation. *Active shooter incidents 20-year review, 2000–2019*. (2020). <https://www.fbi.gov/file-repository/active-shooter-incidents-20-year-review-2000-2019-060121.pdf/view>

Federal Bureau of Investigation. (2021). *Active shooter incidents in the United States in 2020*. <https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2020-070121.pdf/view>

Federal Bureau of Investigation. (2022). *Active shooter incidents in the United States in 2021*. <https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2021-052422.pdf/view>

Federal Bureau of Investigation. (2023). *Active shooter incidents in the United States in 2022*. <https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2022-042623.pdf/view>

de Anda, H., Dibble, T., Schlaepfer, C., Foraker, R., & Mueller, K. (2018). A cross-sectional study of firearm injuries in emergency department patients. *Missouri Medicine*, 115(5), 456–462.

Kirby, A. M. (2016). *Comparing policy decisions for active shooters using simulation modeling*. Purdue University. <https://search.proquest.com/openview/15386d04c6d8d638949e94f179af04c6/1>

Kirby, A., Anklam, C. E., & Dietz, J. E. (2016). Active shooter mitigation for gun-free zones. In *Proceedings of the IEEE Symposium on Technologies for Homeland Security (HST)* (pp. 1–6). <https://doi.org/10.1109/THS.2016.7568957>

Lee, J. Y. (2019). *Agent-based modeling to assess the effectiveness of run hide fight* [Master's thesis, Purdue University Graduate School]. <https://doi.org/10.25394/pgs.8020763>

Lee, J. Y., Dietz, E. J., & Ostrowski, K. (2018). Agent-based modeling for casualty rate assessment of large event active shooter incidents. In *Proceedings of the 2018 Winter Simulation Conference* (pp. 2737–2746). Available at: <https://doi.org/10.1109/WSC.2018.8632535>

Pedestrian Library | AnyLogic Help (2023). Accessed July 5, 2023, from <https://www.anylogic.com/features/libraries/pedestrian-library/>

Texas HB 496. (2019). <https://capitol.texas.gov/tlodocs/86R/billtext/html/HB00496F.htm>

Tzvetanov, K. T. (2021). *Improving the fidelity of agent-based active shooter simulations through modelling bloodloss and injury management* [Master's thesis, Purdue University].

Tzvetanov, K. (2023a). *AnyLogic implementation of injury and blood loss, and hemorrhage control models in the context of*

*active shooter simulations* [Manuscript submitted for publication].

Tzvetanov, K. T. (2023b). *Modelling hemorrhage control in the context of agent-based active shooter simulations* [Manuscript submitted for publication].

Tzvetanov, K. (2023c). *Modelling injury and blood loss in the context of agent-based active shooter simulations* [Manuscript submitted for publication].

Tzvetanov, K. T., and Dietz, J. E. (2023). The need for higher fidelity active shooter simulation. In *Proceedings of the 1st Conference of the Purdue Military Research Institute Conference Proceedings*.

# A Brief History and Critique of Cybersecurity Attack Frameworks

Sayako Quinlan and Cory-Khoi Quang Nguyen

CrowdStrike

sayako.quinlan@crowdstrike.com, cory.nguyen@crowdstrike.com

**Abstract** Cybersecurity attack frameworks, which we define as “derivable and generalizable structures for describing or categorizing cybersecurity attacks,” enable a common language. However, as threat-hunting researchers, we found that popular frameworks struggle to predict new attacks or even to apply to all types of attacks. While others have also evaluated cybersecurity attack frameworks, our research objective was to document their evolution. To begin, we propose a definition and explain the levels of detail in cybersecurity attacks frameworks. Then, we walk through a brief history of select frameworks, chosen based on release date, definition eligibility, and popularity. Grouping the frameworks by decade between 1990 and 2020, our methodology looks at each framework’s origins, strengths, and weaknesses. Our analysis identifies a novel tension between the educational and implementational qualities of a framework and a consistent inability to predict novel attacks. From these findings, we propose a set of criteria for the cybersecurity community to improve future frameworks.

## INTRODUCTION

As the cybersecurity community has introduced a series of frameworks to the field for classifying, tracking, or profiling attacks, several papers have provided overviews and evaluations of the various models (Al-Mohannadi et al., 2016; Bodeau et al., 2018; Georgiadou et al., 2021; Möller, 2023; Naik, 2022). This paper attempts to document the origin and evolution of selected cybersecurity attack frameworks. Additionally, we will analyze the strengths and weaknesses of the selected attack frameworks.

We will begin by defining a “cybersecurity attack framework” and then propose a categorization schema for the levels of detail in cybersecurity attack frameworks. The paper reviews selected cybersecurity attack frameworks chronologically, investigating their origins, strengths, and weaknesses. Consequently, the takeaways from this investigation will guide and recommend improvements to future security frameworks.

## CYBERSECURITY ATTACK FRAMEWORK SELECTION METHODOLOGY

To identify the appropriate frameworks to analyze, it is important to define the term “cybersecurity attack framework” and rule out potential misconceptions. Then, we explain our selection criteria for this paper and illustrate the types of cybersecurity frameworks.

### *What Is a Cybersecurity Attack Framework?*

This paper leverages the following definition: “A cybersecurity attack framework is a derivable and generalizable

structure for describing or categorizing cybersecurity attacks, where a cybersecurity attack means real or simulated unauthorized activity on a system or in an environment, where generalizable means that the structure is meant to apply to different types of attacks, and where derivable means that there is a consistent set of rules for how to describe or categorize attacks.”

This definition is from our assessment of cybersecurity attack frameworks. The phrase “simulated unauthorized activity” was included because a cybersecurity attack framework should also be a tool for red teaming, penetration testing, and security research, which all provide significant contributions to our understanding of the threat landscape. The term “derivable” was included because we observed that the persistent goal of each framework was to systematically describe the diverse array of attack methods. Finally, the term “generalizable” highlights how each framework attempts, with varying degrees of success, to describe a wide variety of attack types or phases within the threat landscape.

### *What Is Not a Cybersecurity Attack Framework*

We would like to clarify the common models that this paper considers outside the scope of analysis.

### *Prescriptive Frameworks*

Frameworks focused on cybersecurity program development, management, or compliance are not included. These frameworks often offer prescriptive actions and go beyond the simple question, “What could or did the attacker do?” However, it is not uncommon for these prescriptive frameworks to incorporate cybersecurity

attack frameworks. For example, the process for attack simulation and threat analysis (PASTA) and NIST’s cybersecurity framework can integrate the various frameworks that we will cover, but they are not themselves cybersecurity attack frameworks (Brash, 2022; Uceda-Velez, 2012).

**Machine Learning Categorization Models**

Many research papers explore the ability for machine learning models to sort through cybersecurity attacks (Buczak and Guven, 2016; Kilincer et al., 2021; Li et al., 2019). However, these models leverage datasets labeled or categorized according to a cybersecurity attack framework or an arbitrary collection of attack terms (Alqahtani et al., 2020; Buczak and Guven, 2016; Li et al., 2019). Another application of machine learning is to determine whether data reflects malicious or benign activity (Chalé and Bastian, 2022). This is distinct from our definition because cybersecurity attack frameworks categorize only malicious activity.

**Offensive Security Tools**

Security practitioners sometimes use the term “framework” to refer to a modular attack tool. Below are some examples:

- “Empire is a post-exploitation **framework** that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent” (EmpireProject, 2020).
- “Metasploit: the world’s most used penetration testing **framework**” (Rapid7, n.d.).

The examples are practical tools utilized in the process of exploitation or an attack. However, the frameworks we discuss are theoretical tools that may coincidentally materialize as digital tools.

**Levels of Detail in Cybersecurity Attack Frameworks**

To illustrate the varying degree of technical content that can be in a cybersecurity attack framework, we provide in Figure 1 a schema categorizing the three levels of detail, inspired by the three levels of warfare (Harvey, 2021):

Some of the discussed frameworks explain attacks very technically, illustrating precisely what is occurring in terms of software and hardware. Other frameworks answer high-level questions such as an attacker’s country of origin. Frameworks can also include content from multiple levels. We include this diagram to help readers understand why two seemingly disparate frameworks, such as a high-level attack diagram and a low-level vulnerability categorization schema, deserve to be included and compared.

**How We Identified Cybersecurity Attack Frameworks**

We leveraged our professional experience and Google Scholar to identify frameworks with the following qualifications:

1. adhere to our definition of “cybersecurity attack framework,”
2. released between 1990 and 2020,
3. has more than 100 Google Scholar citations from publications referencing the framework in the first page of results for that framework sorted by relevance.

Level of Detail	Questions Answered	Content	Examples
Strategic	Who?	Adversary Attribution	Fancy Bear, APT 1, North Korea, Evil Corp
	Why?	Adversary Motive	Political/Espionage, eCrime/Financial
		Attack Tactic	Reconnaissance, Persistence
Operational	Where?	Affected Entity	Cloud, mobile, Kubernetes, a particular hostname, a particular app
	How?	Attack Technique	A vulnerable web service, logon script
Tactical	What?	Attack Procedure	An API call, a DNS request, malicious code execution

Figure 1. Levels of detail within cybersecurity frameworks

Term Used in This Paper	Other Spellings and Synonyms					
cybersecurity	cyber	cyber security	information security	infosec	system security	computer security
attack	intrusion	threat				
framework	model	method	categorization			

Figure 2. Various search term combinations used to identify relevant frameworks

Cybersecurity Attack Framework Name	Date Released	Google Scholar Results*	Levels of Detail
Attack Trees	1999	4,239 citations	Strategic, Operational, Tactical
STRIDE	2001	444 citations <sup>†</sup>	Strategic
CVSS	2004	857 citations	Operational, Tactical
CAPEC	2007	131 citations	Strategic, Operational, Tactical
Cyber Kill Chain (formerly known as Intrusion Kill Chain)	2011	1,716 citations <sup>‡</sup>	Strategic, Operational
Diamond Model of Intrusion Analysis	2013	374 citations	Strategic, Operational, Tactical
ATT&CK	2018	743 citations	Strategic, Operational, Tactical

\* We took a sum of the citation counts on June 1, 2023 for each publication confirmed to be referencing the framework in the first page of results for that framework name.

<sup>†</sup> Due to the commonality of the term “stride,” the search term used for this model was “Microsoft STRIDE”.

<sup>‡</sup> Being the model’s name in the original paper, “Intrusion Kill Chain” was the search term used.

Figure 3. Selected cybersecurity attacks frameworks and their release date, popularity, and level of detail

Although we use the term “cybersecurity attack framework,” Figure 2 outlines other synonyms and taxonomy that we included in our Google Scholar searches to identify eligible frameworks.

This paper does not intend to be a comprehensive examination of cybersecurity attack frameworks. Our goal is to sample among frameworks more familiar to the cybersecurity community. Figure 3 lists the frameworks selected for this paper.

## A BRIEF HISTORY AND CRITIQUE OF CYBERSECURITY ATTACK FRAMEWORKS

### 1990s: Bruce Schneier’s Attack Trees

In 1999, Bruce Schneier wrote an article titled “Attack Trees” (Schneier, 1999). His is likely the most popular

cybersecurity attack framework to come out of the 1990s. However, an earlier, less frequently cited paper by Schneier along with members of the NSA and DARPA also discusses attack trees (Salter et al., 1998). This earlier publication cites models from Los Alamos National Laboratory and AT&T Bell Laboratories as foundations for the framework (Smith et al., 1986; Weiss, 1991). Interestingly, Schneier’s two publications use the term “attack trees” for two different models.

### Origins

The groundwork for the 1999 attack trees article was done in the 1980s. From a federal requirement to conduct risk assessments, Suzanne T. Smith and her teammates at Los Alamos National Laboratory developed a system called LAVA, the Los Alamos Vulnerability/Risk Assessment

system. LAVA incorporated a “dynamic threat analysis” process, which implemented a decision tree (Smith et al., 1986). The decision tree branched into yes or no answers to questions about a system’s “asset attractiveness” along with a threat actor’s motivation, capability, and opportunity to carry out an attack. From the decision tree, the model calculated a “dynamic threat strength.” LAVA’s dynamic threat analysis exemplifies the desire from early on to mathematically quantify cybersecurity attacks.

Government requirements motivated Bell Labs to develop a cybersecurity attack framework as well. In 1991, J. D. Weiss published “A System Security Engineering Process,” which the organization developed to comply with the former military requirement MIL-STD-1785. As part of a security vulnerability analysis (SVA), Weiss introduced a decision tree called a threat logic tree (Weiss, 1991). The tree outlines a single attack objective using branches and leaves that represent the steps required to achieve the attack.

Fast-forwarding to 1998, Schneier and his coauthors, citing dynamic threat analysis and SVA, introduce a model that they call an attack tree (Salter et al., 1998). The attack tree begins with either a component of a system or an attack objective. The component branches into the phases of a defined “software life cycle”: design, production, deployment, operation and maintenance, and destruction. For each phase, the model outlines potential attack nodes based on either physical security or “trust model” vulnerabilities, where a trust model is “how an organization determines whom to trust with its assets” (Salter et al., 1998).

By 1999, Schneier returned to a model nearly identical to Weiss’s threat logic trees. This framework begins with “the goal as the root node and different ways of achieving that goal as leaf nodes” (Schneier, 1999). Schneier chooses to *also* call this model an attack tree, despite its clear divergence from the attack tree he wrote about a year earlier. He advocates that this attack tree, which we differentiate as the “1999 attack tree” versus the “1998 attack tree,” can assess different aspects of an attack, such as likelihood, required resources, and cost.

Although Schneier was a member of private industry at the time he proposed attack trees, the journey to his framework involved collaboration with and influence by peers and predecessors at defense agencies (NSA and DARPA), defense laboratories (Los Alamos), and defense contractors (AT&T Bell Laboratories) (Salter et al., 1998). The aforementioned frameworks emerged from the desire to model threats and vulnerabilities to a system.

#### *Strengths and Weaknesses*

The examples demonstrate the adaptability of decision trees. Each branch and leaf can represent anything the creator decides to illustrate and evaluate. However, we

begin to notice the antagonistic relationship between being easily implementable and educational. Each node teaches you only what the creator chooses. To create one of Schneier’s 1999 attack trees, one needs prior knowledge of various attack techniques. One would struggle to use attack trees to describe attack methods not already known. For this reason, it is also impossible for attack trees to predict new attack techniques.

#### **2000s: STRIDE, CVSS, and CAPEC**

After the turn of the century, government, industry, and academia developed several cybersecurity attack frameworks focused on application and software vulnerabilities. In 2001, Microsoft released the STRIDE threat model (Shostack, 2008). In 2004 and 2007, the US National Infrastructure Advisory Council (NIAC) and the Department of Homeland Security (DHS) tried to address the lack of a common language to describe attacks (Chambers and Thompson, 2004; MITRE, 2019). These frameworks helped the security community describe attacks, but the implementations were limited in scope.

#### *Origins*

Microsoft’s STRIDE model was a late arriver to frameworks inspired by threat modeling. The model reportedly had been used internally at the company since 1999 but was not published until 2001, in the first edition of the textbook *Writing Secure Code* (Shostack, 2008). STRIDE represents six threat categories: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Interestingly, the authors note that the categories integrate into a decision tree model that they call “threat trees” (LeBlanc and Howard, 2002).

While companies were developing proprietary tools and distinct threat models, some called for more standardization in security. The proposal for the common vulnerability scoring system (CVSS), a system for categorizing vulnerability severity, came from recommendations out of NIAC in 2004 (Chambers and Thompson, 2004). Before discussing CVSS, it is important to acknowledge an associated framework, the common vulnerabilities and exposures framework (CVE).

The nonprofit MITRE Corporation initially proposed CVE in 1999 under the name “common vulnerability enumeration.” At the time, MITRE described the need for a unified tracking system for software vulnerabilities. It cited precedent from the histories of the periodic table of elements and the phylogeny of bears as justifications for an initially unstructured, one-dimensional approach. By 2002, the CVE list logged more than 2,000 vulnerabilities but required only “number (also referred to as a name), description, and references” for each vulnerability (Martin et al., 2002). We do not consider CVE as a cybersecurity

attack framework because the structure does not define a method for describing or categorizing an attack.

Whereas the CVE authors intentionally did *not* want to propose a categorization framework, CVSS arose from that desire for a standardized schema. A NIAC working group, chaired by the chief executive officers of Cisco Systems and Symantec, recommended a three-part scoring system that calculated immutable, mutable, and organization-specific aspects of a vulnerability (Chambers and Thompson, 2004). After several bids to house CVSS, NIAC designated the Forum of Incident Response and Security Teams as the umbrella organization for CVSS in April 2005 (National Infrastructure Advisory Council, 2005).

Concurrently, at DHS, the National Cyber Security Division recommended a common language for what it called “attack patterns.” In a 2005 presentation on software assurance, the DHS director for software assurance Joe Jarzombek introduced the common attack pattern enumeration and classification (CAPEC) framework (Jarzombek, 2005). DHS released CAPEC in 2007 with a documented schema and a list of categorized attack patterns (Barnum, 2008; MITRE, 2007). The schema included 33 required and suggested components of an attack, such as “typical severity,” “attack motivation-consequences,” and “attack prerequisites” (Barnum, 2008). Now, MITRE manages CAPEC, which included 38 category groups and 559 attack patterns as of May 2023 (MITRE, 2021, 2023a).

#### *Strengths and Weaknesses*

STRIDE, CVSS, and CAPEC demonstrate the educational and implementation potential of frameworks. Microsoft’s STRIDE model provided defined operational impacts of attacks, from which professionals could learn and research more technical details. CAPEC is a thorough catalog that systematically explains attacks at a tactical level. Meanwhile, CVSS gained industry-wide adoption and is still used today (Scarfone and Mell, 2009).

However, none of the three frameworks is both implementable *and* educational. STRIDE, with only six categories of attacks, does not comprehensively include or characterize attacks. Although STRIDE may anticipate the motive or impact of undiscovered attacks, it cannot predict more technical details. CAPEC, on the other hand, is too descriptive and inclusive. MITRE has tried to address the difficulty of navigating CAPEC with a “Helpful Views,” section but we found those overwhelming (MITRE, 2021). CVSS, although successful, includes only attack techniques that involve vulnerabilities. Both CVSS and CAPEC track attacks reactively.

#### **2010s: Cyber Kill Chain, Diamond Model, and ATT&CK**

The decade of 2010 to 2020 marked a period of significant progress in cybersecurity attack frameworks. In

2011, Lockheed Martin released its Cyber Kill Chain (CKC) (Hutchins et al., 2011). Two years later, a nonprofit organization published its diamond model, and MITRE began work on the ATT&CK framework (Caltagirone et al., 2013; Strom et al., 2018). A decade later, CKC, the diamond model, and ATT&CK remain popular cybersecurity attack frameworks.

#### *Origins*

As the cybersecurity community began to investigate and document complex cybersecurity attacks, organizations had to develop new frameworks. In 2011, Lockheed Martin introduced the Intrusion Kill Chain model, which the company later rebranded to CKC (Hutchins et al., 2011; Lockheed Martin, n.d.). The paper cited forebears from military doctrine such as the US Department of Defense’s kill chain and the US Army’s terrorist operational planning cycle. The authors also referenced cybersecurity firm Mandiant’s “exploitation life cycle” from 2010 (Hutchins et al., 2011; Mandiant, 2010). Mandiant outlined a similarly structured “attack lifecycle” in its famous APT1 report released in 2004 (Mandiant, 2004). Figure 4 is a comparison of the languages used in Mandiant’s two life cycles and Lockheed Martin’s CKC.

The CKC authors argue that their model differed in that “the Mandiant model . . . does not map courses of defensive action and is based on post-compromise actions” (Hutchins et al., 2011). Of the three, Lockheed Martin’s CKC emerged as the most popular framework, based on our citation count analysis.

In 2013, the Center for Cyber Intelligence Analysis and Threat Research released its diamond model of intrusion analysis. The diamond model illustrates the relationship between the adversary, capability, infrastructure, and victim of an attack. With the diamond model, the authors hoped to address how “defenders lacked the models and frameworks for activity documentation, synthesis, and correlation necessary to answer a question of growing importance: will the adversary return as part of a coordinated campaign?” (Caltagirone et al., 2013). Similar to the authors of CKC, the diamond model authors were keen to establish a model that accounted for the defense of a network.

That same year, MITRE began work on ATT&CK. MITRE developed the framework, the company noted, “out of a need to systematically categorize adversary behavior as part of conducting structured adversary emulation exercises.” ATT&CK describes and categorizes various attack methods based on tactics, techniques, subtechniques, and procedures. For techniques and subtechniques, MITRE has a defined object structure that includes information such as platform, permissions required, and impact type, needed to systematically describe each method.

Model Name	Phases						
Attack Lifecycle, Mandiant 2004	Initial Compromise	Establish Foothold	Escalate Privileges	Internal Reconnaissance	Move Laterally	Maintain Presence	Complete Mission
Exploitation Life Cycle, Mandiant 2010	Reconnaissance	Initial Intrusion	Establish a Backdoor into the Network	Install Various Utilities	Privilege Escalation / Lateral Movement / Data Exfiltration	Maintain Presence	
Cyber Kill Chain, Lockheed Martin 2011	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control (C2)	Actions on Objectives

**Figure 4.** A comparison of the difference phase taxonomy between Mandiant’s 2004 attack lifecycle and 2010 exploitation life cycle and Lockheed Martin’s Cyber Kill Chain

MITRE also maintains ATT&CK matrices, which visualize the tactics, techniques, and subtechniques in a table (Strom et al., 2018). Initially, ATT&CK, published in 2018, focused on attacks against Windows enterprise environments, but as of 2023, there are several ATT&CK matrices, including PRE-ATT&CK, enterprise, mobile, cloud, and industrial controls systems (Strom et al., 2018).

CKC, the diamond model, and the ATT&CK framework revolutionized how the cybersecurity community speaks and writes about attacks. CKC is an example of how the private sector can release a universally accepted framework. It is rivaled only by ATT&CK, the influential culmination of decades of cybersecurity attack framework programs by MITRE. Meanwhile, the diamond model continues to appear in cybersecurity curricula, conference presentations, and academic papers (Ertaul and Mousa, 2018; Peers, 2019; SANS, n.d.).

#### Strengths and Weaknesses

CKC, the diamond model, and ATT&CK are arguably the most robust cybersecurity attack frameworks the community has to date. CKC and ATT&CK have enabled cybersecurity professionals to use similar terminology for different types of attacks. The ATT&CK website operates as an educational resource and database for threat actor activity. Like the CVE program, ATT&CK helps standardize how various vendors label attacks. The diamond model, which can integrate with either CKC or ATT&CK, has the advantage of flexibility. The diamond model is also more systematically descriptive than earlier decision tree models, where each node could be any feature an analyst chooses.

However, these models still have unique weaknesses. CKC’s rigid chronology does not match how some intrusions unfold in actuality. ATT&CK, although

more inclusive than CKC, struggles with categorization and scalability. An ATT&CK technique can apply to multiple tactics but miss another tactic. For example, MITRE categorizes DLL side-loading as persistence, privilege escalation, and defense evasion but not as execution. However, MITRE states, “Adversaries may **execute** their own malicious payloads by side-loading DLLs” in the attack’s description (MITRE, 2023b). The expansion and multiplication of matrices raises the question, “Are more matrices the best solution?” Like decision trees, the diamond model suffers from the lack of a technical schema. It *relies* on a CKC or an ATT&CK to provide that function. Last, these frameworks, especially ATT&CK, are reactive. ATT&CK only documents or categorizes an attack once researchers or hackers publicize the method (MITRE, n.d.).

#### FUTURE IMPROVEMENTS

Throughout this analysis, we have seen recurring issues. Educational frameworks that provide users with descriptive categories are rigid. Flexible frameworks that can easily apply to a wide variety of attacks require users to bring their own taxonomy. Ideally, we want a framework that can describe attacks consistently while also adapting to an evolving threat landscape. Finally, as researchers in the threat-hunting field, we long for a framework that can *anticipate* future attack methods, much like how the periodic table of elements predicted the existence of undiscovered chemicals (McFarland, 2019). Therefore, we suggest the following criteria for future improvements and proposals to cybersecurity attack frameworks:

1. The framework must be derivable. The model must consistently describe or categorize attacks, based on a set of rules.



2. The framework must be scalable. The model should adapt to a growing cybersecurity attack landscape.
3. The framework must be predictable. The model should proactively identify potential attack methods.

## ACKNOWLEDGMENTS

We would like to thank Victoria Galvan for her assistance in reviewing works similar to this paper. We would also like to thank Victoria, David Zawdie, Joel Mehler, Rob Herzog, and Rob Ogorek for their feedback during the revision process of this paper.

## REFERENCES

- Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016). Cyber-attack modeling analysis techniques: An overview (pp. 69–76). In *Proceedings of the IEEE 4th International Conference on Future Internet of Things and Cloud Workshops*, Vienna, Austria.
- Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. Md., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques (pp. 121–131). In N. Chaubey, S. Parikh, & K. Amin (Eds.), *Computing science, communication and security*, Springer. doi:10.1007/978-981-15-6648-6\_10
- Barnum, S. (2008). *Common attack pattern enumeration and classification (CAPEC) schema description*. [https://capec.mitre.org/documents/documentation/CAPEC\\_Schema\\_Description\\_v1.3.pdf](https://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1.3.pdf)
- Bodeau, D., Fox, D. B., & McCollum, C. D. (2018). *Cyber threat modeling: Survey, assessment, and representative framework*. <https://apps.dtic.mil/sti/pdfs/AD1108051.pdf>
- Brash, R. (2022). *MITRE ATT&CK vs. NIST CSF*. Retrieved June 1, 2023, from <https://verveindustrial.com/resources/blog/mitre-attck-vs-nist-csf/>
- Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. doi:10.1109/COMST.2015.2494502
- Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis*. <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>
- Chalé, M., & Bastian, N. D. (2022). Generating realistic cyber data for training and evaluating machine learning classifiers for network intrusion detection systems. *Expert Systems with Applications*, 207, 117936. doi:10.1016/j.eswa.2022.117936
- Chambers, J. T., & Thompson, J. W. (2004). Common vulnerability scoring system: final report recommendations by the council. <https://www.cisa.gov/sites/default/files/publications/niac-common-vulnerability-scoring-final-report-10-12-04-508.pdf>
- EmpireProject. (2020). *Empire*. Retrieved June 1, 2023, from <https://github.com/EmpireProject/Empire>
- Ertaul, L., & Mousa, M. (2018). Applying the kill chain and diamond models to Microsoft advanced threat analytics [Conference presentation]. International Conference on Security and Management, Las Vegas, NV. Retrieved June 5, 2023, from <http://borg.csueastbay.edu/~lertaul/SAM9723.pdf>
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK risk using a cyber-security culture framework. *Sensors*, 21(9), 3267, doi:10.3390/s21093267
- Harvey, A. S. (2021). The levels of war as levels of analysis. *Military Review*, November–December, 76.
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>
- Jarzombek, J. (2005). *Software assurance: A strategic initiative of the U.S. Department of Homeland Security to promote integrity, security, and reliability in software*. [https://csrc.nist.gov/CSRC/media/Events/ISPAB-MARCH-2006-MEETING/documents/Software\\_Assurance\\_Session-Mar2006.pdf](https://csrc.nist.gov/CSRC/media/Events/ISPAB-MARCH-2006-MEETING/documents/Software_Assurance_Session-Mar2006.pdf)
- Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*, 188, 107840. doi:10.1016/j.comnet.2021.107840
- LeBlanc, D., & Howard, M. (2002). *Writing secure code*. Microsoft Press.
- Li, M., Zheng, R., Liu, L., & Yang, P. (2019). Extraction of threat actions from threat-related articles using multi-label machine learning classification method (pp. 428–431). In *2nd International Conference on Safety Produce Informatization*. doi:10.1109/IICSPI48186.2019.9095885
- Lockheed Martin. (n.d.). *Cyber Kill Chain*. Retrieved June 5, 2023, from <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>
- Mandiant. (2004). *APT1: Exposing one of China's cyber espionage units*. <https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf>
- Mandiant. (2010). *M-Trends: The advanced persistent threat*. <https://www.christiandve.com/wp-content/uploads/2018/05/M-Trends.pdf>
- Martin, R., Christey, S., & Baker, D. (2002). *A progress report on the CVE initiative*. Retrieved June 4, 2023, [https://cve.mitre.org/docs/docs-2002/prog-rpt\\_06-02/index.html](https://cve.mitre.org/docs/docs-2002/prog-rpt_06-02/index.html)
- McFarland, B. (2019). *Predicting the past with the periodic table*. Retrieved June 5, 2023, from <https://blog.oup.com/2019/05/predicting-past-periodic-table/>
- MITRE. (n.d.). *Contribute*. Retrieved June 5, 2023, from <https://attack.mitre.org/resources/contribute/>
- MITRE. (2007). *capec\_v1.0.xml*. Retrieved June 4, 2023, from [https://capec.mitre.org/data/xml/capec\\_v1.0.xml](https://capec.mitre.org/data/xml/capec_v1.0.xml)
- MITRE. (2019). *About CAPEC*. Retrieved June 4, 2023, from <https://capec.mitre.org/about/index.html>
- MITRE. (2021). *CAPEC list version 3.9*. Retrieved June 4, 2023, from <https://capec.mitre.org/data/index.html>

- MITRE. (2023a). *Schema documentation. Schema version 3.5*. Retrieved June 4, 2023, from [https://capec.mitre.org/documents/schema/schema\\_v3.5.html](https://capec.mitre.org/documents/schema/schema_v3.5.html)
- MITRE. (2023b). *Hijack execution flow: DLL side-loading*. Retrieved June 4, 2023, from <https://attack.mitre.org/techniques/T1574/002/>
- Möller, D. P. F. (2023). Cyberattacker profiles, cyberattack models and scenarios, and cybersecurity ontology (pp. 181–229). In S. Jajodia (Ed.), *Guide to cybersecurity in digital transformation*. Springer.
- Naik, N., Jenkins, P., Grace, P., & Song, J. (2022). Comparing attack models for IT systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK framework and diamond model (pp. 1–7). In *IEEE International Symposium on Systems Engineering (ISSE)*. doi:10.1109/ISSE54508.2022.10005490
- National Infrastructure Advisory Council. (2005). *NIAC quarterly business meeting minutes - April 12, 2005*. Retrieved June 4, 2023, from <https://www.cisa.gov/sites/default/files/publications/niac-qbm-minutes-04-12-05-508.pdf>
- Peers, D. (2019). *Cyber kill chains, diamond models and analysis methods. Understanding how intelligence works*. [https://owasp.org/www-chapter-dorset/assets/presentations/2019-04/Cyber\\_Kill\\_Chains-11-Apr-19-OWASP-Dorset.pdf](https://owasp.org/www-chapter-dorset/assets/presentations/2019-04/Cyber_Kill_Chains-11-Apr-19-OWASP-Dorset.pdf)
- Rapid7. (n.d.). *Metasploit | Penetration Testing Software | Pen Testing Security*. Retrieved June 1, 2023, from <https://www.metasploit.com/>
- Salter, C., Saydjari, O. S., Schneier, B., & Wallner, J. (1998). *Toward a secure system engineering methodology*. <https://www.schneier.com/wp-content/uploads/2016/02/paper-secure-methodology.pdf>
- SANS. (n.d.). *FOR578: Cyber threat intelligence*. Retrieved June 5, 2023, from <https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/>
- Scarfone, K., & Mell, P. (2009). An analysis of CVSS version 2 vulnerability scoring (pp. 516–525). In *3rd International Symposium on Empirical Software Engineering and Measurement*. doi:10.1109/ESEM.2009.5314220
- Schneier, B. (1999). Attack trees. *Dr. Dobbs's Journal*, 24 (12).
- Shostack, A. (2008). *Experiences threat modeling at Microsoft* [Paper presentation]. MODSEC@MoDELS. <http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-413/paper12.pdf>
- Smith, S. T., Lim, J. J., Phillips, J. R., Tisinger, R. M., Brown, D. C., & Fitzgerald, P. D. (1986). *LAVA: A conceptual framework for automated risk analysis* [Conference presentation]. Annual Meeting of the Society for Risk Analysis, Boston. Retrieved from <https://digital.library.unt.edu/ark:/67531/metadc1195396/>
- Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). *MITRE ATT&CK®: Design and Philosophy*. <https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf>
- UcedaVelez, T. (2012). *Real world threat modeling using the PASTA methodology*. [https://owasp.org/www-pdf-archive/AppSecEU2012\\_PASTA.pdf](https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf)
- Weiss, J. D. (1991). A system security engineering process (pp. 572–581). In *Proceedings of the 14th National Computer Security Conference*, National Institute of Standards and Technology/National Computer Security Center, Washington, DC.

# Quantum Circuit Reduction Using Three-Layer Transposition

Christian L. Grauberger  
christian.grauberger@afit.edu

Laurence D. Merkle and Leleia Hsia  
Air Force Institute of Technology, Department of Electrical and Computer Engineering  
laurence.merkle@afit.edu, leleia.hsia@afit.edu

**Abstract** The potential for quantum computing to revolutionize critical military applications has led the US Department of Defense to recognize it as a keen interest. However, the practical implementation of these theoretical applications on physical quantum devices is limited by inherent reliability and accuracy issues in quantum hardware. To mitigate errors stemming from these limitations, the incorporation of software-based solutions is imperative. Quantum circuit optimization stands out as a primary method for increasing the accuracy of quantum computations. One of the key components of this approach is circuit reduction, whereby circuits are condensed to realize the same computation using fewer operations. State-of-the-art reduction schemes include the use of template matching to identify and reduce portions of a circuit. This paper presents an algorithmic approach to quantum circuit reduction that uses layer transposition to achieve greater reductions than state-of-the-art methods. Specifically, it focuses on those transpositions of a single layer with either the preceding or the following pair of layers within a subcircuit that preserve the effect of the subcircuit. Upon executing the transposition operation and revealing a new, equivalent circuit, conventional template matching techniques are employed to identify reductions that were previously undetected. Thus, improved accuracy of quantum computations can be achieved over current state-of-the-art methods.

## INTRODUCTION

Quantum computing is an emerging and quickly growing field of computation that has a wide range of promising applications in optimization, cryptography, communications, and many other important fields. The potential of quantum computing to revolutionize fields related to military applications has led the US Department of Defense to identify it as an Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) critical technology area (OUSD(R&E), 2023). Despite promising work proving the existence of quantum algorithms that can further these fields, such as Shor’s algorithm, the practical implementations of these theoretical approaches are limited by inherent reliability issues in quantum hardware (IBM Quantum, 2021).

IBM state-of-the-art quantum devices can perform single-qubit operations with error rates of around 0.0015 and two-qubit operations with error rates of about 0.009 (IBM Quantum, 2023). Unfortunately, quantum programs of practical interest contain large numbers of operations, each of which must be performed accurately for the overall computation to succeed. As such, these programs are unlikely to produce accurate results without error correcting measures.

One approach to error mitigation is reducing the number of operations needed to achieve the same

functionality (Fösel et al., 2021). Many existing state-of-the-art optimization techniques work toward this goal. However, recent research has shown the existence of potential reductions not considered by these existing techniques (Cole, 2021). Specifically, subcircuits exist in which a layer may be transposed with either the preceding or the following pair of layers without altering functionality, thereby exposing additional potential reductions. Current research aims to develop an efficient method to realize these potential reductions by identifying such subcircuits within a larger circuit. While it is expected that the number of realizable reductions typically will be relatively small, considering the limited number of applicable cases, the algorithm will still offer significant value in situations where achieving maximum optimization is crucial.

## BACKGROUND

This section provides a brief introduction to the basics of quantum circuits, existing optimization methods, and layer commutation.

### Quantum Circuits

Instead of operating on bits that have states of either 1 or 0, a quantum computer operates on qubits, for which the states are unit-length linear combinations of its basis vectors,  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  and  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ . The ket notation (e.g.,

$|0\rangle$  and  $|1\rangle$ ) is the standard quantum mechanical notation for a vector. Thus, a qubit state is represented as  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ , where  $|\alpha|^2 + |\beta|^2 = 1$ .

A quantum gate is an operation performed on one or more qubits. Every quantum gate is represented by a unitary matrix, and the dimensions of the matrix depend on the number of qubits on which the gate operates. The vector resulting from multiplying the gate matrix by the state vector represents the resulting state of the system following the gate operation. Matrices of a few types of quantum gate operations are shown in Figure 1.

Such gates are combined to form a quantum circuit. Software development kits such as Qiskit have been developed to encode quantum circuits, which are often depicted using quantum circuit diagrams (Qiskit, 2023).

Figure 2 shows a simple example of a quantum circuit diagram. The upper three horizontal lines each represent a qubit, labeled  $q_0$  through  $q_2$ . The remaining (double) horizontal lines represent classical bits used for capturing the value from a measurement operation on a qubit. While all aspects of the diagram are necessary for an operational quantum circuit, this paper will focus primarily on the section labeled “Quantum Gates.”

In a quantum circuit, a layer is defined as a set of gates that are specified to be concurrently executable (Qiskit, 2023). The overall effect of the gates in a single layer can be expressed as the tensor product of the matrices of the individual gates in the layer, and the unitary matrix representing the entire circuit can be calculated by computing the product of all layers. This property is useful, as two circuits that are represented by the same matrix are equivalent.

$$\begin{matrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} & \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ \text{Pauli-X gate} & \text{CNOT gate} & \text{Hadamard Gate} \end{matrix}$$

Figure 1. Quantum gate matrices

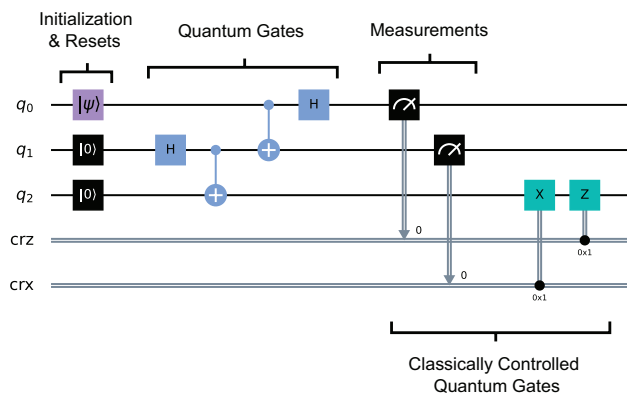


Figure 2. Example quantum circuit diagram (Qiskit, 2023)

### Qiskit Software and IBM Quantum Experience

Qiskit is an open-source software development kit for creating, modifying, and simulating quantum circuits (Qiskit, 2023). Qiskit works, for example, in conjunction with IBM Quantum Experience to run and evaluate circuits on physical quantum devices (IBM Quantum, 2023). The library features many circuit optimization techniques grouped into four optimization levels. Level 0 does no optimizations, while levels 1, 2, and 3 perform light, medium, and heavy optimizations, respectively. The ability to execute circuits on IBM quantum devices and the varying optimization levels led to the selection of Qiskit as the primary software for algorithm development for this research.

### Quantum Circuit Reductions and Template Matching

Like sequences of bit operations, an operation followed by its inverse can be removed from the circuit, provided that the intermediate value is not used elsewhere. For example, consider a circuit consisting of two consecutive Pauli-X gates on the same qubit. A Pauli-X gate, depicted in Figure 1 and commonly referred to as an X-gate, is comparable to a NOT operation on a classical bit. As a NOT operation inverts the value of a bit, the X-gate exchanges the basis state amplitudes of a qubit, taking  $|0\rangle$  to  $|1\rangle$  and vice versa. Performing this operation twice in succession results in the starting state, so these operations can be removed without altering the functionality of the circuit.

More complex reductions are achievable by generalizing this idea through template matching. There are two primary approaches to template matching. The first approach uses identity templates, which are circuits that implement the identity operator (Abdessaied et al., 2013). The identity operator has no effect on the quantum state, so adding an identity template to an existing circuit does not alter its functionality. Figure 3 shows an example of an identity template using CNOT gates. For this example, if we represent the operations of the five layers by the matrices  $L_1, L_2, \dots, L_5$  (right to left), then the overall effect of the template is

$$L_1 L_2 L_3 L_4 L_5 = I,$$

where  $I$  is the identity matrix.

This property can be used to reduce the number of gates in a circuit. If a segment of an identity template

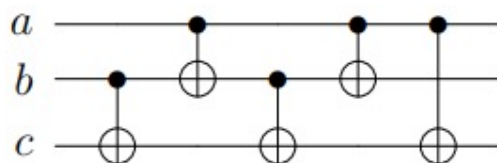


Figure 3. Example identity template (Cole, 2021)

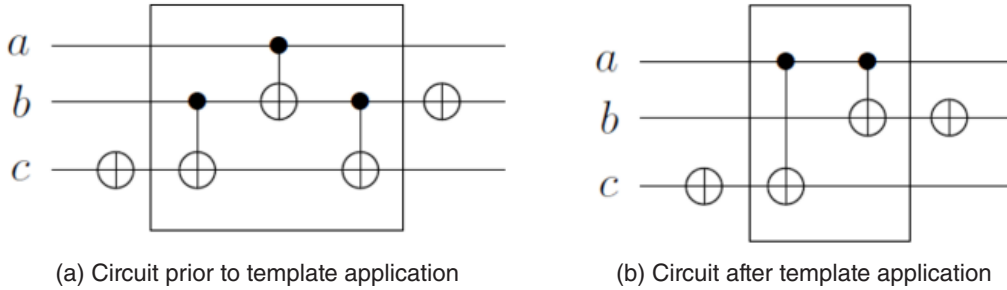


Figure 4. Application of identity template (Cole, 2021)

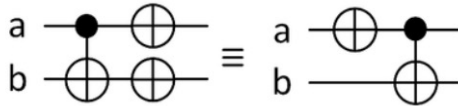


Figure 5. Example library template

containing more than half of the template’s gates is found within a circuit, the segment can be replaced with the inverse of the remaining gates in the identity template, resulting in fewer gates realizing the same functionality. Returning to the previous example, we have  $L_1L_2L_3 = IL_5^{-1}L_4^{-1} = L_5L_4$ , where we have used the facts that  $L_4$  and  $L_5$  are their own inverses. Thus, Figure 4 shows an application of the above template.

The second approach to template matching involves the use of library templates. A library template consists of two circuits that have different operation counts but achieve the same functionality. When analyzing circuits that contain the more expensive template circuit, it is possible to replace the portion corresponding to the more expensive circuit with the less expensive circuit from the library template. This replacement effectively reduces the operation count of the original circuit. Figure 5 shows a simple example of a library template.

### Layer Transposition

The property of equivalent circuits having identical matrices can be used to determine whether layers in a circuit are commutable. Certain layers are commutable if the layers can be reordered without affecting the matrix representation of the circuit. Figure 6 shows the process

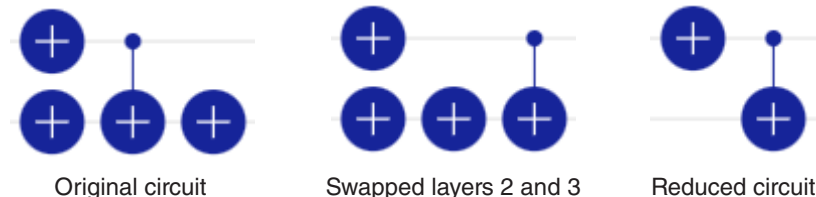


Figure 6. Equivalent circuits with two-layer commutation

of two-layer transposition and circuit reduction on a three-layer circuit.

Current state-of-the-art optimization algorithms are capable of identifying and using pairwise commutes. Further research has proposed the idea and proven the existence of commuting three-layer circuits, in the sense that a single layer commutes with the composition of either the preceding or succeeding pair of layers (Cole, 2021). Here, we are interested only in circuits that contain three layers that are not pairwise commutable but rather must be commuted in pairs. These commutes follow the form of  $L_1L_2L_3 = L_3L_1L_2$  or  $L_1L_2L_3 = L_2L_3L_1$ , where  $L_{1-3}$  represent the layers in the circuit. This research yielded an exhaustive library of 3-, 4-, and 5-qubit circuits following these criteria. The library uses the NCT gate library, which consists of NOT (called X above), CNOT, and Toffoli (CNOT with two control qubits) gates (Handique and Sonkar, 2018).

### ALGORITHM DESIGN METHODOLOGY

The objective of this research is to develop an algorithm that uses the three-layer commuting library and investigates its impact on circuit reduction. The algorithm focuses on templates involving three qubits and consists of three main stages: identification of 3-qubit blocks, template matching using the three-layer commuting library, and application of existing reduction schemes.

The first step is to identify 3-qubit blocks within a circuit. A 3-qubit block is a subcircuit consisting of three or more layers in which operations are constrained to

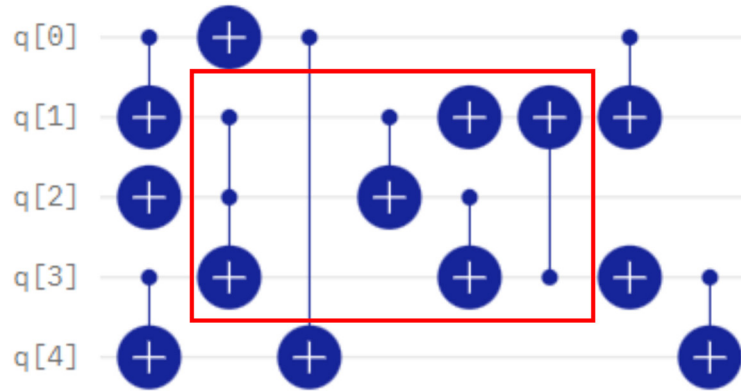


Figure 7. 3-qubit block

be within a set of three qubits. An example of a 3-qubit block with four layers is shown in Figure 7. It is important to note, however, that the qubits involved in the block do not need to be adjacent within the circuit diagram.

This portion of the algorithm is adapted from the Qiskit library’s `Collect2qBlocks` function, which identifies 2-qubit blocks within a circuit (Qiskit, 2023).

Once a 3-qubit block has been identified, a template matching algorithm is used to search the block for sub-circuits contained within the three-layer commuting library. The algorithm for this search is a modified version of the Qiskit library’s `TemplateOptimization` function, adapted to work with the template library (Qiskit, 2023). If a match is found, the original circuit is temporarily stored, and the replacement is made.

The new circuit is then optimized using Qiskit optimization level 3. If the optimization process finds a

possible reduction, the reduced circuit will be saved as the original, and the process will be repeated. If no reduction is found, the original circuit will be restored, and the template matching process will continue until all 3-qubit blocks have been explored. It is important to note that once a replacement from the template library has been made, the template matching process will not continue until a reduction is made or the original circuit is restored. This will prevent recursive substitutions that would otherwise lead to infinite loops. Algorithm 1 provides high-level pseudocode for the proposed algorithm.

### TESTING METHODOLOGY

The testing methodology for this algorithm will involve two components. The initial component will focus on assessing the algorithm’s functionality in accurately

---

#### Algorithm 1 3-Layer Commuting Circuit Optimization

---

**Require:** Input circuit, fully optimized by state-of-the-art methods

- 1:  $3q\_blocks \leftarrow$  3-qubit blocks in circuit
  - 2: **for** block in  $3q\_blocks$  **do**
  - 3:   apply template matching to block
  - 4:   **if** match is found **then**
  - 5:      $new\_circuit \leftarrow$  circuit with substitution
  - 6:     apply level 3 optimization
  - 7:     **if** reduction is found **then**
  - 8:        $circuit \leftarrow new\_circuit$
  - 9:        $3q\_blocks \leftarrow$  3-qubit blocks in updated circuit
  - 10:    **end if**
  - 11:   **end if**
  - 12: **end for**
  - 13: **return** circuit
-

identifying 3-qubit blocks and performing template matching. To achieve this, a comprehensive set of test cases will be designed to cover various scenarios. These scenarios will encompass 3-qubit blocks with nonadjacent qubits, multiple instances of 3-qubit blocks, situations where templates are absent, situations where multiple templates are present, as well as both cases where reductions are possible and where they are not.

Once the algorithm's functionality has been verified, the algorithm's effectiveness will be measured. This component will involve exhaustively testing the set of five-layer circuits for which layers  $L_2$  through  $L_4$  consist of a template from the three-layer commuting library. For each of the 12 reduced templates in the library, all possible combinations of  $L_1$  and  $L_5$  will be tested. Using the NCT library, there are 22 possible 3-qubit layers. This results in  $12 \cdot 22^2 = 5,808$  circuits in the test set.

Before running the algorithm on each of these circuits, the circuit will be optimized using optimization levels 1, 2, and 3 as a baseline for comparison. Performance measures regarding these optimizations, such as the final gate count, specific gate count, and circuit depth, will be reported. The circuit will then be optimized by the proposed three-layer commuting algorithm and the performance measures will be reported. Validation checks will be put in place to ensure the resulting circuit is equivalent to the original circuit. Each unique generated circuit will be run for "multiple iterations, each containing multiple shots, on an IBM Falcon quantum processor to evaluate performance measures such as error rate and execution time.

The testing process serves two primary purposes. The first purpose is to act as proof of concept. The existence of a circuit in the test cases that is reduced by the proposed algorithm further than by Qiskit's optimization process shows that the algorithm is capable of revealing reductions that were not previously seen. Assuming this is the case, the second purpose of the testing process is to investigate the extent to which the algorithm is useful for circuit reduction.

## CONCLUSION

The optimization technique suggested in this research may have significant implications for the Department of Defense. If the testing outcomes reveal substantial reductions in circuit compositions, the suggested algorithm could be regarded as a promising optimization technique for applications that require maximum optimization. This has the potential to benefit the Department of Defense by advancing quantum computing technology and paving the way for the development of a practical and useful system in the future.

Furthermore, if substantial reductions are observed, additional development of this approach may be warranted. The next step is to expand the set of test cases to include circuits containing more than three qubits. This expansion aims to provide a more comprehensive understanding of the algorithm's efficacy on a larger scale, where additional optimizations can be considered by optimization level 3.

Another important area of future work involves advancing the algorithm by expanding its capabilities to consider 4- and 5-qubit blocks. Fortunately, the three-layer commuting library already contains templates for these cases, which simplifies the implementation process. Adapting the algorithm to incorporate these templates will follow a similar procedure as before and provide insight to the scalability of this approach.

Another approach would be to consider recursive template matching to consider the effects of combined swaps on the system. For example, a circuit could follow the layout  $L_1L_2L_3L_4$ , where only  $L_1$ ,  $L_2$ , and  $L_3$  are commutable. After performing the commutation, the resulting circuit  $L_3L_1L_2L_4$  may reveal another subcircuit composed of  $L_1$ ,  $L_2$ , and  $L_4$  and that is now commutable. The proposed algorithm would not consider this revealed commutation, but expanding the algorithm to include recursive template matching could lead to further reductions.

Last, the ordering of operations in the algorithm could be tested. The three-layer commuting library contains 72 templates. Only 12 were considered for this algorithm because the remaining 60 templates contained adjacent gates that would be canceled before the template matching process. If template matching was performed before the original optimization pass, all 72 templates could be considered. This method may result in worse performance in certain cases as a reduction may be hidden due to the commutation, but testing would be required to determine if this approach performs well on average.

## REFERENCES

- Abdessaied, N., Soeken, M., Wille, R., & Drechsler, R. (2013). Exact template matching using Boolean satisfiability. In *Proceedings of the IEEE 43rd International Symposium on Multiple-Valued Logic*. <https://ieeexplore.ieee.org/document/6524685>
- Cole, B. (2021). *Commuting composition for quantum circuit reduction* (Publication No. 4889) [Master's thesis, Air Force Institute of Technology]. <https://scholar.afit.edu/etd/4889>
- Fösel, T., Niu, M. Y., Marquardt, F., and Li, L. (2021). *Quantum circuit optimization with deep reinforcement learning*. <https://arxiv.org/abs/2103.07585>
- Handique, M., and Sonkar, A. (2018). An extended approach for mapping reversible circuits to quantum circuits using NCV-|v1 library. *Procedia Computer Science*, 125, 832–839.

IBM Quantum. (2021). *Shor's algorithm*. Retrieved May 12, 2023, from <https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm>

IBM Quantum. (2023). *Compute resources*. Retrieved May 30, 2023, from <https://quantum-computing.ibm.com/services/resources?services=systems>

Office of the Under Secretary of Defense for Research and Engineering. (2023). *Critical technology areas*. Retrieved June 2, 2023, from <https://www.cto.mil/usdre-strat-vision-critical-tech-areas/>

Qiskit. (2023). *Qiskit: An open-source framework for quantum computing*. <https://qiskit.org/documentation/>

Teris, H., & Karaköse, M. (2022). *An improved and cost reduced quantum circuit generator approach for image encoding applications*. Quantum Information Processing. Retrieved from [https://www.researchgate.net/publication/361298928\\_An\\_improved\\_and\\_cost\\_reduced\\_quantum\\_circuit\\_generator\\_approach\\_for\\_image\\_encoding\\_applications](https://www.researchgate.net/publication/361298928_An_improved_and_cost_reduced_quantum_circuit_generator_approach_for_image_encoding_applications)



# Analysis of the Relative Risks Associated with Firearms as an Active Shooter Mitigation Technique on School Campuses

Captain Richard Weston, USMC  
Purdue Military Research Institute  
Weston.richard.29@gmail.com

J. Eric Dietz, PhD, PE  
Department of Computer and Information Technology  
Purdue University

**ABSTRACT** Computer-based simulations have been used to argue that firearms in the hands of school resource officers (SROs) or teachers can decrease the response time and the number of casualties in an active shooter incident (ASI). However, the introduction of firearms on school campuses can increase the risk of injury to students and staff. This project is focused on a comparative risk assessment of ASIs and firearms used as a mitigation technique on school campuses. Three primary data sources are used for the study. The project uses these data sources to estimate risks for both school shootings and firearm mishandling incidents, to perform statistical analysis, and to create a system dynamics model to simulate primary and secondary risks associated with firearms on school campuses. The project found that there is no significant difference between ASI-induced casualty counts and accidentally induced. Additionally, SROs and unarmed civilians are significant negative predictors of casualties in school firearm related incidents, and *t*-tests demonstrated that immediate first responders decrease response times and casualties. The simulation demonstrated that the secondary risks associated with SROs combined with residual risks are less than the primary ASI risk, which indicates that armed SROs can significantly reduce casualties during an ASI.

## INTRODUCTION

While active shooter incidents (ASIs) are significant events wherever they occur, locations that draw particular attention are kindergartens through high schools (K-12). The FBI’s report on ASIs identified 46 separate incidents occurring on K-12 institutions since 2000 (Blair & Schweit, 2020a,b). These incidents draw the public’s attention since they target a very vulnerable part of society. However, the implementation of firearms on school campuses to address and mitigate ASIs is subject to debate (Webster et al., 2017; Schildkraut & Martaindale, 2022; Rogers et al., 2018; Lott, 2019; Lee, 2019; Kirby, 2016; Jonson et al., 2020; Givens, 2015; Drake & Yurvati, 2018; Anklam et al., 2014). While school resource officers (SROs) are increasingly commonplace, armed school staff of any type is a mitigation technique of controversy. The problem addressed by this study is potential long-term risks incurred by introducing firearms on a school campus as a mitigation technique in either the hands of an SRO/police officer or armed school staff. The risks commonly brought up for firearms on campus include loss or theft of the weapon, accidental discharge

of the weapon by the person designated to carry and/or use it, or its improper use in stressful situations (Giffords Law Center, 2019).

## RESEARCH QUESTIONS AND PURPOSE

The following questions will be considered in this research project:

1. Is the combination of residual and secondary risks from an armed risk response to ASIs greater than the primary risk of ASI induced casualties?
2. Do armed first responders decrease the response time and potential casualties in an ASI?
3. What are the best methods of mitigating the long-term risks associated with legal firearms on K-12 campuses?

The project will test the following hypotheses:

1.  $H^0$ : SROs and civilian interventions are not significant predictors of firearm-related injuries in K-12 schools.

2.  $H^1$ : SROs and civilian interventions are significant predictors of firearm-related injuries in K-12 schools.
3.  $H^0$ : There is no difference between response time and mean number of casualties produced by resolutions from immediate responders and police.
4.  $H^2$ : Immediate first responders decrease response time and potential casualties from ASIs.

### ASSUMPTIONS, LIMITATIONS, AND DELIMITATIONS

The study uses the FBI's established definition of an ASI, which states that it is an incident that involves an individual that is "actively engaged in killing or attempting to kill people" (Blair & Schweit, 2014, p. 5). Additionally, there is a randomness associated with the phenomenon that is separate from pervasive crime trends. Therefore, the study assumes that all educational institutions are equally likely to experience an ASI. The study does not account for any specific training or barriers a school may have in place since these vary drastically from school to school, and there are likely missing school shooting incidents in the dataset. However, if an incident caused an injury, it is most likely included in the dataset.

### METHODOLOGY

The study uses a quantitative approach to determine whether an armed response to ASIs is an effective risk response to ASIs in K-12 schools and to investigate the secondary risks incurred by the firearm's introduction. It uses statistical analysis to form the basis for a system

dynamics model that compares two 10-year periods to each other. For one 10-year period, it is supposed that every school has an SRO present and the secondary risks such as accidental discharge and loss or theft of the firearm are possible. For the other 10-year period, there are no SROs on the school campuses and the chance of secondary risk occurrence is removed.

### DATA DESCRIPTION

The study uses data gathered by the Center for Homeland Defense and Security on K-12 shootings and data from Everytown Research & Policy. The dataset does not include incidents from the Giffords Law Center due to overlap with the other datasets. The dataset represents a compilation of all firearm-related incidents on school campuses from 1999 to 2023. There have been 125 ASI events on school campuses within the date range. While several ( $n = 52$ , 3%) of the ASI events were resolved with no casualties due to the heroic actions of bystanders, SROs, and the police, 73 (4%) incidents caused significant casualties and account for 23% ( $n = 395$ ) of the total casualties in the datasets while they only account for 4% of the total. The mean casualty rate for ASIs ( $M = 3.1$ ,  $SD = 7.1$ ) is significantly higher than any other situation related to school shootings, and all the outliers in the dataset fall into the ASI category. Figure 1 shows the frequency for the number of casualties in ASIs.

The data set, however, contains many situations that were not labeled as ASIs that account for the remaining casualties. Table 1 contains the frequency, mean number of casualties, and standard deviation for each situation. Most of the ASIs fall in the indiscriminate category.

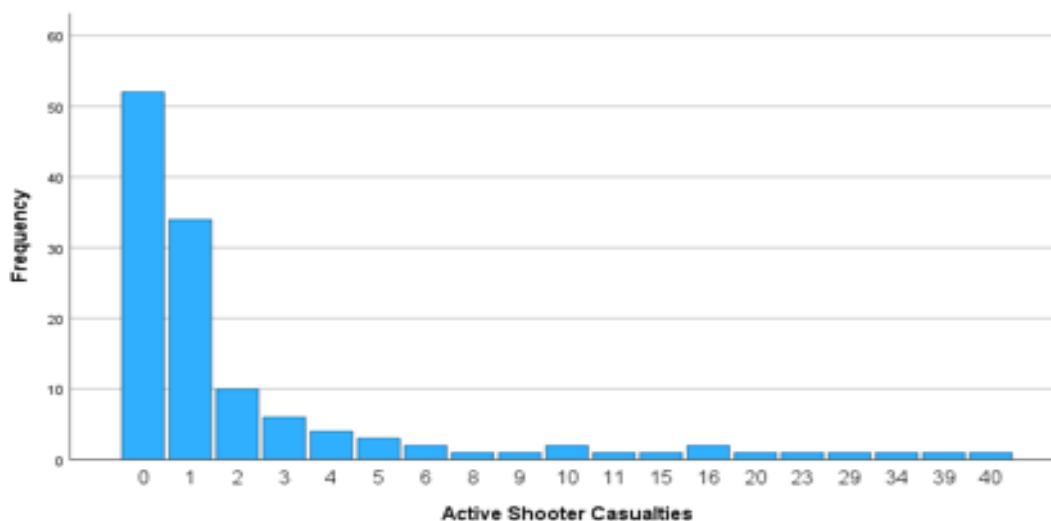


Figure 1. Histogram depicting the frequency of each ASI casualty count

**Table 1.** Descriptives for situation type

Variable	Frequency	Mean Number of Casualties	Standard Deviation
Suicide/attempt	106 (6.5)	.89	.35
Self-defense	11 (.7)	1.00	.45
Psychosis	14 (.9)	.57	.65
Officer-involved	8 (.5)	1.25	.71
Murder/suicide	11 (.7)	1.82	.87
Intentional	63 (3.8)	.08	.27
Indiscriminate	66 (4.0)	4.80	9.01
Illegal activity	98 (6.0)	1.07	2.08
Hostage/stand-off	32 (2.0)	.31	.53
Escalation	519 (31.6)	1.03	1.08
Drive-by	138 (8.4)	.91	1.19
Domestic with targets	59 (3.6)	.93	.69
Bullying	18 (1.1)	1.72	3.44
Anger school related	14 (.9)	1.14	1.61
Accidental	178 (10.8)	.69	.70
Missing	306 (18.6)		
Total	<i>n</i> = 1335 (81.4) <i>N</i> = 1641 (100)	1.10	2.44

## STATISTICAL ANALYSIS RESULTS

The first null and alternate hypotheses that SROs and civilian interventions are significant predictors of firearm-related injuries on K-12 schools are tested through a negative binomial regression with the number of casualties for each incident as the dependent variable (DV), resolution type as the independent variable (IV), and duration in minutes as a covariate. The “other” category in resolution type was programmed as system missing. Table 2 shows the frequency and mean and standard deviation for the number of casualties for each resolution type.

The model includes 1,432 incidents (88%), passed the goodness of fit test ( $X^2(1432) > .05$ ), and the omnibus test indicates that the model is a significant predictor ( $X^2(6) = 198.39, p < .001$ ). Both the resolution types ( $X^2(5) = 196.33, p < .001$ ) and duration in minutes ( $X^2(1) = 12.94, p < .001$ ) predictors are statistically significant. The resolution type “fled” is the reference group for the regression, and each of the types is statistically significant. Both the SRO ( $B = -.45, p < .01$ ) and civilian resolution ( $B = -.47, p = .008$ ) types have a negative effect on the number of casualties, while police ( $B = .36, p < .001$ ), armed civilian ( $B = 1.22, p < .001$ ), and self-induced ( $B = .72, p < .001$ ) have a positive effect on the number of casualties if all other variables remain the same. The incident rate ratios (IRR) indicate that when an SRO resolution is increased by 1, the number of casualties is decreased by a factor of .64 when all other variables remain the same, or there is a 36% reduction in casualties from an increase of 1 SRO. Conversely, when the police resolution is increased by 1,

the number of casualties is increased by a factor of 1.44 (44%). Refer to Table 3 for all  $B$ ,  $SE B$ ,  $X^2$ ,  $p$ , and IRRs for each variable.

While the unarmed civilian resolution type has a negative predictive relationship with the number of casualties, these incidents where an unarmed civilian can stop the shooter occur when the shooter happens to be physically close to the civilian who acted. If there is any distance involved, the unarmed civilian is not usually able to act. For example, in 2018 at North Scott Junior High School, a twelve-year-old student pulled a firearm in class, pointed it at the teacher, and attempted to fire. The weapon’s safety was still on, so the teacher was able to disarm the student and maintain control until the police arrived (Spoerre, 2018). Many other cases in the civilian resolution category are similar to this in that luck and close physical distance combined with the will to act allowed the bystander to take action and end the situation.

The covariate duration in minutes is also a significant predictor of the number of casualties ( $B = .002, p < .001$ ), and the IRR indicates that for every 1 unit of increase in minutes, the number of casualties increases by 1.00. The duration in minutes variable, however, is skewed significantly by several outliers that were caused by hostage situations that lasted for hours. Additionally, the armed staff variable contains thirteen individual incidents, two of which are ASIs and one is an incident of staff cross-fire, causing four casualties. Those three incidents greatly skewed the predictive value of the armed staff resolution category. Overall, the results support the rejection of the

**Table 2.** Resolution type descriptives,  $n = 1641$ 

Variable	Frequency	Mean Number of Casualties	Standard Deviation
SRO	91 (5.5)	.57	.81
Police	205 (12.5)	1.33	3.80
Unarmed civilian	57 (3.5)	.58	1.05
Armed civilian	14 (.9)	2.93	4.10
Self-induced	154 (9.4)	1.89	4.85
Fled	967 (58.9)	.92	.98
Other	153 (9.3)		
Total	1641	1.06	2.33

**Table 3.** Negative binomial regression predicting number of casualties (DV) based on resolution type (IV),  $n = 1439$ 

Predictor Variable	B	Std. Error	Wald Chi-Square	Exp(B)
Intercept	-.07	.03	4.19*	.99
SRO	-.45	.14	9.55**	.64
Police	.36	.07	26.09***	1.44
Unarmed civilian	-.47	.18	6.94**	.63
Armed civilian	1.22	.16	57.89***	3.37
Self-induced	.72	.07	111.40***	2.05
Fled	.00			1.00
Duration in minutes	.002	.0006	12.94***	1.00

second null hypothesis and the acceptance of the second alternate hypothesis.

The second null and alternate are tested by two separate  $t$ -tests. The first  $t$ -test compares the mean duration in minutes of ASI resolved by SROs and unarmed civilian and armed civilian responders ( $M = 1.10$ ,  $SD = 13.23$ ) to incidents that were resolved by the police or the shooter ( $M = 24.56$ ,  $SD = 58.54$ ). The dependent variable was created by recoding the duration in minutes variable into a new variable that excluded all non-ASIs. The test indicates that there is a statistically significant difference between the duration in minutes for the ASIs that were resolved by first responders and ASIs that were resolved by the police or the shooter ( $t(122) = -2.70$ ,  $p < .01$ ). The second portion of the hypothesis is tested with a separate  $t$ -test that uses the same independent variables on a different dependent variable, number of casualties for ASIs. The number of casualties variable was recoded into a new variable that excluded all non-ASIs. The test shows that there is a statistically significant difference in mean casualty numbers from incidents resolved by immediate responders ( $M = 1.19$ ,  $SD = 2.42$ ) and the incidents resolved by the police or shooter ( $M = 4.98$ ,  $SD = 9.42$ ) ( $t(122) = -3.09$ ,  $p < .01$ ) in that the immediate responders had a lower mean casualty number than the police response incidents. Both the  $t$ -tests support the rejection

of the third null hypothesis and the acceptance of the third alternate hypothesis since they both indicate that immediate responders can significantly decrease the duration of the incident and the number of casualties.

### MODEL SIMULATION

An AnyLogic system dynamics simulation is used to answer research question 2. To evaluate the effectiveness of SROs in schools with the potential for accidental injuries, a model that runs in year intervals was created to simulate a 10-year period that represents a designated period of time in the data. The model is then manipulated in such a way that the risks and mitigation techniques can be evaluated.

A simplistic base model is designed to only account for ASIs during the selected time frame. The years 2009 to 2019 are used for the simulation since these years have the most recent and accurate data and are not skewed by school closures resulting from the COVID-19 virus. The 2009–2019 data points were separated out from the main data set and include 572 incidents containing 55 ASIs. The ASIs during that 10-year period resulted in 197 casualties ( $M = 3.58$ ,  $SD = 7.22$ ). These casualties were spread across an average of 131,204 K-12 schools during the selected 10-year period (National Center for

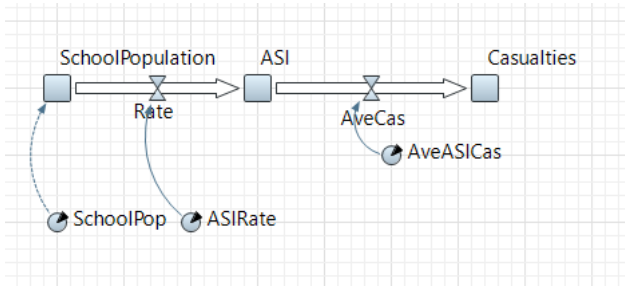


Figure 2. Base ASI model

Education Statistics, 2023). Since ASIs are assumed to be a random event, each school is included without any weight applied. The ASI occurrences and the average number of schools during the period are used to create the ASI yearly rate of .000042 ( $55/10 = 5.5/134204 = .000042$ ), which was placed in the ASIRate parameter depicted in Figure 2.

The average ASI casualty count parameter, AveASICas, uses a triangular function in AnyLogic that allows the researcher to input the minimum and maximum values and the mean. The minimum value inserted is 1 since the model is focused on the ASI events that induced casualties. The maximum value is 34 since one ASI event resulted in 34 casualties. The mean is from the average casualties resulting from ASIs. The java command input into the parameter is `triangular(1, 34, 3.58)`. Figure 2

depicts the base model used to validate the process. The model results in 175.63 casualties for the 10-year period with all parameters fixed and no randomness.

The base model is then manipulated to account for the SRO reduction rate predicted by the negative binomial regression and the secondary risks resulting from accidental discharges. Figure 3 depicts the final model that includes the SRO effect and secondary risk. This includes the addition of a residual casualty stock (ResCas) that is affected by the flow SROEffect. This flow uses a parameter called SROReductionRate to reduce the original casualty count produced by ASIs in accordance with the regression prediction. The IRR from the negative binomial regression for SROs indicates that for every SRO added to the population the number of casualties is reduced by a factor of .64. This number is used in the SROReductionRate parameter. The number of casualties produced by ASIs is multiplied by the SRO reduction parameter (.64) and collected in TotalResCas, which also collects the accidental casualties counts. Since the reduction rate is universally applied, the SRO effect model replicates a scenario in which every firearm-related incident that occurs in a K-12 school in the United States has an SRO on the campus and the SRO resolves the situation.

The second avenue that feeds into the total residual casualties is a model accounting for accidental injuries caused by SROs in K-12 schools. The data set contains seven incidents (1%) where an SRO accidentally

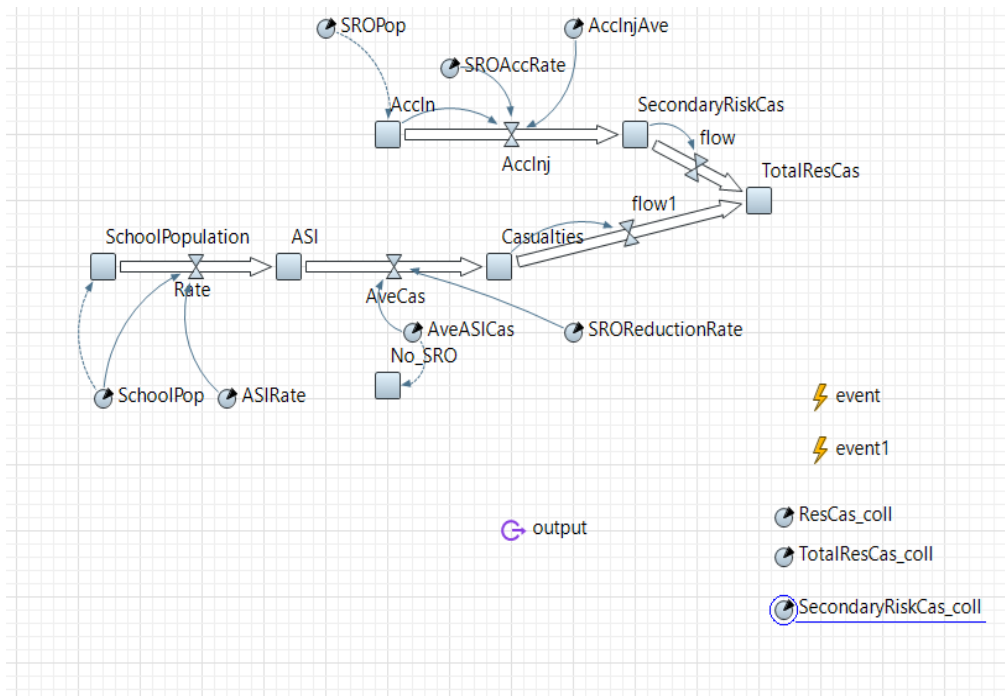


Figure 3. SRO effect model that simulates the addition of an SRO to every incident

discharged their firearm. As mentioned in the limitations of this study, it is likely that there are accidental discharges that are not accounted for in the dataset since it is possible that an SRO accidentally discharges his or her weapon but does not report it. However, it is very unlikely that there are any incidents of accidental discharge that resulted in an injury that are not in the dataset since SROs would be required to report the incident. In the 2009–2019 dataset, one incident resulted in an injury.

According to the National Center for Education Statistics (2019), only 46.7% ( $N = 61,144$ ) of schools in the 2017–2018 school year had an SRO on campus. This is the only school year with statistics for SRO numbers in K-12 schools, so it is used in conjunction with the number of schools in 2017 ( $N = 130,930$ ) to create the SRO accidental rate ( $SROAccRate = .0000114$ ), which is applied across all 10 years. The rate is determined by the number of SRO accidental discharges ( $N = 7$ ) divided by the number of years and the number of schools that had SROs ( $N = 61,144$ ) ( $7/10 = .7/66144 = .0000114$ ). This rate was compared to statistical information on national police accidental discharge rates gathered in 2019 (Bellisle, 2019). The Associated Press study identified 1,422 accidental discharges from 2012–2019, which caused 21 deaths and 232 injuries. The average number of law enforcement officers in the US during that date range is 658,523 (FBI, 2019). The rate of accidental discharges for the 8-year period is .00027. While the rate is higher than the SRO rate reflected in the study’s dataset, it is likely due to the high number of high-risk situations law enforcement officers encounter that require use of their service weapon. SROs, alternatively, rarely draw their service weapons and thus have a lower chance of accidentally discharging them.

The average number of injuries parameter  $AcclnjAve$  is used to quantify the number of casualties induced by an accidental discharge. It also uses a triangular function with the minimum set at 0, the maximum set at 1, and the mean represented by the mean from the dataset ( $M = .14$ ,  $SD = .38$ ). The java function inserted into the parameter is triangular (0,1, .14). Both this parameter and the ASI casualties parameter are set to random generation within the specified bounds for the randomized model.

The average school population is the starting value for the first stock  $Accln$ , which is multiplied by  $SROAccRate$  and  $AcclnjAve$  and fed in the  $SecondaryRiskCas$  stock, which then contributes to the total casualties found in the  $TotalResCas$  stock. With all parameters fixed, the SRO effect model indicates that if every school in the US had an SRO present for the 2009–2019 period, the total residual casualties would be 105.04. This represents a 40% reduction in casualties from the 175.63 casualties in the base model and indicates that the residual risk with the secondary risk accounted for is less than the primary risk. Figure 4 depicts the overall results from the fixed model.

An experiment with 100 hypothetical 10-year periods was generated to further test the model and introduce the randomness present in the ASI phenomenon with a parameter experiment. The experiment replicates the upper and lower bounds for ASI and accidental discharge casualties. Randomness is introduced by allowing the ASI casualties and accidental casualties parameters to randomize. The randomization is restricted to the bounds defined in the triangular function. ASIs without any SRO mitigation resulted in an average of 130.11 casualties ( $SD = 70.48$ ). With the SRO reduction rate applied, the average number of casualties is reduced to 79.90

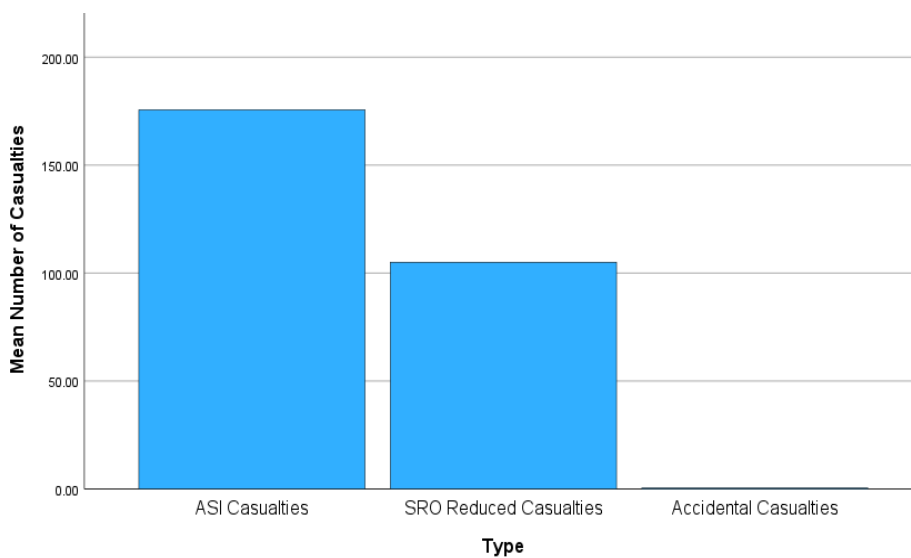


Figure 4. Fixed model overall results from the SRO effect model

( $SD = 40.62$ ). The average number of casualties caused by accidental discharges is .55 ( $SD = .32$ ). The mean casualty counts represent a 38% overall reduction in casualties. These results answer the second research question and indicate that the residual risk from ASIs is less than the primary risk even when the secondary risk of accidental discharges is accounted for and randomness is introduced into the model. The results of the experiment are graphically depicted in Figure 5.

The model is further modified to account for the effect of more restrictive carry conditions used to mitigate the secondary risk from firearms on campuses. The model used simulation data from an unpublished 2014 paper by Kirby to estimate the effectiveness of the carry conditions. The response time and casualty averages from the most restrictive carry condition for SROs were incorporated into the model and indicate that the mean

number of residual casualties after restrictive carry conditions are applied to the average number of casualties is 96.64 ( $SD = 59.75$ ), which is still a 26% reduction from the mean casualty number of 130.95 ( $SD = 80.96$ ) for unmitigated ASIs. These results represent a 17% increase from the ready carry condition SRO effect. This suggests that the most restrictive carry conditions can still reduce the mean number of casualties, but it is less effective than SROs with their weapons in the ready condition. Figure 6 depicts the results of the experiment variation graphically.

### CONCLUSION

There is a significant gap in the literature on ASI mitigation in K-12 schools that uses a quantitative approach to evaluate the risks from ASIs and mitigating them through

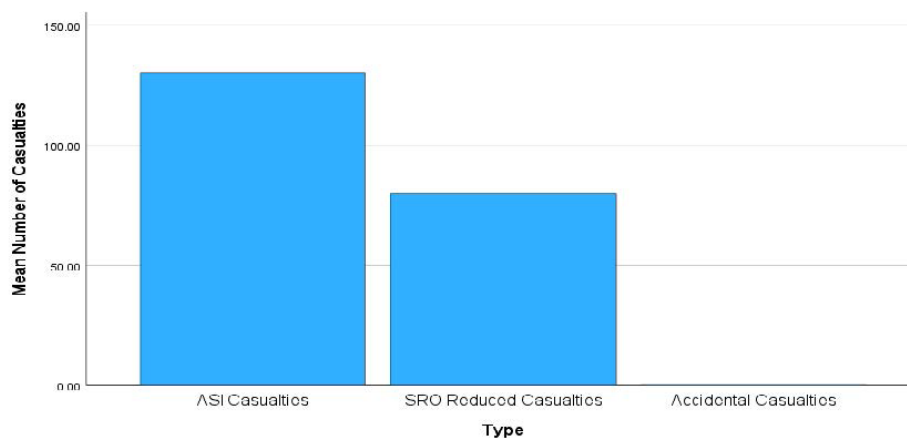


Figure 5. Mean number of casualties by ASI without mitigation, the residual number of casualties with mitigation, and the accidental casualties

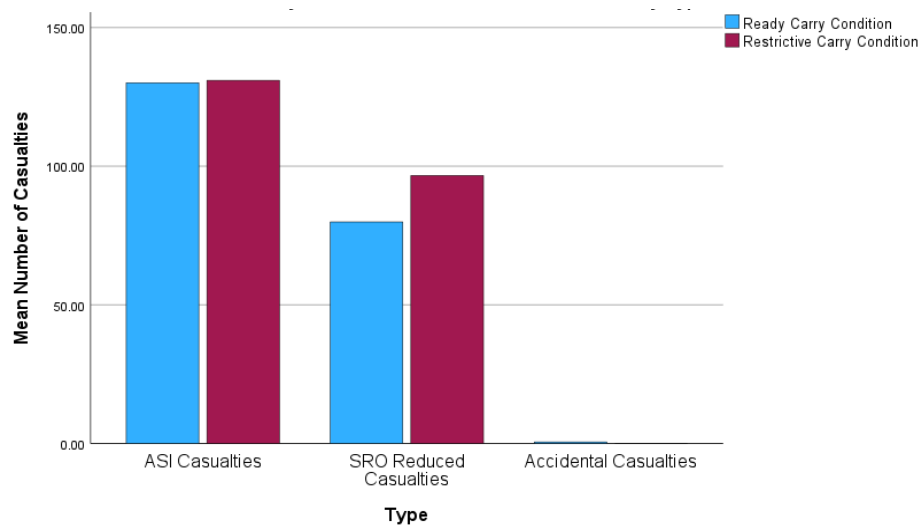


Figure 6. Results of the SRO effect model modified to reflect carry condition data

armed first responders. Other sources have investigated the issue through qualitative means or simulations based on a singular historical incident. This study strives to include all data sources for the topic to run statistical analysis that supports simulation modeling. The results indicate that armed responders in K-12 schools as a mitigation technique for ASIs is an appropriate risk treatment plan that does not incur significant secondary risks. The regression revealed that SROs and unarmed civilians can decrease the number of casualties in all firearm-related incidents on school grounds, including ASIs, should the other variables remain the same. But waiting for the police to respond and end the situation predicts a higher number of casualties. This indicates that the sooner a situation can be resolved, the fewer casualties that will result, as indicated by the positive predictive nature of the duration of the incident.

While there are secondary risks associated with the armed response treatment plans, they are minimal and can be mitigated with training. The simulation model demonstrates and answers the equation ( $a + S < A$ ) used to determine whether a treatment plan is worth implementing despite its secondary risks. The results of the model show that the residual risk ( $a$ ) of casualties following the addition of SROs combined with the secondary risk of the introduction of firearms on school campuses ( $S$ ) are 38% less than the primary risks or casualties from ASIs ( $A$ ).

## REFERENCES

- Adams, J. (2007). Risk management: It's not rocket science . . . it's much more complicated. *Risk Management Magazine* 54(5), 36–40. <https://www.proquest.com/docview/227006505?pq-origsite=gscholar&fromopenview=true>
- Agnich, L. E. (2014). A comparative analysis of attempted and completed school-based mass murder attacks. *American Journal of Criminal Justice* 40(1), 1–22. <https://link.springer.com/article/10.1007/s12103-014-9239-5>
- Anklam, C. E., Kirby, A., Sharevski, F., & Dietz, J. E. (2014). Mitigating active shooter impact; analysis for policy options based on agent/computer based modeling. *Emergency Management* 13(3), 1–24. [https://foac-pac.org/uploads/Reports-Studies/2014-09-Dealing\\_With\\_Active\\_Shooters-Purdue\\_Research\\_Paper-Compr.pdf](https://foac-pac.org/uploads/Reports-Studies/2014-09-Dealing_With_Active_Shooters-Purdue_Research_Paper-Compr.pdf)
- Avila, M. (2019). *The School Guardian Program*. Florida Department of Law Enforcement. <https://flaglerlive.com/wp-content/uploads/Avila-Marco-paper.pdf>
- Bellisle, M. (2019, December 9). *Accidental shootings show police training gaps*. Associated Press. <https://apnews.com/article/accidents-ar-state-wire-ia-state-wire-wa-state-wire-iowa-009ac6cf0a174a58d88d9d01308aedd6>
- Berlin, S. (2022, August 19). *Signs warn about 'deadly force' at Florida schools: 'Teachers are armed.'* Newsweek. <https://www.newsweek.com/signs-warn-deadly-force-florida-schools-teachers-are-armed-1735325>
- Blair, J. P., & Schweit, K. W. (2014). *A study of active shooter incidents in the United States between 2000 and 2013*. Texas State University and Federal Bureau of Investigation. <https://www.fbi.gov/file-repository/active-shooter-study-2000-2013-1.pdf/view>
- Blair, J. P., & Schweit, K. W. (2022a). *Active shooter incidents in the United States in 2021*. Texas State University and Federal Bureau of Investigation. <https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2021-052422.pdf/view>
- Blair, J. P., & Schweit, K. W. (2022b). *Active shooter incidents 20-Year Review, 2000–2019*. Texas State University and Federal Bureau of Investigation. <https://www.fbi.gov/file-repository/active-shooter-incidents-20-year-review-2000-2019-060121.pdf/view>
- Borshchev, A. (2014). Multi-method modelling: AnyLogic (pp. 248–279). In S. Brailsford, L. Churilov, & B. Dangerfield (Eds.), *Discrete-event simulation and system dynamics for management decision making*. Wiley. <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118762745.ch12>
- Clarke, R. V. (2009). Situational crime prevention theoretical background and current practice (pp. 269–276). In M. D. Krohn, A. J. Lizotte, & G. P. Hall (Eds.), *Handbook on crime and deviance*. Springer. [https://link.springer.com/chapter/10.1007/978-1-4419-0245-0\\_14](https://link.springer.com/chapter/10.1007/978-1-4419-0245-0_14)
- Crime Prevention Research Center. (2022). *Massive errors in FBI active shooting reports regarding cases where civilians stop attacks*. Crime Research. Massive errors in FBI's Active Shooting Reports regarding cases where civilians stop attacks: Instead of 4.4%, the correct number is at least 34.4%. In 2021, it is at least 49.1%. Excluding gun-free zones, it averaged over 50%
- Cummings, P. (2009). The relative merits of risk ratios and odds ratios. *Archives of Pediatrics and Adolescent Medicine*, 163(5), 438–445. <https://jamanetwork.com/journals/jama-pediatrics/fullarticle/381459#:~:text=In%20summary%2C%20the%20risk%20ratio,to%20exposure%20among%20the%20exposed.&text=The%20odds%20ratio%20lacks%20any,the%20change%20in%20average%20odds>
- Cummings, C. L., Rosenthal, S., & Kong, W. Y. (2021). Secondary risk theory: Validation of a novel model of protection motivation. *Risk Analysis*, 41(1), 204–220. <https://onlinelibrary.wiley.com/doi/full/10.1111/risa.13573>
- Everytown Research & Policy. (2023). *Gunfire on school grounds in the United States*. <https://everytownresearch.org/maps/gunfire-on-school-grounds/>
- Drake, D. S., & Yurvati, E. (2018). *Teachers with guns: Firearms discharges by schoolteachers, 1980–2012*. Center for Homicide Research. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/teachers-guns-firearms-discharge-schoolteachers-1980-2012>
- FBI. (2019). *Full-time law enforcement employees*. <https://ucr.fbi.gov/crime-in-the-u.s/2013/crime-in-the-u.s.-2013/tables/table-74>
- Finn, P. (2006). School resource officer programs: Finding the funding, reaping the benefits. *FBI Law Enforcement Bulletin*,



- 75(8), 1–7. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/school-resource-officer-programs-finding-funding-reaping-benefits>
- Frantz, B. M. (2021). *Active shooter mitigation for open-air venues* (Publication 14593671) [Doctoral dissertation, Purdue University].
- Giffords Law Center. (2019). *The truth about school shootings*. <https://giffords.org/lawcenter/report/the-truth-about-school-shootings/>
- Givens, A. (2015). Missing the mark: School personnel should not be armed. *University of Dayton Law Review*, 40(2), 201–224. [https://heinonline.org/HOL/Page?handle=hein:journals/udlr40&div=13&g\\_sent=1&casa\\_token=](https://heinonline.org/HOL/Page?handle=hein:journals/udlr40&div=13&g_sent=1&casa_token=)
- Grigoryev, I. (2022). *AnyLogic in three days: A quick course in simulation modeling* (6th ed.).
- Gun Violence Archive. (2022, June 18). <https://www.gunviolencearchive.org/>
- Hanna, J., & Yan, H. (2017). *Sutherland Springs church shooting: What we know*. CNN. <https://www.cnn.com/2017/11/05/us/texas-church-shooting-what-we-know/index.html>
- Hillson, D. (1999). Developing effective risk responses. In *Proceedings of the 30th Annual Project Management Institute Seminars & Symposium*, Philadelphia. <https://risk-doctor.com/wp-content/uploads/2020/09/Hillson-Developing-risk-responses-PMI-Oct1999.pdf>
- Hutchinson, A. (2013). *Report of the national school shield task force*. National School Shield. [https://www.edsource.org/wp-content/uploads/old/NSS\\_Final.pdf](https://www.edsource.org/wp-content/uploads/old/NSS_Final.pdf)
- Jonson C. L., Burton A. L., Cullen F. T., Pickett J. T., & Burton V. S. (2020). An apple in one hand, a gun in the other: Public support for arming our nation's schools. *Criminology & Public Policy* 20(2). <https://onlinelibrary.wiley.com/doi/pdfdirect/10.1111/1745-9133.12538>
- Judd, G. (2018). Polk county school safety guardian program—a partnership that works. *All Points Bulletin*, 28(3), 14–15. [http://trendmag.trendoffset.com/publication/?i=543002&article\\_id=3239038&view=articleBrowser&ver=html5](http://trendmag.trendoffset.com/publication/?i=543002&article_id=3239038&view=articleBrowser&ver=html5)
- Kent, J. K., & Curran, F. C. (2021). Pulling the trigger: The decision of arming school staff in a large, diverse school district. *Journal of Cases in Educational Leadership* 24(3), 87–104. <https://journals.sagepub.com/home/jel>
- Kirby, A. M. (2016). *Comparing policy decisions for active shooters using simulation modeling* (Publication No. 10149736) [Doctoral dissertation, Purdue University].
- Lee, J. Y. (2019). *Agent-based modeling to assess the effectiveness of Run Hide Fight* (Publication No. 8020763) [Doctoral dissertation, Purdue University]. [https://hammer.purdue.edu/articles/thesis/AGENT-BASED\\_MODELING\\_TO\\_ASSESS\\_THE\\_EFFECTIVENESS\\_OF\\_RUN\\_HIDE\\_FIGHT/8020763](https://hammer.purdue.edu/articles/thesis/AGENT-BASED_MODELING_TO_ASSESS_THE_EFFECTIVENESS_OF_RUN_HIDE_FIGHT/8020763)
- Li, C., Ren, J., & Wang, H. (2016). A system dynamics simulation model of chemical supply chain transportation risk management systems. *Computers & Chemical Engineering* 89(9), 71–83. <https://www.sciencedirect.com/science/article/pii/S0098135416300564>
- Lincke, S. J., & Khan, F. (2020). Ethical management of risk: Active shooters in higher education. *Journal of Risk Research* 23(12), 1582–1578. <https://www.tandfonline.com/doi/full/10.1080/13669877.2019.1687575?cookieSet=1>
- Lott, J. (2019). *Schools that allow teachers to carry guns are extremely safe: Data on the rate of shootings and accidents in schools that allow teachers to carry*. Crime Prevention Research Center. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3377801](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3377801)
- Martinez-Moyano, J., & Richardson, G. P. (2013). Best practices in system dynamics modeling. *System Dynamics Review* 29(2), 102–123. <https://onlinelibrary.wiley.com/doi/full/10.1002/sdr.1495>
- Mooney, M. (2018). *The hero of Sutherland Springs shooting is still reckoning with what happened that day*. Texas Monthly. <https://www.texasmonthly.com/articles/stephen-willeford-sutherland-springs-mass-murder/>
- National Center for Education Statistics. (2019). *2005–06, 2007–08, 2009–10, 2015–16, and 2017–18 School Survey on Crime and Safety (SSOCS)*. [https://nces.ed.gov/programs/digest/d19/tables/dt19\\_233.70.asp](https://nces.ed.gov/programs/digest/d19/tables/dt19_233.70.asp)
- National Center for Education Statistics. (2021). *Table 105.50. Number of educational institutions, by level and control of institution: 2009–10 through 2019–20*. <https://nces.ed.gov/fastfacts/display.asp?id=84>
- National Conference of State Legislatures. (2022). *School Safety: Guns in Schools*. <https://www.ncsl.org/research/education/school-safety-guns-in-schools.aspx>
- Project Management Institute. (2017). *A guide to the Project Management Body of Knowledge* (6th ed.).
- Riedman, D., & O'Neill, D. (2020a). *K-12 school shooting database*. [www.chds.us/ssdb/](http://www.chds.us/ssdb/)
- Riedman, D., & O'Neill, D. (2020b). *K-12 school shooting database: Research methodology*. [www.chds.us/ssdb/](http://www.chds.us/ssdb/)
- Rogers, M., Ovares, E. A., Ogunleye, O. O., Twyman, T., Akkus, C., Patel, K., & Fadlalla, M. (2018). Is arming teachers our nation's best response to gun violence? The perspective of public health students. *American Journal of Public Health* 108(7), 862–863. <https://web.p.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=d5253ec8-7ed9-4c55-b4dd-5fc57ecd2b01%40redis>
- Rogers, R. W. (1975). A protection motivation theory of fear appraisals and attitude change. *Journal of Psychology* 91(1), 93–114. <https://www.tandfonline.com/doi/abs/10.1080/00223980.1975.9915803>
- Sawchuk, S. (2021). *School resource officers (SROs) explained*. Education Week. <https://www.edweek.org/leadership/school-resource-officer-sro-duties-effectiveness>
- Schildkraut, J., & Martaindale, M. H. (2022). Should firearms be allowed in K-12 public schools? An analysis of law enforcement's perceptions of armed teacher policies. *Security Journal*, 35, 1288–1307. <https://doi.org/10.1057/s41284-022-00327-4>
- Spoerre, A. (2018, July 5). *Trial begins Monday for Iowa middle-schooler accused of attempting to shoot his teacher in front of classmates*. Des Moines Register. <https://www.desmoinesregister.com/story/news/crime-and-courts/2019/07/05/iowa-school-shooting-luke-andrews-davenport-north-scott-eldridge-attempted-murder-trial-teacher/1635581001/>
- Tuttle, H. (2015). Preparing for an active shooter incident. *Risk Management* 62(9), 6–7. <https://www.proquest.com>

/docview/1732565749?pq-origsite=gscholar&from  
openview=true

Tzvetanov, K., Cline, T., Thomas, G., Wood, C., & Dietz, J. E. (2022).  
Active shooter mitigation strategies in small rural  
churches. *Emergency Management 20*(2), 111–125.  
<https://europepmc.org/article/med/35451048>

Waldrop, T. (2022). *What we know about the armed bystander  
who killed the shooter at an Indiana mall*. CNN. <https://www>

.cnn.com/2022/07/19/us/eli-dicken-indiana-mall-shooting  
-bystander/index.html

Webster, D., Crifasi, C., Vernick, J., & McCourt, A. (2017).  
*Concealed carry of firearms: Fact vs. fiction*. Center for Gun  
Policy and Research. [https://www.jhsph.edu/research/centers-and-institutes/johns-hopkins-center-for-gun-violence-prevention-and-policy/\\_archive-2019/\\_pdfs/concealed-carry-of-firearms.pdf](https://www.jhsph.edu/research/centers-and-institutes/johns-hopkins-center-for-gun-violence-prevention-and-policy/_archive-2019/_pdfs/concealed-carry-of-firearms.pdf)

## Equivariant Decoders for Quantum LDPC Codes

Jim Z. Wang, Laurence D. Merkle, and Leleia A. Hsia

Department of Electrical and Computer Engineering

Air Force Institute of Technology

Jim.Wang@afit.edu, Laurence.Merkle@afit.edu, Leleia.Hsia@afit.edu

**Abstract** Quantum error correction (QEC) enables both industrial and defense applications of quantum computing. Toric codes and other quantum low-density parity-check (LDPC) codes, such as the hyperbolic surface code, are promising and well-researched methods of QEC. However, their decoding cost increases exponentially with a computer’s qubit count. Neural networks have been shown to decode a code’s error syndrome both accurately and fast enough for a real-time error-correcting scheme. Recent key developments introduced convolutional neural networks (CNNs) to implement an equivariant decoder for a toric code. These CNN decoders both outperform Neural Network (NN) decoders and require less training data. These techniques may be expanded to other LDPC codes. This paper presents a machine learning (ML) approach to QEC using CNNs and LDPC codes. This approach leverages these models’ high data efficiency, a product of CNNs equivariance and some LDPC codes’ inherent symmetries. Further, unlike the minimum weight perfect matching decoder and other non-ML approaches, these models correctly count degenerate errors and are consequently more accurate. Therefore, equivariant decoders both require less data than traditional NN decoders and surpass non-ML decoder performance.

### INTRODUCTION

Reliable large-scale quantum computing necessitates quantum error correction (QEC). Quantum computers have exponential computing power relative to classical computers and are exhibited as a “critical technology” by the Office of the Under Secretary of Defense for Research and Engineering (Shyu, 2022). However, their capabilities rely on highly volatile and error-prone qubits. Subject to decoherence and the unavoidable noise of real-world quantum systems, these qubits require error correcting for application. This problem is further exacerbated by the no-cloning theorem, which states that qubit states cannot be arbitrarily copied. Therefore, qubit buttressing cannot rely on mere replication and must employ more creative error-correcting methods. However, recent developments in quantum low-density parity-check (LDPC) codes and neural decoders for those codes offer insight into and hope for a future with realized quantum computing.

Effective QEC would lead to multitudes of quantum computing applications. Quantum computers offer an exponential computational speedup for some applications. Since a qubit in superposition is in multiple states simultaneously, quantum computers can process information in multiple states simultaneously. Therefore, conceptually, a single quantum computer may perform an exponentially larger number of computations in parallel compared to a classical computer. This inherent parallelization enables polynomial time solutions for at least

one important class of problems for which no polynomial time classical solution is known.

While the potential for speedup over classical computation is a theoretical fact, practical quantum supremacy remains contested. Though qubits enable the aforementioned exponential acceleration, their high susceptibility to noise has hindered their ability to achieve indisputable quantum supremacy. They are usable only for short periods and are highly susceptible to error. All existing quantum computers suffer from these drawbacks, and as a whole, the field exists in the noisy intermediate scale quantum computing era. This era is characterized by error correction and benchmarking. Therefore, the current state of the art in quantum computing relies on effective QEC.

Researchers have turned to classical computing for error correction inspiration. Classical LDPC codes encode data at a higher encoding rate than a repetition code (Breuckmann & Eberhardt, 2021). This increased efficiency, combined with the consideration of the no-cloning theorem, suggest that a quantum analog of LDPC code may be highly auspicious (Badger, 2021). The toric code and its planar cousin, the rotated surface code, are two of the most well-researched families of LDPC codes (Badger, 2021). Other proposed LDPC codes, such as the hyperbolic surface code and lifted product code, have a higher encoding rate but require rigorous testing and evaluation (Breuckmann & Eberhardt, 2021).

The method of selecting corrective operations to execute on the circuit, known as decoding, varies between

error-correcting codes. LDPC codes are categorized as low-level; they correct individual faulty qubits encoded in the code. Equivariant decoders exploit the inherent symmetries in a toric code and have been shown to outperform both feed-forward neural networks and the minimum weight perfect matching (MWPM) algorithm (Egorov et al., 2023).

This research aims to implement and evaluate an equivariant convolutional neural network (CNN) decoder on the hyperbolic surface code. Since many of the symmetries that allow for an equivariant decoder on the toric code exist also on a hyperbolic surface code, the natural extension of previous research is immediately evident. Therefore, this paper builds on previous data generation methods (Egorov et al., 2023) and a construction of a CNN decoder for a hyperbolic LDPC code.

## BACKGROUND

This section presents a brief overview of the basics of quantum computation, existing LDPC codes, and CNN decoders.

### Quantum Computation

Quantum computers owe their computational uniqueness to the qubit, often represented visually in a Bloch sphere (Figure 1). While classical bits can assume values of 0 and 1, a qubit state exists as a linear combination of basis states represented by vectors  $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$  and  $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ . Therefore, a value of a qubit is represented by  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , where  $\alpha$  and  $\beta$  are complex numbers and  $|\alpha|^2 + |\beta|^2 = 1$ . Written as a vector, a qubit has state  $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ .

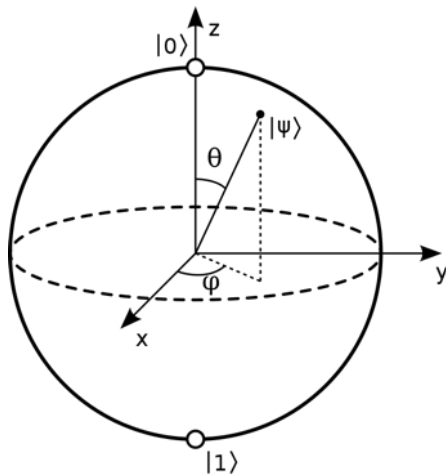


Figure 1. Bloch sphere. Adapted from Badger (2021).

Four fundamental single-qubit operations are the Identity, Pauli X, Pauli Z, and Pauli Y operations represented as matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

respectively. For any single bit operator with matrix  $A$ , its operation on a qubit  $|\psi\rangle$  is defined by  $|\psi'\rangle = A|\psi\rangle$ .

### Existing Quantum LDPC Codes

LDPC codes come from classical computing and are a class of error-correcting codes that use additional bits to check the parity of a bitstring. Modern technologies such as WiFi and 5G use LDPC codes for error correction (Breuckmann & Eberhardt, 2021).

Quantum LDPC codes can be seen as an extension of the classical LDPC code. In 2013, they gained increased attention due to Gottesman's result showing that quantum LDPC codes with a constant encoding rate can reduce the overhead of quantum computation too (Breuckmann & Eberhardt, 2021). Therefore, fault-tolerant quantum computers would not need nonlinearly increasing code sizes and qubit counts to perform large computations.

Two extensively researched and documented families of LDPC codes are those of the toric code and the rotated surface code (Badger, 2021). These codes check for qubit errors that are either bit-flips or phase-flips. The literature refers to these errors as  $X$  or  $Z$  errors respectively, respectively, and they are checked by a code's  $X$ -type and  $Z$ -type ancillae, also respectively. A code's ability to correct for the four possible combinations  $\{I, X, Z, XZ\}$  extends to its ability to correct general quantum errors. For these codes, each qubit is either a data qubit or an ancilla qubit. Data qubits encode data, whereas ancilla qubits support the error-correcting abilities of the code. Figure 2 shows the toric code square lattice with a vertex and a plaquette highlighted.

Though dependent on implementation, data qubits are conventionally placed on the edges, while ancilla

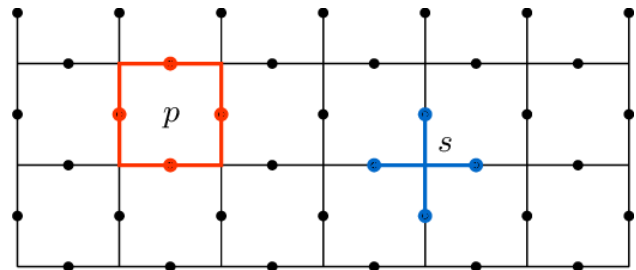


Figure 2. Toric code tiling. Plaquettes are represented in red by  $p$  and vertices in blue by  $s$ . Data qubits are represented in black on the edges of the tiling (Bausch et al., 2017).

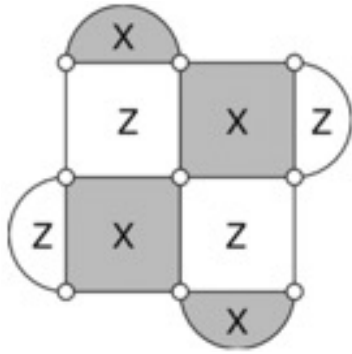


Figure 3. Depth-3 rotated surface code

qubits exist on the vertices and plaquettes. The rotated surface code shown in Figure 3 adopts another placement with data qubits on vertices, and plaquettes representing both kinds of ancilla qubits.

Each ancilla qubit contributes to detecting errors on the data qubits to which it is incident. This is accomplished by entangling the data qubit with its neighboring ancilla qubits. As a result, ancilla qubits provide insight into the state of a data qubit without collapsing that data qubit. For each error-correcting cycle, the set of ancilla qubits that detect an error is called the error syndrome. A decoder uses the syndrome to determine which data qubits have had errors and what types of errors they are. A toric code encodes two logical qubits, and a surface code encodes one.

A hyperbolic surface code is a close relative to the toric code. However, rather than the code being represented by a tiling of Euclidean space, a hyperbolic surface code tiles hyperbolic space. The Schläfli symbol  $\{r, s\}$  lends a method of categorizing such a tiling (Breuckmann et al., 2017). This symbol represents a tiling with  $s$  regular  $r$ -gons meeting at each vertex. Since both the toric and surface codes tile squares with four squares at each vertex, the codes are of Schläfli symbol  $\{4, 4\}$ . This paper focuses on the  $\{4, 5\}$  tiling as it is more efficient for quantum information storage (Breuckmann et al., 2017) and is most similar to the toric code.

Quantum LDPC code parameters are described by the symbol  $[[n, k, d]]$ , where  $n$  is the number of qubits in the code,  $k$  is the count of encoded qubits, and  $d$  is the distance, or maximum amount of error correctable, of the code (Breuckmann & Eberhardt, 2021). For an  $L \times L$  grid, the toric code and rotated surface code have parameters  $[[2n, 2, \sqrt{n}]]$  and  $[[2n, 1, \sqrt{n}]]$ , respectively, for  $n = L^2$ . Therefore, if a code using qubits is a toric or a rotated surface code, the number of encoded qubits remains at a constant 2 qubits or 1 qubit, respectively. Further, the distance scales at rate  $\sqrt{n}$ .

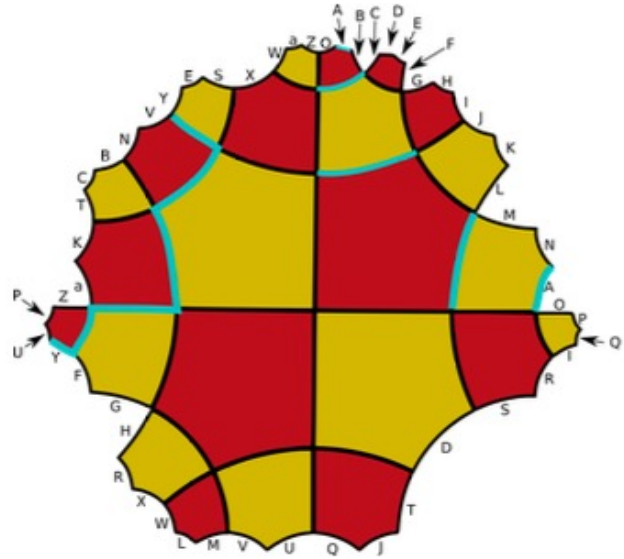


Figure 4. tiling of hyperbolic space (Breuckmann et al., 2017)

In contrast, a two-dimensional qubit hyperbolic surface code has parameters  $[[n, (1 - \frac{2}{r} - \frac{2}{s})n + 2, \Theta(\log n)]]$  for a tiling with Schläfli symbol  $\{r, s\}$ . The number of encoded qubits scales at a rate of  $\Theta(n)$  with its distance  $\Theta(\log(n))$ . Therefore, while a hyperbolic surface code encodes qubits more efficiently, it has a lower limit to its code distance and can correct fewer errors than a toric or rotated surface code.

### Decoders

Given an error syndrome on a QEC code, a decoder solves for the data qubits on which an error occurred and the type of each error. It then decides what corrective operations to perform on the code. The most common

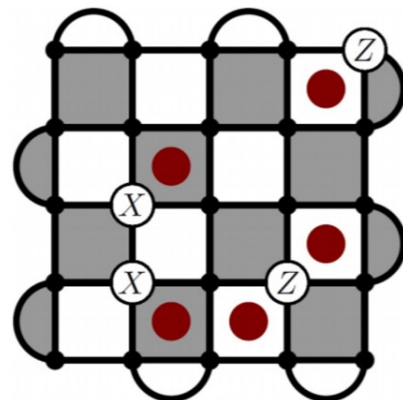


Figure 5. Example of a depth-5 surface code. Xs and Zs denote errors and red dots denote ancilla detections (Badger, 2021)

algorithmic decoder is the MWPM decoder, which finds the most likely path between two endpoints on a QEC code. Should a chain of adjacent data qubits experience error on a QEC code, the subsequent “error chain” is marked by ancilla qubits that detect the error. Figure 5 illustrates the relationship between a set of data qubit errors and the surface code’s corresponding error syndrome.

While the MWPM algorithm is fast and accurate, it assumes that errors are independent and have equal probability. Real-world quantum systems are unlikely to follow this assumption. Therefore, neural network decoders are an auspicious research avenue since they decode independently of statistical assumption. Further, while the MWPM algorithm runs in  $O(n^2)$  time, a neural network runs in  $O(1)$  time. This allows for more frequent QEC cycles in real-world applications.

Equivariance is a property of systems for which applying a symmetry transformation to the input produces the corresponding symmetry transformation in the output. CNNs are one example of such systems and have great potential in their application to surface codes. Their equivariance allows them to recognize error syndrome patterns and features irrespective of the position or orientation of the syndromes. CNNs have been shown to decode toric codes with greater accuracy than both MWPM and feed-forward decoders (Egorov et al., 2023).

## EXPERIMENT METHODOLOGY

This experiment aims to evaluate the performance of a CNN decoder against the performance of an MWPM algorithm in the context of decoding a two-dimensional hyperbolic surface code. Therefore, a large dataset is needed to train the CNN decoder. Specifically, this project focuses on evaluating decoder performances on a series of {4, 5} tiled hyperbolic surface code of parameters  $[[60,8,4]]$ ,  $[[160,18,6]]$ , and  $[[360,38,8]]$ . These are the smallest codes of this tiling.

Since there are  $4^n$  possible decodings for a code with data qubits, it is infeasible to generate an exhaustive dataset. Therefore, this experiment proposes the following dataset generation method. Given a depolarizing noise model (Egorov et al., 2023) from which to sample errors, for each error, compute the error syndrome on the series of codes detailed above. This experiment generates  $10^6$  samples for each surface code parameter set. The error syndrome and correcting qubit operations will serve as the input and output, respectively, for the supervised learning tasks.

This experiment then implements an MWPM decoder and a CNN decoder for each of the codes. The MWPM decoder serves as a baseline performance measure for the

CNN decoder. The CNN adapts the wide-resnet (WR) architecture used by Egorov et al. (2023) and uses the AdamW optimizer for hyperparameter tuning (Egorov et al., 2023). Logical accuracy, the number of decoded syndromes over the total syndromes, is used to evaluate and test the decoders. This accuracy is assessed at probability thresholds of 0.155, 0.155, 0.187, and 0.18, used by Egorov et al. for the sake of intermodel comparison.

## CONCLUSION AND FUTURE WORK

Effective QEC will enable effective quantum computing and provide a tremendous advantage against adversary information systems. Unlike most modern neural decoders, equivariant neural decoders leverage code symmetries to bolster decoder performance. Therefore, should such decoders yield better logical accuracy results than MWPM on the hyperbolic surface code, they should be regarded as a promising avenue into quantum LDPC code decoders. Therefore, hardware implementations of such a neural decoder should be investigated. Since such implementations have been shown to operate fast enough for real-time error correction on a rotated surface code (Overwater et al., 2022), similar hardware implementation may be promising for a hyperbolic code.

Further work would seek to expand equivariant neural decoders to other quantum LDPC codes. In particular, the family of “good” quantum LDPC codes (Panteleev and Kalachev, 2022) presents a promising class of codes. These codes have logical encoding rates and distances that scale linearly with the qubit count, exceeding those measures in toric, rotated surface, and hyperbolic codes alike.

## REFERENCES

- Badger, C. (2021). *Performance of various low-level decoder for surface codes in the presence of measurement error*. <https://scholar.afit.edu/cgi/viewcontent.cgi?article=5888&context=etd>
- Bausch, J., Cubitt, T. S., Lucia, A., Pérez-García, D., & Wolf, M. S. (2017). Size-driven quantum phase transitions. *Proceedings of the National Academy of Sciences*, 115(1), 19–23. <https://doi.org/10.1073/pnas.1705042114>
- Breuckmann, N., & Eberhardt, N. J. (2021). *Quantum LDPC codes*.
- Breuckmann, N. P., Vuillot, C., Campbell, E., Krishna, A., & Terhal, B. M. (2017). Hyperbolic and semi-hyperbolic surface codes for quantum storage. *Quantum Science and Technology*, 2(3), 035007. <https://doi.org/10.1088/2058-9565/aa7d3b>
- Egorov, E., Bondesan, R., & Welling, M. (2023). *The END: An equivariant neural decoder for quantum error correction*. <https://doi.org/10.48550/arXiv.2304.07362>

Martin, B. (2022). *Evaluating neural network decoder performance for quantum error correction using various data generation models*. <https://scholar.afit.edu/cgi/viewcontent.cgi?article=6483&context=etd>

Overwater, R. W. J., Babaie, M., and Sebastiano, F. (2022). Neural-network decoders for quantum error correction using surface codes: A space exploration of the hardware cost-performance tradeoffs. *IEEE Transactions on Quantum*

*Engineering*, 3, 1–19. <https://doi.org/10.1109/tqe.2022.3174017>

Panteleev, P., and Kalachev, G. (2022). *Asymptotically good quantum and locally testable classical LDPC codes*. <https://doi.org/10.48550/arXiv.2111.03654>

Shyu, H. (2022). *USD(R&E) Technology Vision for an Era of Competition*. [online] Available at: [https://www.cto.mil/wp-content/uploads/2022/02/usdre\\_strategic\\_vision\\_critical\\_tech\\_areas.pdf](https://www.cto.mil/wp-content/uploads/2022/02/usdre_strategic_vision_critical_tech_areas.pdf).

# Exploring the Use of UAV-Based Traffic Monitoring for Real-Time Routes Optimization for Military Vehicles

Dr. Claudio Martani

Laboratory for Future-Ready Infrastructure (FuRI Lab)  
School of Construction Management Technology  
Purdue University

**Abstract** Routes optimization for military vehicles is a critical task that affects the several (sometimes conflicting) interests of multiple stakeholders. As such, it cannot be done using simple indicators of single services. The hypothesis of this paper is to use hazard mapping from unmanned aerial vehicle monitoring, and decision optimizations based on the utilitarian approach, to quantitatively and rigorously select the optimal routing path for military vehicles, accounting for the interests of all involved stakeholders and the uncertainty on the hazards. To this scope a method is proposed, based on the utilitarian approach used in infrastructure asset management, that consists of four main steps: (1) set the boundaries of the analysis, (2) define an objective function and consistent impact hierarchy, (3) identify a hazard and define alternative candidate paths, and (4) estimate the consequences for each candidate path and select the optimal one. The use of the method is then demonstrated using a fictive example, and conclusions are drawn on the suitability of the method for use in practice. Finally, indications are also provided on the envisioned further research required to overcome the limitations of this exploratory work.

## INTRODUCTION

Routes optimization for military vehicles is a critical task that requires the ability to properly account for the risks connected to alternative paths, e.g., the risk to encounter a hazard—such as an attack—in each of the possible paths.

Real-time routes optimization considering uncertain conditions is now a consolidated practice. This is what, for example, is done by satellite navigators for civil use that can adjust live the suggested route based on current or predicted traffic conditions. These route optimizations are typically done considering simple service indicators such as travel time or travel distance.

Despite being very useful in everyday life, e.g., driving in city traffic, routes optimizations using simple indicators of single service (e.g., the shorter or the faster route) is not suitable for path management of military vehicles. This is because the routes chosen by military vehicles impact numerous services (sometimes conflicting) provided to multiple stakeholders, such as the cost of operation and maintenance of the vehicles by the army, the risk of travel delay and accidents both for the users of the military vehicles and for civilians driving on the same roads. To properly handle the complexity of the interests involved, the routes of military vehicles should be optimized considering the probability hazards such as attacks and the impacts on all involved stakeholders.

In infrastructure asset management, the utilitarian approach has been largely used in recent years to quantitatively, rigorously, and orthogonally (i.e., without double counting) optimize decisions affecting multiple stakeholders (Adey et al., 2019; Esders et al., 2020; Martani et al., 2022; Adey et al., 2022). Although its use has never been attempted for routes optimization, from a methodological standpoint no logical impediment exists in translating the use of the utilitarian approach to this context. To also account for the probability of an attack, a real-time mapping of hazards is needed. The midrange mapping of territories to identify potential hazards appears to be possible using unmanned aerial vehicles (UAV) with RGB cameras and motion sensors (Giordan et al., 2017), along with artificial intelligence-based algorithms to recognize hazards from the images (Tian, 2020).

The hypothesis of this paper is to use hazard mapping from UAV monitoring and decision optimizations based on the utilitarian approach to quantitatively and rigorously select the optimal routing path for traveling military vehicles, accounting for the interests of all involved stakeholders and the uncertainty of the hazards.

### ***A New Method to Optimize the Routes of Military Vehicles in Real Time***

To optimize the routes of military vehicles, accounting for the interests of all involved stakeholders and uncertainty about hazards, a method is proposed in this paper



based on the utilitarian approach used in infrastructure asset management (Adey et al., 2019). The method consists of four main steps: (1) set the boundaries of the analysis, (2) define an objective function and consistent impact hierarchy, (3) identify a hazard and define alternative candidate paths, and (4) estimate the consequences for each candidate path and select the optimal one. Each step is described in the following subsections using a fictive example.

### SET THE BOUNDARIES OF THE ANALYSIS

The example consists of optimizing the route for one troop traveling on a military vehicle. The troop will need to travel choosing among the 26 edges of the road network,

characterized by the dimensions and traffic conditions as described in Figure 1. In this example it is also considered that civilian vehicles are not allowed (for safety reasons) to travel on the same edges where the military vehicles pass. Therefore, in this example it is considered that civilian vehicles are rerouted from the path where the military vehicles travel for the time of their passage.

### DEFINE AN OBJECTIVE FUNCTION AND CONSISTENT IMPACT HIERARCHY

In order to optimize the decision on the path, an objective function with its consistent impact hierarchy is to be determined (Adey et al., 2020). In this example the interest of four categories of stakeholders were considered (Table 1):

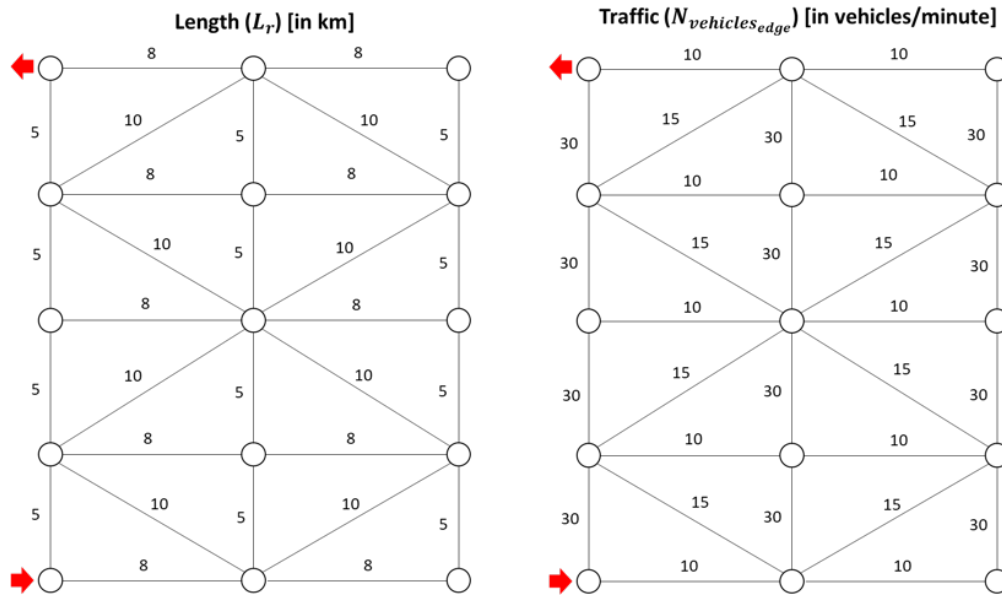


Figure 1. Schematic representation of the road network with indications of the lengths (left) and traffic (right) of each edge of the network.

Table 1. Impact hierarchy for the optimization

Stakeholder		Symbol	Impact	Symbol	Unit value	Unit
Owner	Army	$C_{tr}$	Cost of the troop	$UC_{tr}$	10,000,000	\$/troop
Users	Staff	$C_{t_u}$	Travel time	$UC_{t_u}$	5	\$/min
		$C_{a_u}$	Accident	$UC_{a_u}$	50,000	\$/person
		$C_{pd_u}$	Property damage	$UC_{pd_u}$	1,000	\$/accident
DAP	Civilians using the road	$C_{t_{dap}}$	Travel time	$UC_{t_{dap}}$	10	\$/min
		$C_{a_{dap}}$	Accident	$UC_{a_{dap}}$	50,000	\$/accident
		$C_{pd_{dap}}$	Property damage	$UC_{pd_{dap}}$	20,000	\$/accident
IAP	Society	$C_{d_{iap}}$	Delay	$UC_{t_{iap}}$	100	\$/min
		$C_{l_{iap}}$	Loss of goods	$UC_{l_{iap}}$	1,000,000	\$/accident

the owner, the users, and directly and indirectly affected people (DAP and IAP). Given the demonstrative purpose of this example, the unit values in Table 1 are fictive.

The objective function for the analysis is the minimization of all negative impacts (here called costs) of all involved stakeholders, as reported in equation (1).

$$\text{Min } (Z) = \min (C_o + C_u + C_{DAP} + C_{IAP}) \quad (1)$$

where  $C_o$  is the cost for the owner,  $C_u$  is the cost of the users,  $C_{DAP}$  is the cost for DAP, and  $C_{IAP}$  is the cost for IAP. Details on the estimate of each of these costs is reported in equations (2) to (13), and the parameters involved are provided in Table 2.

$$C_o = P_{acc} * C_{tr} \quad (2)$$

$$C_u = C_{t_u} + C_{a_u} + C_{pd_u} \quad (3)$$

$$C_{t_u} = (1 - P_{acc}) \cdot (L_r \cdot T_I \cdot N_{p_{group}} \cdot UC_{t_u}) \quad (4)$$

$$C_{a_u} = \sum_{edge=1}^E (P_{acc_{edge}} \cdot N_{p_{group}} \cdot UC_{a_u}) \quad (5)$$

$$C_{pd_u} = \sum_{edge=1}^E (P_{acc_{edge}} \cdot N_{p_{group}} \cdot UC_{pd_u}) \quad (6)$$

$$C_{dap} = C_{t_{dap}} + C_{a_{dap}} + C_{pd_{dap}} \quad (7)$$

$$C_{t_{dap}} = ((1 - P_{acc}) \cdot (N_{vehicles_{edge}} \cdot N_{drivers} \cdot Re_d \cdot Re_t \cdot UC_{a_{dap}})) + ((P_{acc}) \cdot (N_{vehicles_{edge}} \cdot N_{drivers} \cdot T_{res} \cdot Re_t \cdot UC_{a_{dap}})) \quad (8)$$

$$C_{a_{dap}} = \sum_{edge=1}^E (P_{acc_{edge}} \cdot N_{vehicles_{edge}} \cdot N_{drivers} \cdot UC_{a_{dap}}) \quad (9)$$

$$C_{pd_{dap}} = \sum_{edge=1}^E (P_{acc_{edge}} \cdot N_{vehicles_{edge}} \cdot N_{drivers} \cdot UC_{pd_{dap}}) \quad (10)$$

$$C_{iap} = C_{t_{iap}} + C_{l_{iap}} \quad (11)$$

$$C_{t_{iap}} = (1 - P_{acc}) \cdot (L_r \cdot T_I \cdot N_{iap} \cdot UC_{t_{iap}}) \quad (12)$$

$$C_{l_{iap}} = \sum_{edge=1}^E (P_{acc_{edge}} \cdot UC_{l_{iap}}) \quad (13)$$

### IDENTIFY A HAZARD AND DEFINE ALTERNATIVE CANDIDATE PATHS

In this step, it is assumed that given the information provided by a UAV (here replaced by an assumption), a hazard has been identified in the proximity of one edge of the network (Figure 2, top left). Based on the position of the hazard and on the point of entrance and exit of the network (marked with the two red arrows in Figure 2), the seven candidate paths to be evaluated are reported in Figure 2. One (path 1) passes directly on the

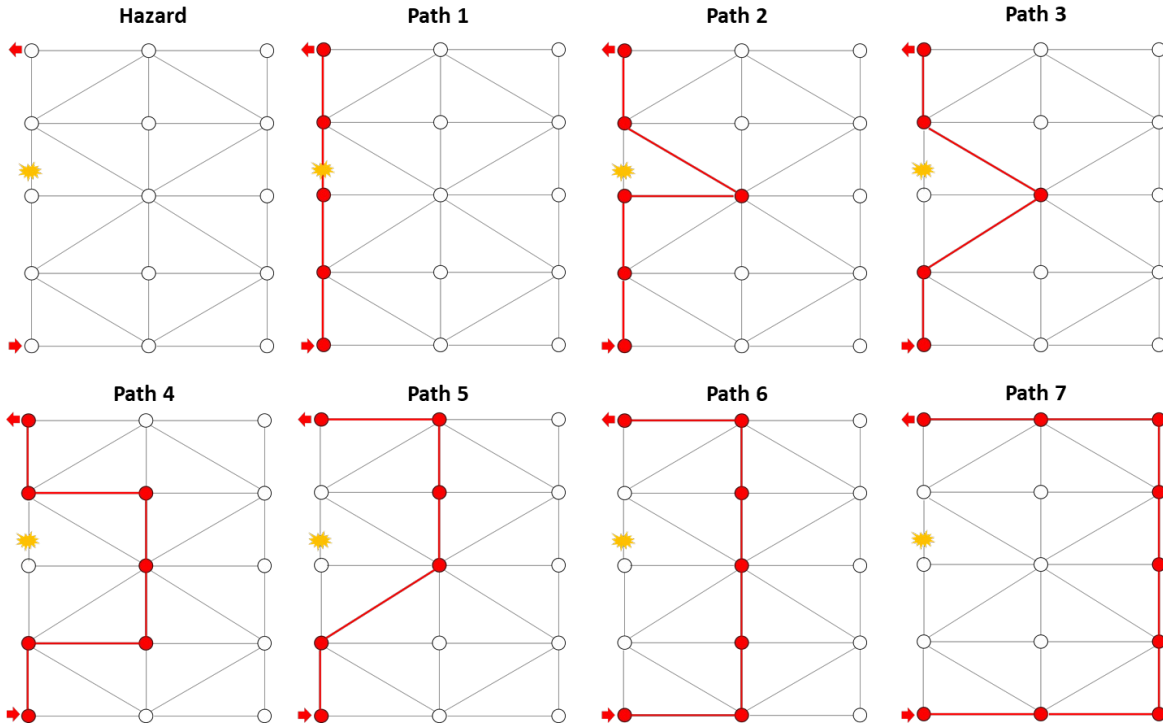


Figure 2. Localization of the hazard in the road network and the seven candidate paths considered.

edge directly involved in the potential hazard and some (paths 2 and 3) pass on edges adjacent to it. The others pass on all edges that are further away from the identified hazard.

### ESTIMATE THE CONSEQUENCES FOR EACH CANDIDATE PATH AND SELECT THE OPTIMAL ONE

The consequences to the services provided to all stakeholders, connected to each of the seven candidate paths (defined in step 3) on the road network (defined in step 1) are estimated according to the objective function (defined in step 2). The results show that the optimal route is Path 4, with less than \$16 million of total impact (Figure 3, top left). This is mostly due to the important reduction in the costs for DAP (Figure 3, top right). Indeed, the costs for all other stakeholders seem to vary modestly for each of the paths, while these for DAP are these with the most significant variation, weighting substantially on the overall estimate. In particular, it is the impact on the travel time for DAP to change greatly for different paths (Figure 3, bottom). This is due to the fact that, according to equation (8), the estimate of travel time for DAP is affected by both rerouting caused by the passage of the military vehicles and rerouting caused by accidents (i.e.,

traffic deviations during the restoration of the road after an attack). Therefore, Paths 1 and 2 have a higher risk of accident, since they pass either directly on the edge involved in the potential hazard or on one adjacent to it, while the other paths do not but involve progressively more edges and therefore impact on more civilian vehicles (according to the traffic provided in Figure 1). Path 4 is the most balance points between the two effects and, as such, results in the lowest impact on the travel time for DAP.

Although Path 4 is the optimal route when considering all the interests of all stakeholders, as described in Table 1, this may not be the case when looking specifically at one or a few services. For example, the breakdown of impacts for each specific service reported in Figure 4 shows clearly that Path 4 is far from being the optimal solution when the decision-maker would be interested in minimizing the cost of delays for IAP or of travel time for the users, i.e., the staff of the troop. It is also not the best one for minimizing the negative impact in terms of accidents and property damage, both for users and DAP. This is useful to observe when making the decision because while optimizing the route for all interests involved in the objective function, it also allows quantifying rigorously and orthogonally the effect of decisions on all

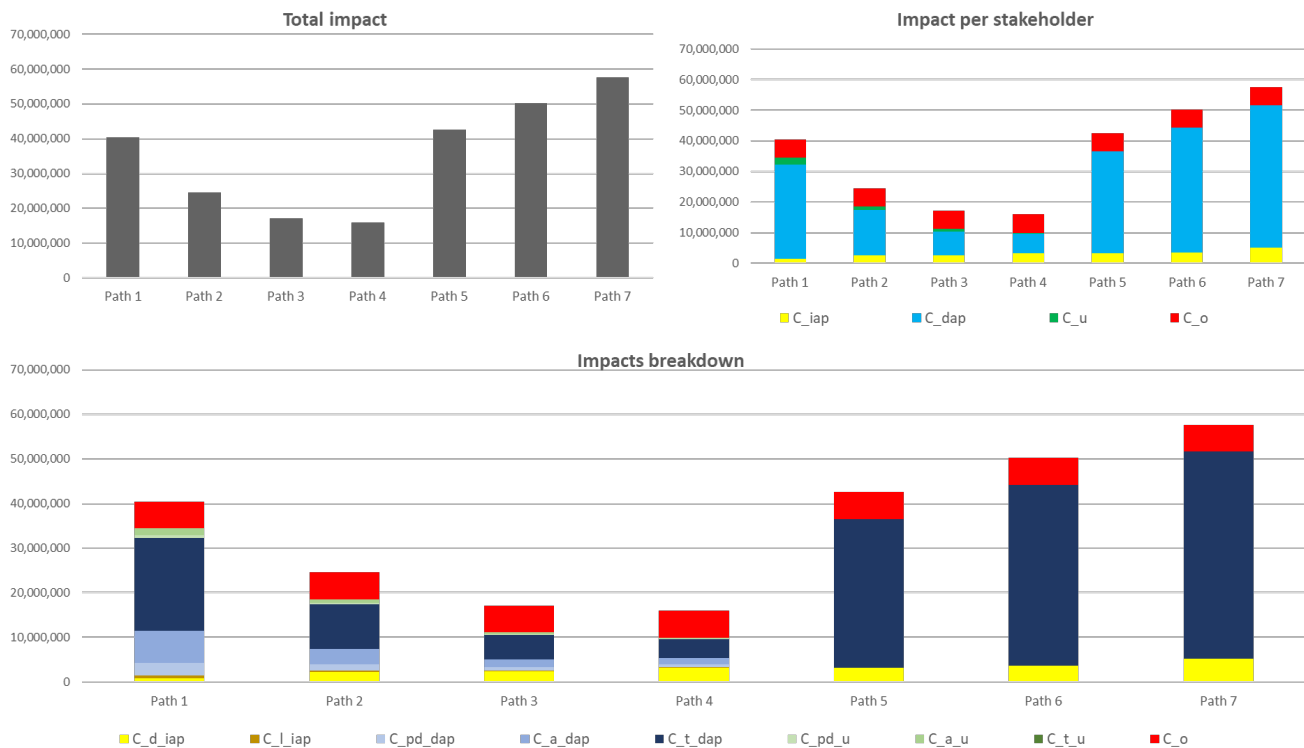
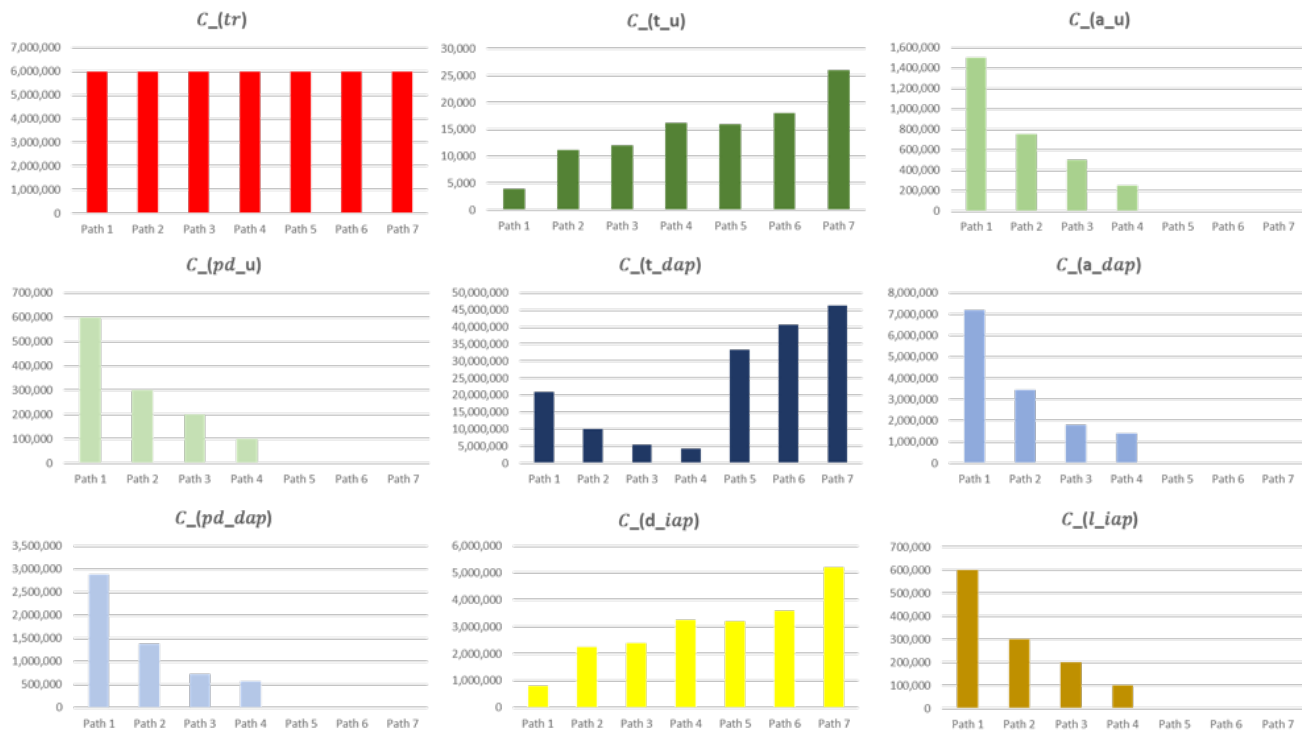


Figure 3. Estimated impact associate with each of the seven paths, displayed in total (top left), cumulated per stakeholder (top right), and per specific type of impact (bottom). The values on the y-axes are expressed in dollars.



**Figure 4.** Estimated impact associate with each of the seven paths, displayed per each of the nine specific types of impact on services. The values on the y-axes are expressed in dollars.

stakeholders, giving a clearer view of the broad effect of the choices.

## CONCLUSIONS

The method proposed in this article to optimize paths for military vehicles in real time has been demonstrated to be suitable for use in practice for quantifying rigorously and orthogonally the effect of decisions on all stakeholders. Despite the encouraging indications of this preliminary study, further research is envisioned by the author to overcome some limitations of this initial exploratory phase. In the immediate future the author intends to

- verify the usability of the method in real situations by replacing the fictive example with a real case study, where (i) hazards are mapped using UAV to verify the quality of information provided, (ii) realistic assumptions on the rerouting policies have to be defined, and (iii) precise estimates of the rerouting time needs to be made using traffic models;
- validate the quality of the predictions. The method needs to be first calibrated and then validated using real situations from the past where the outcome of route decisions is known.

Moreover, and with a view to the long term, the ability to optimize paths could have large-scale implications in the future for the development of adaptable roads, i.e., roads able to optimize the space allocation for use demand (Valença et al., 2021).

To achieve both the short-term objectives and the long-term view, a PhD position has recently been opened by the author at the Purdue FuRI Lab for candidates from the Purdue Military Research Institute to investigate the use of UAV for the development of adaptable roads.

## REFERENCES

- Adey, B. T., Burkhalter, M., & Martani, C. (2020). Defining road service to facilitate road infrastructure asset management. *Infrastructure Asset Management*, 7(4), 240–255. <https://doi.org/10.1680/jinam.18.00045>
- Adey, B. T., Martani, C., & Hackl, J. (2022). Investing in water supply resilience considering uncertainty and management flexibility. *Proceedings of the Institution of Civil Engineers—Smart Infrastructure and Construction*, 175(3), 104–115. <https://doi.org/10.1680/jsmic.21.00005>
- Adey, B. T., Martani, C., Papathanasiou, N., & Burkhalter, M. (2019). Estimating and communicating the risk of neglecting maintenance. *Infrastructure Asset Management*, 6(2), 109–128. <https://doi.org/10.1680/jinam.18.00027>

- Esders, M., Martani, C., & Adey, B. T. (2020). Decision-making model of residential redevelopment: A multi-disciplinary perspective. *International Journal of Architecture, Engineering and Construction*, 9(4), 1–21. <https://doi.org/10.7492/IJAEC.2020.029>
- Giordan, D., Manconi, A., Remondino, F., & Nex, F. (2017). Use of unmanned aerial vehicles in monitoring application and management of natural hazards. *Geomatics, Natural Hazards and Risk*, 8(1), 1–4. <https://doi.org/10.1080/19475705.2017.1315619>
- Martani, C., Eberle, S., & Adey, B. T. (2022). Evaluating highway design considering uncertain mobility patterns and decision flexibility. *Infrastructure Asset Management*, 9(3), 135–155. <https://doi.org/10.1680/jinam.21.00018>
- Tian, Y. (2020). Artificial intelligence image recognition method based on convolutional neural network algorithm. *IEEE Access*, 8, 125731–125744. <https://doi.org/10.1109/ACCESS.2020.3006097>
- Valença, G., Moura, F., & de Sá, A. M. (2021). Main challenges and opportunities to dynamic road space allocation: From static to dynamic urban designs. *Journal of Urban Mobility*, 1, 100008.

## Using Just-in-Time Training to Evaluate Retention

Mason Lane, Madison Thomas, J. Eric Dietz, PhD, PE, and Rylee Lane

**Abstract** Active shooter events are on the rise throughout the United States. This study utilizes just-in-time training to identify how it can assist traditional crisis response training in K-12 schools. There has been limited prior research evaluating the retention of knowledge gained from just-in-time training. The results of this study showed after three months that there was no loss in information retention regarding active shooter responses. Therefore, training once per semester is sufficient to establish and maintain active shooter responses. Just-in-time training is an effective training method to save schools money and time when training.

### INTRODUCTION

The purpose of this study is to examine how just-in-time training can assist traditional crisis response training in K-12 schools and, if it helps, what frequency of training is the most effective for information retention. Understanding the most beneficial frequency will provide organizations information to keep their employees safe and informed while being time- and cost-effective.

Research has shown that it is common for schools to experience some type of crisis event during the school year (Gurdineer, 2013). Thus, it is important to develop a crisis plan to deal with these events. Researchers evaluated demographics and resources (such as training and materials) for effectiveness regarding school crisis plans. Demographics and amount of training had a significant impact on quality of school crisis plans, but the resources included in the quality plans were found to have a bigger impact on the effects of the crisis plans (Gurdineer, 2013). Crisis team members and schools without written crisis plans were the biggest variables affecting the quality of crisis plan implementation. The number of crisis team members had a positive correlation with the quality of the crisis plan. State funding for schools can affect how many people can be on a crisis team, but funds are essential in order to strengthen a crisis plan. Crisis management training is a part of the teacher's role in leadership at a school. The more professionalism and trust teachers provide, the more students will trust and follow their lead. An abundance of leadership can cause students to perceive the teacher as strict and deficient, which can cause a lack of obedience in students (Tschannen-Moran, 2009). Therefore, a balance of both is required to effectively manage student impressions.

In addition to managing leadership, teachers are asked to deal with large class sizes, training related to their profession, daily lesson preparedness, and disruptive student behavior. Teachers turn to administrators to provide necessary training and help with disruptive

students (Lee, 2008). Crisis training is one type of training teachers want assistance on, so they can act appropriately in a crisis. Lee found that teachers do not perceive themselves as capable of managing a crisis because they do not receive enough practice on safety planning skills (Lee, 2008). Administrators need to assist teachers with training to increase their confidence about the proper procedure to follow in a crisis. In a training session, one school administrator noted, “I’m not worried about having a crisis plan in my school because I have it all in my head” (Lee, 2008, p. 4). Crisis plans are useless unless the plan is written down and learned. Experts have warned that without training for faculty, crisis plans do not work (Lee, 2008). Schools need crisis plans and training for crisis prevention and preparation.

Prevention, intervention, and postvention are most likely lacking in the Comprehensive Crisis Plan Checklist (CCPC). Intervention programs that can be added to a CPCC to improve its quality are dealing with crowd issues after a crisis, identification of dead and wounded, and victims of violence. Additionally, postvention programs can improve the quality of a crisis plan by adding a plan to inform students and families about the crisis, parent-child reunification, and sign-out procedures after the crisis event (Gurdineer, 2013). Although these areas require dedicated funds, adding these programs to the crisis plan can improve the quality of a school's CPCC.

Active shooters have become an issue in current crisis management. An active shooter is a suspect whose activity is immediately causing death and serious bodily injury (Williams, 2015, p. 4). Since active shooter events are spontaneous and unpredictable, it is important for organizations to follow National Incident Management System (NIMS) guidelines. NIMS is a nationally recognized emergency operation plan that is adapted for large crisis incidents (Williams, 2015). NIMS is important to follow because it requires cooperation among local law enforcement and the efficient use of resources and information in the case of a crisis.

The city of Houston, Texas, developed RUN.HIDE.FIGHT. (RHF) to better prepare for active shooter incidents (Houston Emergency Management, 2002). The goal for this strategy is to lower the casualty rate in an active shooter incident. The first step in the process is to run and get out of the active shooter area. If running is not an option, the next step is to hide by getting to a place that is out of the shooter's point of view. Last, if hiding is not an option, then fight by attempting to disarm the shooter. RHF has been implemented in both public and private sectors across the United States.

Over the past 15 years, school safety during active shooter events has been a focal point in the United States. During this period, schools have implemented active shooter policies and training. Implementing an active shooter training program can be difficult, as there is no one-size-fits-all approach (Rorie, 2015). Many activities occur throughout the school day: students are in class and are moving through the hallways to other classes, teachers are on breaks. At night, students might be engaging in extracurricular activities. In addition, location impacts the necessary procedures and training for an active shooter. The Denver Department of Health adopted the three-step RUN.HIDE.FIGHT strategy for staff members to follow in the case of an active shooter situation (Rorie, 2015). Additionally, the Denver Department of Health published training videos that employees can watch to refresh their active shooter exercises (Rorie, 2015). Implementing an active shooter training program keeps employees prepared for an active shooter event. Active shooter training videos, the three-step run-hide-fight strategy, and practicing with first responders are three techniques that can assist in the implementation of an active shooter plan.

Another strategy developed after the Columbine High School shooting was AvoidDenyDefend (ADD). ADD is taught in the advanced law enforcement rapid response training that Texas State University puts on to train emergency responders about active shooter incidents (Texas State University, 2004). ADD and RHF follow the same concepts but use different terms to describe them. The first step in ADD is to "avoid" the area where the shooter is and to have an exit plan. If avoiding is not an option, the next step is to "deny" the shooter by creating barricades for protection from the threat in a sheltered place. If avoiding and denying are not an option, then "defend" by being aggressive and committing to how you plan on disarming the shooter.

The RHF philosophy was tested with the 1999 Columbine shooting to see if it would have reduced casualty rates (Lee, 2019). (RHF was created retroactively to the shooting.) AnyLogic was used to simulate the philosophy inside the Columbine library. Three scenarios tested—run, hide, and fight—with 56 agents/individuals

in the library. In the run scenario, it was found that the survival probability for running is 92.1%, which is 30.4% higher than the Columbine event (Lee, 2019). A critical part of surviving during the run scenario was knowing the escape plan and where the active shooter was. The hide scenario resulted in a survival probability of 5.16%, which is 57.1% lower than the Columbine event (Lee, 2019). Placing locks on doors can help slow a shooter by keeping them out of rooms where individuals are hiding. Last, the fight scenario resulted in a survival probability of 97.6%, which is 35.7% higher than the Columbine event (Lee, 2019). Swarming the shooter allowed them to block the shooter from firing. Hiding is the least effective action to take during an active shooter situation. Overall, depending on the active shooter situation, the RHF philosophy decreases the number of casualties.

Duration of an active shooter event can vary. Police response is dependent on how far the police station is from the school. Research has been done comparing the number of casualties to the time to engage based on various scenarios. The scenarios are basic (no resource officer or concealed weapons carry), resource officer, 5% of the people with a concealed weapon, 10% of the people with a concealed weapon, 5% of the people with a concealed weapon and a resource officer, and 10% of the people with a concealed weapon and a resource officer (Anklam et al., 2015). Based on the analysis, the researchers found that the time to engage and the number of casualties was the lowest in the scenarios: resource officer, 5% of the people with a concealed weapon and a resource officer, and 10% of the people with a concealed weapon and a resource officer (Anklam et al., 2015). These results show that there are multiple ways to defend against active shooter events and eliminate casualties.

For an active shooter situation, shelter-in-place and lockdown are two terms that can be misused in a crisis management plan for safety. The difference between shelter-in-place and lockdown is based on the type of emergency: natural or technological events versus human-led incidents. Human-led incidents are commonly known as an active shooter situation or a civil disturbance. When a lockdown occurs because of an active shooter situation, people are asked to remain where they are and barricade the doors. The purpose of a lockdown is to prevent the shooter from entering rooms to cause harm to individuals and to make sure individuals do not wander into the "hot" zone. An example of a shelter-in-place scenario is the outcome of severe weather or a chemical disturbance (Worsham, 2017). While sheltering in place, individuals are instructed to go to a chosen room, noted in the crisis plan, and to remain away from danger. Training for both situations is essential once both crisis plans are established.

Shelter-in-place, over time, has been shown as a safer approach than trying to evacuate students into a potentially contaminated or dangerous environment (White, 2018). While a shelter-in-place is in effect, no one can leave until the situation is contained or safe. Most lockdowns in schools occur because of police activity unrelated to the school, but close to it (White, 2018). In a lockout scenario, just the school is locked, and no one can leave or enter, but school still runs normally (White, 2018). In a lockdown scenario, students are supposed to hide in rooms (White, 2018). Lockdown would occur during the hide part of the RHF philosophy.

Revisiting active shooter policies and protocols is essential to creating a quality crisis management plan. Most active shooter protocols contain the same advice: implement lockdown procedure, minimize the target profile, and wait for the police to neutralize the situation (Buerger & Buerger, 2010). Essentially, the policy is to hide in place and hope the active shooter does not find individuals. The problem with these procedures is that they do not account for crowded classrooms or rooms that are locked when the student arrives. A crisis may occur during lunchtime or during passing periods when many students are not in a classroom. Cell phones can compromise victims hiding in place if a phone rings and the shooter locates the victims. Since active shooters are commonly first identified by students, communication is important to enable response teams to act quickly and effectively (Buerger & Buerger, 2010). Without quick and effective communication, an effective crisis plan will not work.

In unique situations, there are critical issues that occur when following active shooter policies. Included in most of the school's active shooter policies, the policy is to lock down the school in the case of an active shooter. However, this practice locks out the first responders coming to help. Special Weapons and Tactics (SWAT) team members have advanced training in breaching, but local police are not trained extensively on breaching (Nichols, 2010). Issues with breaching may occur in a rural area where a SWAT team is not present. Critically evaluating and updating active shooter policy and training is essential to finding critical issues. Focusing on what can be learned from other active shooter tragedies can benefit current active shooter policies and training in schools.

School shooting drills are now being substituted for fire and tornado drills given the frequency of active shooter events in the United States (Shah, 2013). States are looking into making laws about different types of safety drills. The executive director of the National School Safety Center said, "whether the additional practice and paperwork will actually improve schools' defense against shooters and intruders is hard to say" (Shah, 2013). Crisis management training is continually changing due to

actively occurring events; therefore, having one-size-fits-all training is difficult (Shah, 2013). Multiple training sessions occur at schools because a single uniform training takes time away from education. Drills can take 15 to 45 minutes, depending on the drill (Shah, 2013). A fire drill can take 15 to 30 minutes, depending on building size, speed of evacuation, and whether the drill is coordinated with emergency first responders (Weill Cornell Medicine, 2018). An active shooter drill can take the same amount of time. The average length of an active shooter event is 10 minutes, and it takes on average 12 to 15 minutes before law enforcement arrives at the scene (Destein, 2016). Often, when the drill is over, students lose focus, teachers lose preparation time, and school administrators must complete written safety plans and audits (Shah, 2013). Crisis management training is critical because it is life-saving training. The training is effective only if schools complete the crisis response training as it is written in the crisis management plan. Crisis training needs to be efficient and effective because a crisis can happen at any moment and individuals need to be prepared to react.

Traditionally, training is necessary to prepare, avoid, or mitigate a crisis that may occur. Training techniques change over time because of past events and lessons learned from the events. After the Sandy Hook Elementary School shooting in 2012, administrators changed their training and crisis response procedures as they were deemed outdated and obsolete and therefore ineffective during the event. The Sandy Hook final report, published by the Federal Bureau of Investigation, provided recommendations on ways to improve training for active shooter events and called for a revisit of the policies they had in practice (Malloy, 2015). Some of these recommendations were for procedures to provide full-perimeter lockdown capabilities, to establish safe havens where building occupants can lock the door from the inside, and to include school custodians as part of school security and safety committees (Malloy, 2015). Due to the Sandy Hook incident, these recommendations for training and safety have been implemented.

As a result of previous school shootings, current practice is that each school has its own active shooter policy (Wisconsin Association of School Boards, 2016). Due to the current epidemic of active shootings occurring across the country, it is imperative that training be conducted to increase the effectiveness of the active shooter plan. The University of Wisconsin published a crisis communication case study about the shooting at Antigo High School during its prom. The active shooter did not make it into the building before the police took control of the situation (Wisconsin Association of School Boards, 2016). The active shooter policy that Antigo High School had in place was correctly followed by the prom



staff. Since the active shooter situation happened during the prom, there were more chaperones than school workers (Wisconsin Association of School Boards, 2016). The chaperones need to be provided with proper training to be able to respond correctly to the current crisis plan. Not only do these active shooter case studies provide acceptable recommendations and lessons, but they also inform schools around the country about issues that could happen at their schools and help them improve their crisis plans based on past events.

School leaders have a large influence on efficiency and frequency of training. Government agencies cannot mandate every school's crisis training policy and procedure; therefore, schools must take charge of its policies and procedures for training. Based on the importance of school leaders in crisis training, a study was conducted to see the perceptions school leaders had on active shooter training. Ryals sent out a survey to 228 parochial and public school leaders across six school districts in Louisiana; of those, 93 responded to the survey. Of the 93 respondents, 60 were parochial school leaders and 33 were public school leaders (Ryals, 2014, p. 64). With these results, the research found that the biggest complaint among school leaders was the anxiety an active shooter drill may cause for the students, staff, and parents. The results also showed that the school leaders' favorite component was to bring in law enforcement to help with the training (Ryals, 2014). Including law enforcement in the school training can aid both the school's and the officers' training. Also, it provides more of a real-life crisis event when an organization includes law enforcement. At a time when the frequency of shootings is increasing, it is more important to implement successful training to make sure the faculty, students, and staff know how to effectively respond to a crisis. Ultimately, this responsibility falls on the school executive.

As in all states, the Indiana Department of Education provides standards on training required for schools inside its jurisdiction. Although each school may have different protocols and procedures based on location and resources, all are required to meet the Indiana Department of Education standards. Schools are required by the state to do two training sessions per year for manmade occurrences, one of which must be a lockdown/lockout drill (McCormick, 2018). Lack of or poor quality of training is apparent when a crisis happens. One of the recommendations that the State of Indiana has for its schools is to incorporate school safety and risk recognition training into new-teacher training programs as this could potentially help with crisis prevention (McCormick, 2018). The Security School Safety Board, under the Indiana Department of Homeland Security, has given \$53 million to schools since 2014 for additional safety equipment and threat

assessment training (McCormick, 2018, p. 4). A study was done to see how many schools in Indiana hold joint training exercises to stay current and prepared for an emergency; 71% either do not or are not sure (McCormick, 2018, p. 18). Government agencies mandate general guidelines for schools inside their jurisdiction, but schools have leeway regarding some aspects of implementation. It is important to revisit the policies and procedures for crisis training to make sure they are still effective.

Organizations in the United States spend a total of \$135 billion on training individuals each year (Salas et al., 2012). Training can help reduce errors in high-risk situations. Decisions on what to train, how to train, and how to evaluate the training are important when implementing training (Salas et al., 2012). It is important to invest in training because it allows individuals to learn information related to their jobs and keeps them safe. Being prepared for the training and preparing individuals before the training is important. Motivation and promotion of the training can assist in learning of the training. After the training is over, it is key to evaluate how the training went and make changes to correct any problems.

There are multiple approaches to training; two common approaches are asynchronous and synchronous training. Asynchronous training sessions are administered individually, while all participants are present for synchronous training at the same time (Craig, 2016). Asynchronous online courses provide a flexible and self-paced learning environment for individuals. In synchronous online courses, the instructor of the course and the learners participate simultaneously (Skylar, 2009). A synchronous online course is more similar to traditional learning than an asynchronous online course. A study conducted using the Likert scale to test whether students learned more through synchronous or asynchronous online learning showed no significant difference in learning (Skylar, 2009). These two training approaches are important to understand and test to improve the training's specific outcome. Improved understanding of situational training will also improve the training effectiveness and therefore positively affect the trainees and their knowledge. Knowledge transfer is the application of acquired skills and knowledge to different situations. Knowledge transfer is used to establish whether online training (synchronous or asynchronous) would be more effective than traditional, face-to-face training. The results from Craig's research determined that, in the short term, face-to-face training is more effective in a behavioral modeling approach than asynchronous or synchronous online training (Craig, 2016).

However, switching from traditional learning to asynchronous online learning can be difficult for students. As seen during the COVID-19 pandemic, many children switched to asynchronous online learning. A study by

Kaffenberge simulated that when students are out of school for longer than three months, their learning can fall behind up to a year (2020). Asynchronous learning hindered students' ability to communicate in a natural way with their peers as in traditional learning. Traditional learning in a brick-and-mortar setting allows students to communicate in person and have structured class times (Glenn, 2018). Asynchronous online learning normally requires more time, more writing, and less direct contact with other students and with instructors. Asynchronous online learning can be overwhelming since it is accelerated, but incorporating traditional learning styles and methodologies into asynchronous online learning can help students adjust to the different learning styles. Nevertheless, joining the learning styles can be problematic. Student motivation and pace of the class are two common problems (Glenn, 2018). Students have a difficult time adjusting to the lack of structure, and a disorganized approach can overwhelm students and reduce motivation. By developing a communicative culture and addressing students' needs and concerns early, improvements can be made to asynchronous online learning (Glenn, 2018).

Though initial training is a necessity that can be conducted without affecting productivity, retraining within companies or educational facilities can be difficult to schedule and implement. Asynchronous online training is used to assist with the retraining process and avoid time constraints associated with traditional training. Retraining of senior employees builds on current training and expands skills. A study by McEdwards in 2014 tested whether asynchronous training can retrain senior officials and help them learn new skills. The study found that senior officials can continue to improve their skills. Additionally, asynchronous training can be retained longer than traditional training as asynchronous training allows for individuals to seek repeated assistance if needed (McEdwards, 2014).

One of the biggest problems in training is knowing how long information may be retained. Interpreting the success or failure of a training can be difficult because the instructor or leader cannot see everything happening in the training (Miller et al., 1997). Instructors and leaders need to see whether the training was completed, how the training was written, and whether the trainees will remember what to do in a crisis (Miller et al., 1997). Evaluating training can be difficult but is necessary for the completion of the training. One of the most effective tools for helping people remember the training are picture or word reminders (Miller et al., 1997). Pictures or word reminders of crisis training are commonly posted at facilities to increase retention of the training.

Some studies refer to just-in-time training as just-in-time teaching. For the purposes of this study the

researchers will use the term just-in-time training. Besides traditional and online training, just-in-time training (JITT) offers another approach to learning that can determine how long trainees retain information and skills (Craig, 2016). JITT is becoming an important tool for performance improvement in the global changing workforce (Vico et al. 2007). JITT is being tested on health training to give first responders a quick refresher on immediate tasks that need to be performed. JITT can be done through smartphones, lasts no more than five minutes, and can be translated into several languages (Vico et al., 2007). JITT allows health training to be mobile and delivered when needed, eliminating waiting on the next instructor-led training.

Just-in-time training has been incorporated into higher education schools as well. It was first implemented in an introductory physics course to address nontraditional students' needs (Abreu & Knouse, 2014). JITT has also been used in advanced foreign language classes. Professors noticed that certain key concepts in courses were being forgotten, and JITT allows students to go back and refresh their memory later in the course, creating more opportunities for student learning (Abreu & Knouse, 2014).

Additionally, JITT is being used to train nonmedical hospital staff on workforce requirements (Spitzer et al., 2007). JITT was tested with only a small number of individuals at hospitals with two point-of-dispensing (POD) exercises. One POD exercise was designed to test the duration of the exercise individuals participated in, and the other POD exercise was used to approximate the waiting time at the station (Spitzer et al., 2007). The results showed that JITT can be used by individuals in high-throughput environments. Thus, JITT can be used in schools to save time on training, since one can complete the training with a high throughput of individuals on the system.

Another viable option for training is computer training, instead of school instructors physically assisting in training for crisis response. Computer training may include watching a training video whenever possible. The computers allow for flexible crisis training, instead of planned personnel-led training (Harrington & Walker, 2003). A review of studies comparing computer-based training and instructor-led training shows that trainees prefer computer-based training, but there was no significant difference between the two training sessions regarding posttraining information retention (Harrington & Walker, 2003). Thus, schools should consider this as an alternative to the costs associated with traditional active shooter training. Additionally, such training could be overseen and approved by local law enforcement, keeping up best practices associated with traditional active shooter training.

The mentioned studies discuss school crisis training and its effectiveness. Some methods for training are asynchronous, synchronous, in-person, and just-in-time training/teaching. However, there is limited research on crisis training retention among classroom leaders and how often training should be conducted to maintain satisfactory retention.

## **METHODS**

This research tests how long crisis training information is retained before it goes below an acceptable level. The research also addresses how JITT could benefit individuals when training sections are not retained. The study will take place over four months with crisis leaders as the participants. Crisis leaders are individuals in charge of crisis prevention and preparedness or who participate in a significant way. Crisis leaders include administrators, teachers, school aides, people in the workforce, and student teachers in the process of becoming teachers. This study will assume that everyone has had prior training, but watching an RHF video will be required to ensure each participant is trained with the same material, so testing can accurately test the length of crisis training retention over time.

Crisis leaders were drawn from the state of Indiana and includes individuals in college, in the workforce, and employed by K-12 schools.

## **PARTICIPANTS**

Convenience sampling will be used in the study. Convenience sampling was chosen because the volunteers were accessible based on the purpose of the study. To connect with the volunteers, the researcher will send out an email. The email list will be taken from the department of education database and from crisis leaders in the area.

The sample size will be 20 crisis leaders, based on the number of crisis leaders (college students from Purdue University because of access, workforce, and K-12 teachers) that volunteer for this survey.

The population of this study will be a group of crisis leaders in Indiana. There will be no stratification of the population because the characteristics of the population do not matter for the purpose of this study. For the purpose of the study, all classroom leaders are considered equal.

## **MATERIALS**

The researcher will develop a Qualtrics survey based on the just-in-time crisis video that participants are required to watch at the beginning of the study

## **Procedure**

Individuals were invited to participate in the study in the form of a survey. This study will explore the retention rate based on time for just-in-time crisis training. The study hopes to show when retention from training declines, therefore predicting when training is needed again.

Retention results were collected for individuals who are currently in classroom crisis leadership opportunities. The unit of measure is the amount of information retained based on time. Every month, the volunteers will be given the same survey to see whether retention has declined.

The observed variables are related to the JITT video that all the volunteers will watch at the beginning of the study. The independent variable will be time, and the dependent variable will be the amount of information retained.

The volunteers must watch the active shooter training video before the first survey in order to get a baseline for the training. The survey is created based on current active shooter procedures and will be revised by subject matter experts.

The data was collected through an online survey. The survey will be given every month. The crisis leaders will start in July 2019 and finish in October 2019. The survey will be completed once a month. The researcher will notify participants by email about where they can watch the RHF crisis training video and provide a hyperlink to the Qualtrics survey. The online survey will allow for faster response times and allow volunteers to complete the survey on their own time. The researcher will also send reminder emails to the volunteers to complete the survey each month. The anonymity of the responses will be protected.

## **RESULTS**

The JITT data gathered, shown below, indicates a different demographic of the results and different ways the data can be interpreted. Once the data was collected, cleaned, and analyzed, it was used to produce four graphs. Figure 1 shows the difference between score by time for gender, Figure 2 shows the difference between score by time for employment, Figure 3 shows the difference between score by time for training, and Figure 4 shows the overall difference between score by time.

Figure 1 shows that there is no statistically significant difference for retention between females and males. In time 0 (Training), there were eleven male and seven female participants. In time 1, there were ten male and five female participants. In time 2, there were nine male and five female participants. In time 3, there were six male and three females.

There are a few outliers in months 1 and 2 for females that could be pulling the average score down, but

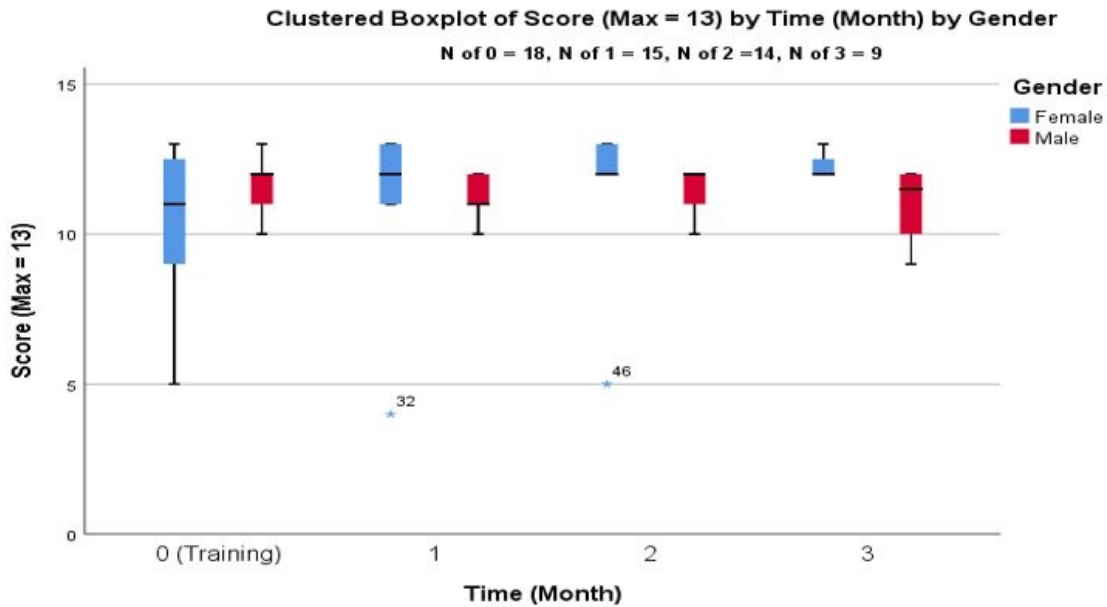


Figure 1. Overall Retention Scores by Gender

Table 1. Statistical Summary of Overall Retention Scores by Gender

Estimates of Fixed Effects <sup>a</sup>							
Parameter	Estimate	Std. Error	df	t	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Intercept	11.157471	.482070	20.782	23.145	.000	10.154309	12.160632
[Employment=College Student (Over 18)]	-.244478	.577947	53.715	-.423	.674	-1.403333	.914376
[Employment=Workforce]	0 <sup>b</sup>	0	.	.	.	.	.

a. Dependent Variable: Score (Max = 13).

b. This parameter is set to zero because it is redundant.

overall, the scores based on time for gender are close to a straight line. Table 1 shows that there is no significant difference based on gender because the confidence interval contains zero between the upper and lower bounds.

Figure 2 shows no statistically significant difference for retention loss based on employment. There were five outliers for participants in the workforce. When the outliers are taken out, the scores based on time for employment are close to a straight line. Table 2 shows that there are no significant differences based on employment because the upper and lower bounds contain zero.

Figure 3 shows no statistically significant difference for retention loss based on previous training. There are three outliers with no previous training and one outlier with previous training, and they pulled the averages down. Overall, the scores over time for training are close to a straight line and show no real reduction in retention.

Table 3 shows that there is no significant difference between the previous training or no previous training because between the lower bounds and upper bounds contains zero.

Figure 4 shows the score by time not based on any demographics. There are four outliers, one in each month. There are little differences between each month, but between where the average started and where it ended up, there is no real difference between the four months. Overall, there is no statistically significant difference for retention, but more of a straight line. Table 4 shows how close the means are over the course of four months.

Figure 5 shows the score by time based on the nine individuals who participated in every survey. There is one outlier in month 3. This outlier brought the mean down in month 3. The means of each month are as follows:

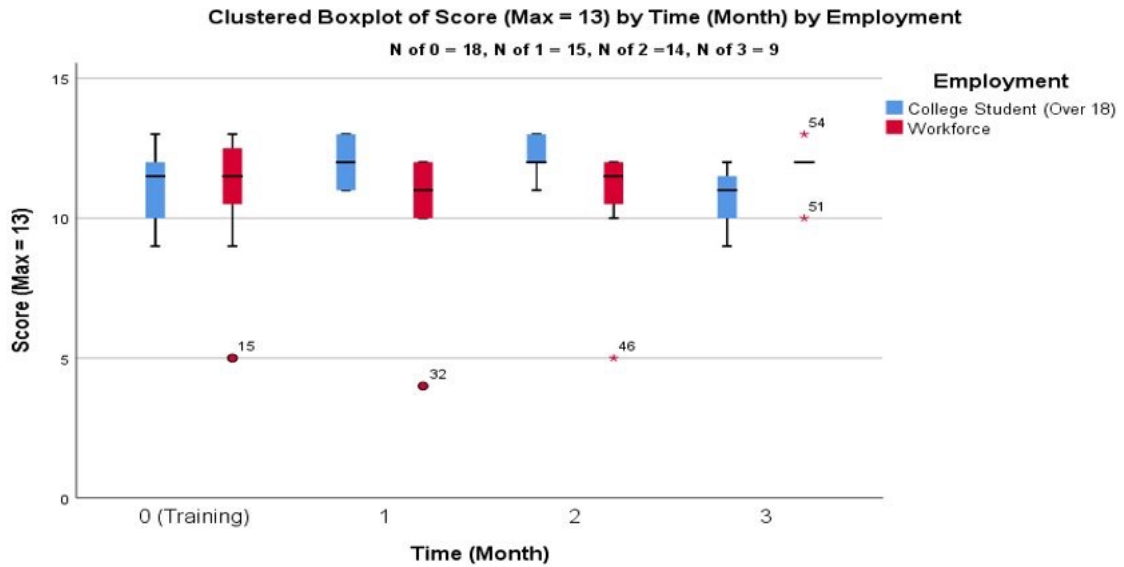


Figure 2. Overall Retention Scores by Employment

Table 2. Statistical Summary of Overall Retention Scores by Employment

Estimates of Fixed Effects <sup>a</sup>							
Parameter	Estimate	Std. Error	df	t	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Intercept	11.157471	.482070	20.782	23.145	.000	10.154309	12.160632
[Employment=College Student (Over 18)]	-.244478	.577947	53.715	-.423	.674	-1.403333	.914376
[Employment=Workforce]	0 <sup>b</sup>	0	.	.	.	.	.

a. Dependent Variable: Score (Max = 13).

b. This parameter is set to zero because it is redundant.

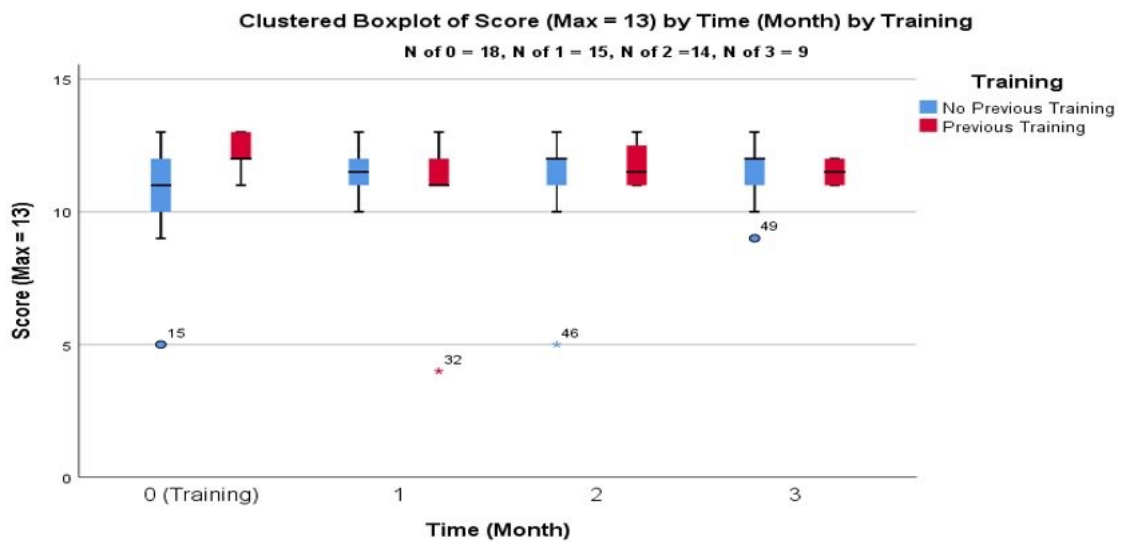


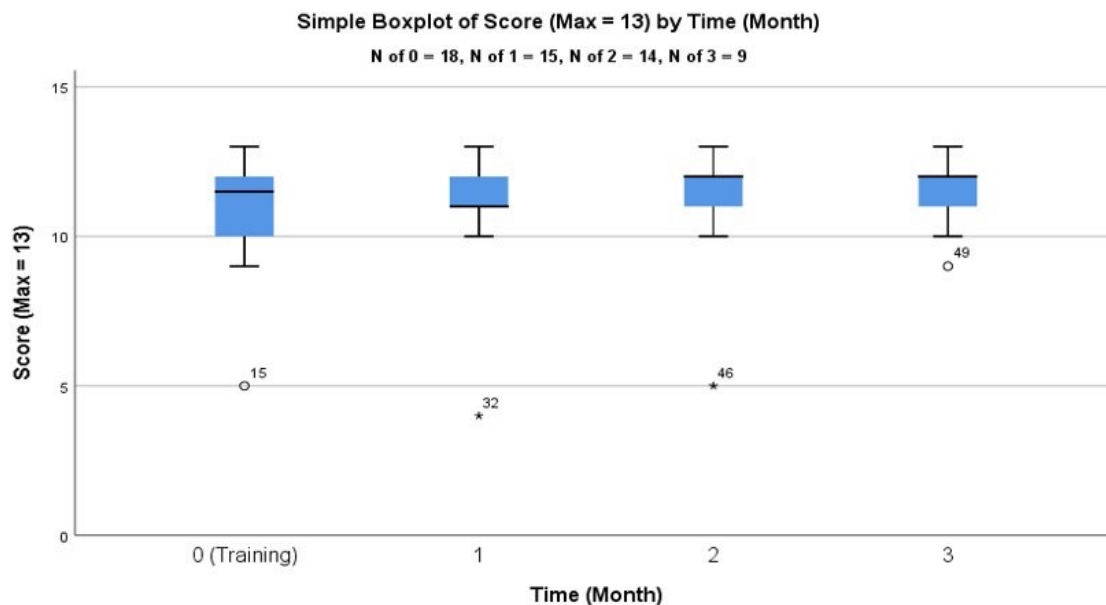
Figure 3. Overall Retention Scores by Previous Training

**Table 3.** Statistical Summary of Overall Retention Scores by Previous Training

Estimates of Fixed Effects <sup>a</sup>							
Parameter	Estimate	Std. Error	df	t	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Intercept	11.904188	.683477	32.965	17.417	.000	10.513588	13.294788
[Training=No Previous Training]	-1.099412	.711890	47.095	-1.544	.129	-2.531473	.332650
[Training=Previous Training]	0 <sup>b</sup>	0	.	.	.	.	.

a. Dependent Variable: Score (Max = 13).

b. This parameter is set to zero because it is redundant.



**Figure 4.** Overall Retention Scores without Demographics

month 0 (Training) = 11.44, month 1 = 11.22, month 2 = 11.67, and month 3 = 11.44; the average is 11.44. Based on these means, interpretation can be made that the mean scores do not change from month 0 (Training) to month 3. Overall, there is no statistically significant difference for retention because the average of the means is 11.44, which is the same as month 0 (Training).

Table 4 shows the average from one month to the next. The averages could change based on the number

**Table 4.** Brief Statistical Summary of Overall Retention Scores without Demographics

Time (Month)	Mean	N	Std. Deviation
0 (Training)	11.06	18	1.984
1	11.00	15	2.138
2	11.29	14	1.978
3	11.44	9	1.236
Total	11.16	56	1.886

**Table 5.** Percentage of Questions Answered Correctly

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13
Month 0 (N=18)	83%	89%	89%	100%	78%	78%	100%	94%	94%	89%	39%	78%	94%
Month 1 (N=15)	80%	87%	87%	100%	93%	73%	100%	100%	80%	93%	33%	80%	93%
Month 2 (N=14)	86%	93%	79%	100%	93%	79%	93%	93%	86%	93%	36%	93%	100%
Month 3 (N=9)	89%	89%	100%	100%	89%	78%	100%	89%	100%	100%	33%	78%	100%

of participants dropping each month. Since all the standard deviations are low, this means all scores are close to the mean and not spread out.

Table 5 shows the percentage of questions answered correctly for each month. The goal is to show the questions the participants struggled on. Highlighted in red is any question that is lower than 75%. Table 5 shows that the participants struggled on question 11. The participants also got below 75% on question 6 during the second time taking the survey. Further analysis will be discussed in another part of this paper.

## DISCUSSION

Figures 1, 2, and 3 show the demographics and how they affect retention. Figure 1 shows how gender affects the scores over time. Figure 2 shows how employment affects score over time. Figure 3 shows how previous training affects score over time. All these outcomes show that the retention level is flat, and a curve of drop-off based on the demographics is not shown. Figure 4 shows the score based on time, not on demographics. Overall, Figure 5 had a high retention rate, and there was no drop-off in retention based on time. The average mean score goes from 11.06 in month 0, then after training to 11.44 in month 3, which is the fourth time the participants took the survey. This increase was not predicted. This research shows that three months training, there is no retention loss. This research also shows that JITT can be used to assist with traditional active shooter training because there was no retention loss after JITT. The researcher recommend that the retention rate stay above 70% based on the results of the survey. That 70% comes from the standard way we look at a passing grade. Once the retention rate goes below 70%, JITT can be used to refresh and raise the retention to the 70% level. Based on the results of the data, we still recommend doing an active shooter training every semester as stated in Indiana Department of Education standards. The research team believes that training for an active shooter situation once per semester would be sufficient to keep the retention rate high.

Throughout, this research shows the possibility of using JITT to assist with active shooter training. Since there was no retention loss during the research, the study may need to be continued for a longer time period to see when the retention curve starts to fall.

Some reasons why the retention rate stayed high are that some questions were viewed as common knowledge, there were recent active shootings, participants learned from the news about what to do when shootings occur, and the research period was not long enough to see a retention curve.

All the outliers in Figure 1 and in Figures 2, 3, and 4 just in time [0 (Training), 1, and 2] were the same participant. These low scores could be due to the participants not taking the survey seriously and just guessing on the questions instead of thinking about the correct answer. Also, a participant may not have watched the training video and just took the survey. This is an issue with online surveys where participants cannot be monitored. Another problem was that the researcher sent the survey and training video to a group of teachers identified from the Indiana teachers' association website and none of them participated in the study.

Table 5 shows the percentage of questions answered correctly for each month. Based on the analysis, question 11 participants could not figure out the correct answer consistently over the course of the research.

Evaluating retention of knowledge on active shooter situations is important. There have been many active shooter situations, and is necessary to learn from what happened in previous active shooter cases. Since more active shootings are occurring, there are more case studies to learn from. Learning from previous active shooter cases where crisis plans and active shooter preparedness are flawed can help save lives and potentially protect against an active shooter situation.

When examining the findings of our research, we saw additional room for improvement for later works. Expanding the number of questions and sample size, refining the current survey questions, and expanding the time frame of the study would be beneficial in validating the retention curve we saw in our work.

While the RHF model used in this research was applicable for a general population, it leaves room for improvement as each school could create its own RHF video. Instead of the video being general, it could be specific to the school to make the training more effective.

Since the research population was small, it does not reflect the population size of schools or big venues where active shooter situations normally occur. Schools generally have big populations; a lower retention rate might be sufficient since many students may retain proper response knowledge and could act as crisis leaders. With students becoming crisis leaders in active shooter situations, administrators and teachers can feel more prepared in an active shooter situation.

Additional research can be created based on the results of this research shown in Figure 1. This figure shows that the female average for retention is higher than the male average.

## REFERENCES

- Abreu, L., & Knouse, S. (2014). Just-in-time teaching: A tool for enhancing student engagement in advanced foreign language learning. *Journal of Effective Teaching, 4*, 49–68. [https://uncw.edu/jet/articles/Vol14\\_2/Abreu.pdf](https://uncw.edu/jet/articles/Vol14_2/Abreu.pdf)
- Anklam, C., Kirby, A., Sharevski, F., & Dietz, J. E. (2015). Mitigating active shooter impact: Analysis for policy options based on agent/computer-based modeling. *Journal of Emergency Management, 13*(3), 201–216. <https://doi.org/10.5055/jem.2015.0234>
- Buerger, M. E., & Buerger, G. E. (2010). Those terrible first few minutes: Revisiting active-shooter protocols for schools. *FBI Law Enforcement Bulletin, 79*. <https://heinonline.org/HOL/Page?handle=hein.journals/fbilib79&id=292&div=92&collecti on=journals>
- Craig, C. R. (2016). *Examining the difference between asynchronous and synchronous training*. <https://search.proquest.com/docview/1851001439/fulltextPDF/AE7DF5392B2D4AFAPQ/1?accountid=13360>
- Destein, J. (2016). *Active shooter*. ASIS School Safety & Security Council. [https://www.asisonline.org/globalassets/news/security-topics/soft-target--active-shooter/active\\_shooter\\_wp\\_sssc.pdf](https://www.asisonline.org/globalassets/news/security-topics/soft-target--active-shooter/active_shooter_wp_sssc.pdf)
- Glenn, C. W. (2018). Adding the human touch to asynchronous online learning. *Journal of College Student Retention: Research, Theory & Practice, 19*(4), 381–393. <https://doi.org/10.1177/1521025116634104>
- Gurdineer, E. E. (2013). *The impact of demographics, resources, and training on the quality of school crisis plans* (Publication No. 3565074) [PsyD dissertation, SUNY Albany]. <https://www.proquest.com/openview/123ff656ab834015ce91b83466eafb91/1?pq-origsite=gscholar&cbl=18750>
- Harrington, S., & Walker, B. (2003). Is computer-based instruction an effective way to prevent fire safety training to long-term care staff? *Journal for Nurses in Staff Development, 19*(3), 147–154. <https://oce.ovid.com/article/00124645-200305000-00007/HTML>
- Houston Emergency Management. (2002). *Active shooter*. Retrieved October 16, 2019, from <http://houstontx.gov/oem/pages/preparedness/hazards/active-shooter.html>
- Lee Brown, L. (2008). *The role of teachers in school safety* [PhD dissertation, University of Southern Mississippi]. <https://aquila.usm.edu/dissertations/1200>
- Lee, J. Y. (2019). *Agent-based modeling to assess the effectiveness of RUN HIDE FIGHT* [Master's thesis, Purdue University]. [https://www.researchgate.net/publication/333292303\\_AGENT-BASED\\_MODELING\\_TO\\_ASSE](https://www.researchgate.net/publication/333292303_AGENT-BASED_MODELING_TO_ASSE)
- Malloy, D. P. (2015). *Final report of the Sandy Hook advisory commission*. [http://www.shac.ct.gov/SHAC\\_Final\\_Report\\_3-6-2015.pdf](http://www.shac.ct.gov/SHAC_Final_Report_3-6-2015.pdf)
- McCormick, D. J. (2018). *2018 Indiana school safety recommendations*. <https://www.in.gov/dhs/files/2018-Indiana-School-Safety-Recommendations.pdf>
- McEdwards, C. (2014). The efficacy of deliberate practice delivered using asynchronous training. *International Journal of Advanced Corporate Learning, 7*(1), 43–46. <http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=6&sid=da6a7df4-3d7e-42cd-aff5-0e3a46121540%40sessionmgr102>
- Miller, P., Coyle, T., & Slawinski, J. (1997). Instructing children to use memory strategies: Evidence of utilization deficiencies in memory training studies. *Developmental Review, 17*(4), 411–441. <https://doi.org/10.1006/drev.1997.0440>
- Nichols, T. (2010). *Critical issues in active shooter response and training*. *Sheriff, 62*(1), 31–32.
- Rorie, S. (2015). Implementing an active shooter training program. *AORN Journal, 101*(1), C5– C6. [https://doi.org/10.1016/S0001-2092\(14\)01325-8](https://doi.org/10.1016/S0001-2092(14)01325-8)
- Ryals, C. C. (2014). *School leaders' perceptions of conducting active shooter drills* (Publication No. 3646191) [EdD dissertation]. <https://www.proquest.com/openview/89a5669f8e8745b0e078d2befdc04a/1.pdf?pq-origsite=gscholar&cbl=18750>
- Salas, E., Tannenbaum, S. I., Kraiger, K., & Smith-Jentsch, K. A. (2012). The science of training and development in organizations. *Psychological Science in the Public Interest, 13*(2), 74–101. <https://doi.org/10.1177/1529100612436661>
- Shah, N. (2013). States stepping up mandates for school safety drills. *Education Week, 32*(32), 1.
- Skylar, A. A. (2009). A comparison of asynchronous online text-based lectures and synchronous interactive web conferencing lectures. *Issues in Teacher Education, 18*(2), 69–82. <https://files.eric.ed.gov/fulltext/EJ858506.pdf>
- Spitzer, J. D., Hupert, N., Duckart, J., & Xiong, W. (2007). Operational evaluation of high-throughput community-based mass prophylaxis using just-in-time training. *Public Health Reports, 122*(5), 584–591. <https://doi.org/10.1177/003335490712200505>
- Texas State University. (2004). *ADD. Avoid | Deny | Defend*. Retrieved October 16, 2019, from <http://www.avoiddenydefend.org/add.html>



- Tschannen-Moran, M. (2009). Fostering teacher professionalism in schools. *Educational Administration Quarterly*, 45(2), 217–247. <https://doi.org/10.1177/0013161X08330501>
- Vico, F. J., Canteli, V., Lobo, D., Fernández, J. D., Bandera, C., García-Linares, A., Rivas, R., Rosen, M., & Schlegel, B. (2007). *Mobile just-in-time training application for emergency healthcare services*. <https://riuma.uma.es/xmlui/bitstream/handle/10630/6728/iadis2007preprint.pdf?sequence=6>
- Weill Cornell Medicine. (2018). *How long does a fire drill normally last?* <https://ehs.weill.cornell.edu/faq/how-long-does-fire-drill-normally-last>
- White, J. (2018). *Shelter-in-place vs. lockdowns*. <https://www.rcoe.us/administration-business-services/operational-support-services/emergency-preparedness/parent-emergency-information/shelter-in-place-vs-lockdowns/>
- Williams, J. (2015). *Active shooter safety considerations for educators*. <https://doorbearacade.com/wp-content/uploads/2015/10/ActiveShooterSafetyConsiderationsForEducators.pdf>
- Wisconsin Association of School Boards. (2016). *Antigo prom shooting* [PowerPoint slides]. Retrieved from <https://wasb.org/wp-content/uploads/2018/01/CrisisCommunication-CaseStudy.pdf>
- Worsham, W. (2017). *Know the difference: Shelter in place and lockdown 2 very different emergency responses*. United States Army. [https://www.army.mil/article/184872/know\\_the\\_difference\\_shelter\\_in\\_place\\_and\\_lockdown\\_2\\_very\\_different\\_emergency\\_responses](https://www.army.mil/article/184872/know_the_difference_shelter_in_place_and_lockdown_2_very_different_emergency_responses)

## Appendix A: Survey Questions

1. What is the best and most common strategy to use during an active shooter event?
  - a) Avoid/Deny/Defend
  - b) RUN. HIDE. FIGHT.
  - c) Awareness, Preparation, Activate
  - d) Call 911
  - e) All of the above
2. Individuals should always try and escape and evacuate even when others insist on staying.
  - a) True
  - b) False
3. Individuals should let others slow them down when trying to escape
  - a) True
  - b) False
4. Should you grab your belongings before you run?
  - a) Yes
  - b) No
5. Individuals should not help other individuals avoid the area where the active shooter is.
  - a) True
  - b) False
6. Of the six objectives to do during the RUN part, what is the last thing you should do?
  - a) Leave your belongings behind
  - b) Help others escape if possible
  - c) Call 911 when you are safe
  - d) If there is an escape path, attempt to evacuate
7. When individuals are hiding, should they barricade and lock the door?
  - a) Yes
  - b) No
8. It is important to not turn off the lights and to not silence your cell phone because it will let the shooter know something is not right with that room and someone maybe in there.
  - a) True
  - b) False

9. When hiding, individuals should not trap or restrict your options for movement.
  - a) True
  - b) False
10. When fighting individuals should act with aggression using improvised weapons to disarm the active shooter.
  - a) True
  - b) False
11. Of the four objectives for the fighting part, what is the last thing you should do?
  - a) Act with physical aggression
  - b) Commit to your actions
  - c) Improvise weapons
  - d) Attempt to incapacitate the shooter
12. The first responders that are first on the scene are not there to evacuate or take care of the injured, but are there to take down the active shooter.
  - a) True
  - b) False
13. What is true when the law enforcement arrives?
  - a) Remain calm and follow instructions
  - b) Keep your hands visible at all times
  - c) Avoid pointing or yelling
  - d) Know that help for the injured is on its way
  - e) All of the above

#### Answers

- 1.) B
- 2.) A
- 3.) B
- 4.) B
- 5.) B
- 6.) C
- 7.) A
- 8.) B
- 9.) A
- 10.) A
- 11.) B
- 12.) A
- 13.) E

## Active Shooter Prevention Methods in Schools

Katherine Reichart, Madison Thomas, and J. Eric Dietz, PhD, PE

**Abstract** This research investigates how to measure school active shooter safety against current policies in place regarding two different areas of school climate. Using the state of Indiana as a case study, 55 schools from 38 counties, various socioeconomic environments, and school types (public, private, etc.) were surveyed. Research was conducted through a survey of approximately 40 questions posed to the school principal. The data collected shows how demographics, policies, and procedures affect school active shooter prevention. Analysis showed that school size may relate to lower social-emotional security scores. Additionally, middle schools appear to score higher on social-emotional security than K-12 schools. Nonpublic schools also appear to score lower on active shooter prevention than public schools, with there being a moderate effect between the two. This should be considered by schools and policymakers across the country when developing active shooter safety plans.

### INTRODUCTION

Active shooter incidents (ASIs) refer to planned or unplanned attacks in which the primary weapon of attack is a firearm of any type. ASIs can range from homicide (killing another person) to mass murder (killing four or more people during an event with no cooling-off period) (Federal Bureau of Investigation, 2018). Additionally, suicide can be considered an active shooter incident, if done with a firearm. ASIs are recognized as a global public health concern. In an editorial by Rivara et al., the authors discuss and analyze firearm-related deaths from 195 countries and territories in 2016 (2018). A directed ASI in a school is known as a school shooting. School shootings must occur on school grounds but can involve staff, faculty, or students. In a Federal Bureau of Investigation report comparing active shooter events between 2000 and 2019, pre-K through 12th grade schools were the third most common location for ASIs (Federal Bureau of Investigation, 2021). This paper focuses on school shooting incidents, how to prevent these incidents, and current incident responses. Active shooter prevention is defined as “the action schools and school districts take to prevent a threatened or actual incident from occurring” (US Department of Education, n.d.).

Schools are continually a target for both insider and outsider threats because they are large places of social gathering. Schools have been particularly susceptible to this type of attack despite continuing to adopt firearm policies. For example, the 2018 Parkland High School shooting and the 2021 Oxford High School shooting both occurred on school grounds despite policies against firearms (Maher, 2018; Shapiro et al., 2021). By exploring active shooter school safety prevention against existing policies, schools can determine which type of measurements are

more effective than others. Current policies regarding ASIs lack detailed measurements about school preparedness because the previous focus has been on response as opposed to prevention. However, preventing ASIs results in saved lives and mitigated risk.

The first recorded school shooting happened at the University of Virginia in 1840 between a professor and a student and is cited as the instigating factor in the creation of the school’s honor code (“John Anthony Gardner Davis,” 2016). Since then, school shooting incidents have been recorded and recounted to others (Rosenwald, 2018). School shooting incidents have varied in structure, size, number of students, and educational level (primary, secondary, higher education), and demographics such as average socioeconomic status, number of students on free and reduced lunch, and others have varied from school to school. The one connecting principal is that most are gun-free zones (Toppo, 2018). Despite this, the Centers for Disease Control and Prevention (CDC) conducted a study that determined 135,000 guns were brought to various schools (Toppo, 2018). According to the CDC (2018), findings from this same study shows an overall drop in school-associated death between 1992 and 2015 despite the large number of guns brought into these areas. Risk potential related to homicide in children has not decreased as homicide is the second leading cause of death among those age five to eighteen (Centers for Disease Control and Prevention, 2018).

While the American Medical Association notes that mass shootings as a type of gun violence are a smaller fraction of firearm-related deaths on a global scale, it is one of the most visible (Rivara et al., 2018). One of the most widely discussed school shootings is the Columbine High School shooting. Two Columbine students with knowledge of school procedures sought to cause

chaos, destruction, and death using assault as their primary weapon. Per a US Fire Administration (USFA) after-action report (AAR), “The wanton violence associated with terrorist-style assaults is intended to inflict both physical and psychological injury, often indiscriminately” (US Department of Homeland Security, 1999, pp. 3). In this AAR, the USFA detailed the incident resulting in 15 fatal casualties, 14 of them in high school (including shooters), and 22 nonfatal casualties. The school had a daily population of approximately 2,000 people. Additionally, the active Columbine High School emergency procedure plans during the ASI are included in the AAR but did not include ASIs (US Department of Homeland Security, 1999). If emergency procedure plans related to ASIs were included, potentially lives could have been saved and the ASI length of 30 minutes decreased.

Despite this event, mass active shooter school incidents are still prevalent today. During a recent example, in 2018, there were 17 fatal casualties and 17 nonfatal casualties at Parkland High School. Official sources published an AAR detailing the school’s response to the incident, including real-time data and audio and video of the event (Hobbs et al., 2018). The perpetrator acted alone, was a former student, and planned his attack prior to committing it. As recounted in McMahon (2018), limitations to school security, policy, and procedure contributed to both successes and failures in this incident.

In contrast to student active shooters, the perpetrator of the 2012 Sandy Hook Elementary School shooting did not attend or work at the elementary school. The assailant was not an insider threat but did have ties to the institution through his mother. In this event, a single perpetrator with a semiautomatic weapon and two pistols fatally shot 28 people with many of the casualties students who were seven or eight years old. Comparing Columbine and Sandy Hook implies that active shooters are both insider and outsider threats or have some type of relationship with their victims (O’Neill et al., 2016). Examining both insider and outsider threats to a school could decrease the potential for an active shooter event. As shown in Figure 1, the next step in the NYPD recommendations is to institute procedures that align with those policies related to both types of threats (Active shooter, 2016). Also focusing on physical and social emotional security could prevent future ASIs. These two measurements encompass the idea of school climate.

School climate refers to the environment of a school. Readiness and Emergency Management for Schools defines school climate as a range of campus conditions (Indiana Department of Homeland Security, 2019), which may include the quality and character of school life (National School Climate Center, 2022). School climate may be broken down into six categories with thirteen dimensions. The six categories of school climate are safety,



Figure 1. NYPD recommendations following active shooter programs (“Active shooter,” 2016)

teaching and learning, interpersonal relationships, institutional environment, social media, and leadership and professional relationships.

Physical security, an aspect of school climate, is an imperative way to prevent outsider threat ASIs. Commonly cited physical security measurements in schools include room layout, locks, and resource officers. As recounted in a study by McMahon (2018), limitations to school physical security policy and procedure contributed to both successes and failures in the 2018 Parkland shooting. The Parkland shooter successfully completed their plan through unsafe classroom and door design (McMahon, 2018). As defined in the Marjory Stoneman Douglas High School AAR (2019), hard corners constitute an area that cannot be accessed or seen from a window as to remain safe. In the same report, the Marjory Stoneman Douglas Public Safety Commission (2019) noted that obstructed hard corners were rendered useless as there were no policies in place. Additionally, the classrooms were constructed of drywall and many areas were shot through, despite the shooter specifically aiming through the windows. This has led to the creation of policy and products meant to fortify and reinforce hard corners. Notably, the active shooter never entered classrooms, choosing instead to fire through windows inset in the doors. Due to smoke, fire evacuation procedures began, which contributed to additional victims (Hobbs et al., 2018). However, a policy requiring windows that are hurricane impact resistant prevented further casualties as the active shooter could not fire on evacuating students (McMahon, 2018). This success shows how building design contributes to the physical security of a school.

One way to encompass physical security into new school building design is crime prevention through environmental design (CPTED). CPTED relies on how physical building design features affect crime and behavior (Vagi et al., 2018). CPTED does not fully define what types of crime can be prevented in schools, nor does it give specific guidelines for schools to follow, which can be off-putting to architects of new school. Assessors can determine a school's CPTED rating, but this is not the most cost-effective measure. As CPTED is rooted in building design, evaluations and suggestions are customized per school. This approach may be useful for schools that can afford to or must remodel. However, it is not feasible to implement for most existing schools (Vagi et al., 2018).

An additional way to improve physical security on a smaller budget would be through surveillance cameras. Prospective costs related to surveillance cameras would include camera and installation costs, storage for footage to be uploaded, a backup storage option, and monitoring during school or activity hours. Surveillance cameras were in place before the Parkland shooting, but

it is unclear whether they were monitored closely (Hobbs et al., 2018).

School resource officers may improve physical security of a school. At the time of the Parkland school shooting, the campus had one school resource officer to patrol fourteen buildings (Marjory Stoneman Douglas Public Safety Commission, 2019). A solution to employ an additional school resource officer, install additional security cameras, or reduce auxiliary building utilization. As shown by Smith and Renfro (2016, p. 1), additional physical security measurements found in schools include visible signage, random guard patrols, adequate lighting of exterior parking and entrance areas, closed-circuit television (CCTV) cameras, substantial exterior door locks, simple access control systems (turnstiles, badges, etc.), and secure locking doors to key areas or passageways.

When preventing schools from insider active shooter threats, measuring the social-emotional security of a school, also referred to as a dimension of school climate, is important (National School Climate Center, 2017). School climate may include both subjective and measurable features, such as culture and discipline (Indiana Department of Education, 2018a). Per Figure 2, school climate appears to encompass all facets of a school, which include subjective measurements. School climate should include a scale to produce numerical, quantitative measurements. Measuring a school's climate prior to an ASI is difficult but essential as insider threats can be prevented by enhancing a school's social-emotional security through reporting the active shooter's threatening behavior to an appropriate authority. Reporting this behavior is critical, because if it is not done in a timely manner or taken seriously, it can lead to death, as seen in the Oxford High School shooting in November 2021. Ethan Crumbley, the assailant, was reported to school officials by teachers earlier on the same day as the shooting, because he had posted on social media the night before about troubling behavior in the classroom. Instead of asking Ethan to go home for the day, he was allowed back in the classroom, and the ASI happened a few hours later (2021). As mentioned in an FBI report studying preattack behaviors, Silver et al. (2018, p. 7) noted, "On average, each active shooter displayed 4 to 5 concerning behaviors over time that were observable to others around the shooter. The most frequently occurring concerning behaviors were related to the active shooter's mental health, problematic interpersonal interactions, and leakage of violent intent." To score a school environment in preventing ASIs, threat assessments represent a real option by producing a measurable social-emotional security report. Per the FBI's violence prevention guidelines, a threat assessment is a social-emotional security measurement where school officials use viable and reasonable ways to assess

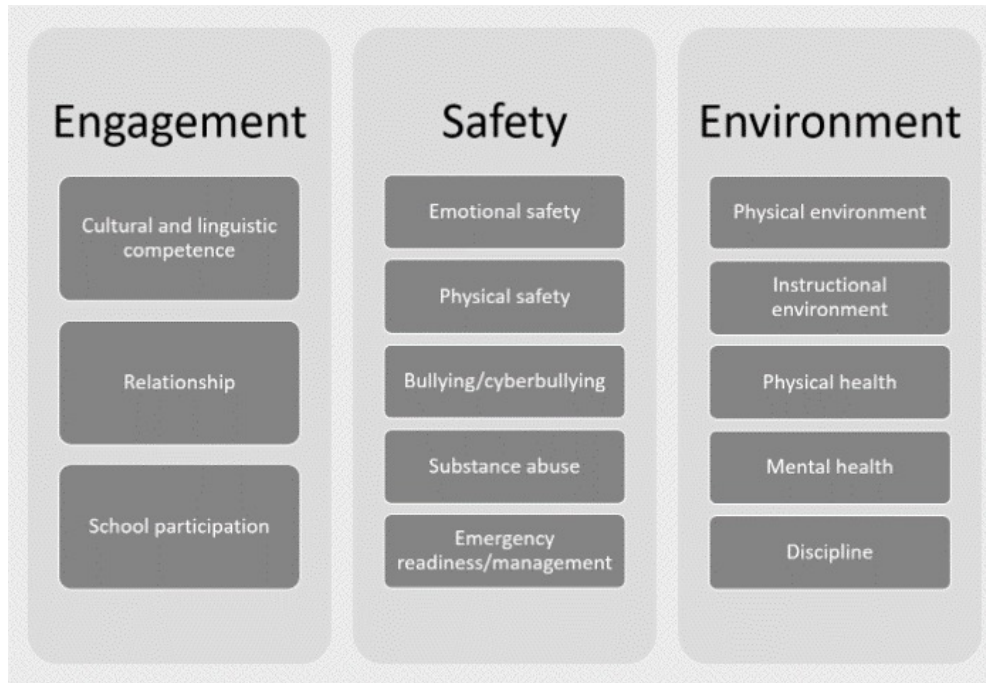


Figure 2. School climate model (National Center on Safe Supportive Learning Environments, 2018)

Who Noticed	Number	%
Schoolmate*	11	92
Spouse/domestic partner**	13	87
Teacher/school staff*	9	75
Family member	43	68
Friend	32	51
Co-worker	25	40
Other (e.g. neighbors)	23	37
Law enforcement	16	25
Online individual	6	10
Religious mentor	3	5

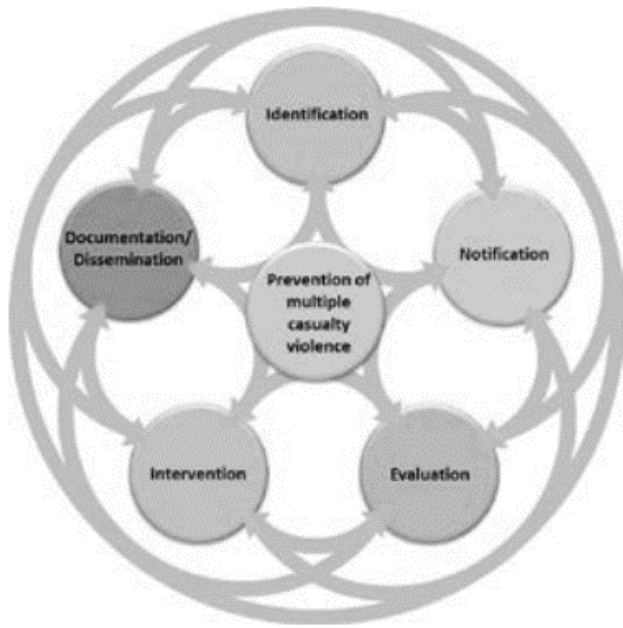
\* Percentage calculated only with those active shooters who were students at the time of the offense

\*\* Percentage calculated only with those active shooters who were in a relationship at the time of the offense

Figure 3. Measuring the preattack behavior of active shooters (Silver et al., 2018)

threatening student behavior. Student reporting guidelines are also available via the FBI's website on stopping bullying (Federal Bureau of Investigation, 2018). The validity of threat reporting and assessments are confirmed by Figure 3. Per a Department of Justice report (Paparazzo et al., 2013), a threat assessment can be composed of the processes outlined in Figure 4 and can prevent multiple-casualty violence, like ASIs. There are five points to this process: identification, notification, evaluation,

intervention, and documentation/dissemination. Threat assessments reveal concerning behaviors of potential insider threats and active shooter scenarios. Measuring concerning behavior is best done through safe and proper reporting. Policies unassociated with ASIs can be used to identify behavior patterns before an incident. In a National Threat Assessment Center report (2018), school policy to promote reporting may not be directly associated with ASIs but can influence whether behavior



**Figure 4.** Steps to preventing multiple casualty violence (Paparazzo et al., 2013)

is reported. Questioning current reporting policies at the individual school, school corporation, and state levels could show which procedures prevent ASIs the best.

School ASIs are often planned, with some sort of preparation associated with them (Federal Bureau of Investigation, 2017). Thus, intervention can occur before an incident by monitoring and measuring preattack behavior (Silver et al., 2018). A foiled school shooting is defined as “an incident that is stopped before the shooter reaches the intended target” (Silva & Greene-Colozzi, 2022). Foiled school shooting plots are mainly obstructed due to direct notification of law enforcement, occasionally through school intervention (“Active shooter,” 2016). A New York City Police Department report (“Active shooter,” 2016) details several foiled plots, many of which were resolved via reporting by family, peers, and authority figures. These foiled plots show that active shooter prevention can occur via reporting efforts of others. A Department of Justice report (Paparazzo et al., 2013) illustrates that prevention of mass school shootings has shifted from a stigmatized mental health intervention to anonymous reporting of threatening behaviors. Mental health is still a factor, but reporting concerning behaviors through threat assessments is a means to measure the social-emotional security of a school, depending on how they comply with threat assessments of students through both teachers and students.

Understanding the mental health of students, reporting concerning behaviors, and taking threat assessments

seriously are ways to potentially foil an active shooter plan. The Marjory Stoneman Douglas High School AAR thoroughly documents the prior behavior of the shooter and his social-emotional state. These sections reflect on how Marjory Stoneman Douglas High School reacted to concerning behaviors before the incident. The shooter admitted to his plan (leakage) several times publicly before committing the crime. This concerning behavior, among others, necessitated reporting and assessing the shooter, which could have resulted in a foiled plot as opposed to a successful one (Marjory Stoneman Douglas Public Safety Commission, 2019). Many students witnessed Cruz’s behavior and knew of his intentions. Coworkers, peers, and family members noticed extremely concerning behaviors, but the reports occurred after the incident. Reporting to authority figures (principals and possibly police officers) occurred, but procedure was not carried out. Notably, Marjory Stoneman Douglas High School had a three-part process to report concerning behaviors, which involved reconnaissance, training, and eventual threat assessment. However, the report on the shooter was dismissed. This school policy failure may have significantly contributed to the shooter’s intentions being carried out (Marjory Stoneman Douglas Public Safety Commission, 2019).

The researchers note that firearm violence affects school systems and policies, stating “armed guards patrol some schools, and some politicians have advocated allowing teachers to carry guns” (Marjory Stoneman Douglas Public Safety Commission, 2019, p. 1). However, additional policies that do not directly state active shooter policy are included in building plans. In the Safety Plan Audit Checklist provided by the Indiana Department of Education, the questions “Are threats of physical harm or violence investigated?” and “Are exterior doors locked, secured or monitored during the school day?” are related to active shooter prevention (Figure 4) (Indiana Department of Education, 2018b). However, the checklist does not refer to these questions as active shooter policy, instead referring lockdown or lockout procedures to “man-made occurrence drills” (Indiana Department of Education, 2018b). Additionally, lockdown/lockout drills are known as preventative measurements to outsider threats. As seen in a training study by Craig (2016), having more than one drill every two months has shown increased retention in process knowledge. Notably, ASIs may require different procedures than other manmade occurrences (Indiana Department of Education, 2018b).

Some previously mentioned topics are difficult to include in the proposed study as the measurements are not quantitative, nor easily scaled. However, per the Indiana Department of Education’s *Compass*, some of this data (bullying, emergency management, cultural and

linguistic competence) are measured per school year. These quantitative measurements are typically collected in July after the school year is completed as opposed to midway through the school year. Though schools may choose to audit themselves regarding this data at that time, the state corresponds to the end of the school year (Indiana Department of Education, 2018a).

However, the Indiana Department of Education regularly updates its resources regarding physical building security and includes school resource officers in its emergency preparedness plans but does not mandate them by law (Indiana Department of Education, 2018c). Furthermore, building design is not mandated in the audit checklist beyond exterior door procedures (Indiana Department of Education, 2018b). Dorn et al. (2014) address seven building design features that can increase safety in schools, including implementing school resource officers, surveillance technology (cameras, CCTV, etc.), and metal detecting technology (Indiana Department of Homeland Security, n.d.). Research suggests that these resources can prevent outsider active shooters in schools. Therefore, one can assume that schools are incurring both personnel and equipment costs.

The state of Indiana has a unique advantage of having a certification process on school safety called the Indiana School Safety Specialist Academy. This is a free certification program occurring over five basic training days and two advanced training days (Indiana Department of Education, 2018, October 22). The certification can be maintained through participating in advanced training annually. Thus, the cost for the program is not entirely financial, but it primarily requires time and participation. The Indiana Department of Education (2018, October 22) states that public schools have 100% program participation versus nonpublic schools. This makes sense as nonpublic schools do not require safety personnel or plans, which negatively impacts their participation in the certified Indiana School Safety Specialist Program (Indiana Department of Education, 2018, October 22). There are approximately 2,340 certified Indiana school safety specialists that may or may not be employed at a school or apply to multiple schools (Indiana Department of Education, 2018, October 22).

The state of Indiana has policies in place to measure levels of social-emotional security. Primarily, bullying and arrest data are required to be reported to the Indiana Department of Education and be publicly accessible to all as an Excel file online (Indiana Department of Education, n.d.). Additional resources include threat assessment teams and worksheets, cyberbullying information, and school climate survey guidelines (Indiana Department of Education, 2018c). The social-emotional security of a school has complex measuring criteria in concrete

terms other than reporting data (cyberbullying, threat assessments, and student surveys). Additionally, social-emotional security has shifting viewpoints as opinions of both faculty and students may differ despite operating in the same environment. Definitions also differ on whether social-emotional security is a tangible focus or a learning ideology. Both are used in active shooter prevention measurements; however, grant funding from the Indiana Secured Safety Grant prohibits grant money from being applied to social-emotional services. This shows a potential discrepancy in how grant funding is approached in Indiana, though priority legislation will attempt to rectify this in the future (Indiana Department of Education, 2018, October 22). Thus, costs do exist regarding social-emotional security in terms of personnel and training.

## **METHODOLOGY**

This research was done over two months using a survey of 37 questions comprising of both quantitative and qualitative data. The Indiana school system was chosen to act as the population for school active shooter prevention. Data was cleaned and anonymized to prevent misuse. Questions were posed to principals, recorded, then analyzed using the Statistical Package for the Social Sciences (SPSS) to determine standard statistically significant data. Incomplete data was removed before analysis. Data was checked to determine whether responses were unique, and schools did not answer twice. The survey was composed of a potential of 37 questions dependent on answers. These questions are given in Figure 5 (Reichert, 2019).

In this study, physical security measurements from the survey correspond to six of the seven building design features that may enhance school safety per the Indiana Department of Education recommendations. The seventh building design feature (promotion) relies on a subjective area of physical building design as it relates to emotional response. Even though the survey is experimental, the survey questions uniquely reflect the physical security measurements of schools in Indiana.

The study is meant to provide a basis on which to measure a school's social-emotional security procedures. According to publicly available school corporation data (2018–2019), 433 school corporations oversee 1,913 public schools and 362 nonpublic schools. Nonpublic schools (religious/private institutions, etc.) may be overseen by the same or separate entities classified under the same corporation ID. This data does not include homeschooled (an unaffected entity of school shootings as such could be construed as homicide). This data, made accessible by the Indiana Department of Education, equates to approximately 2,275 schools.



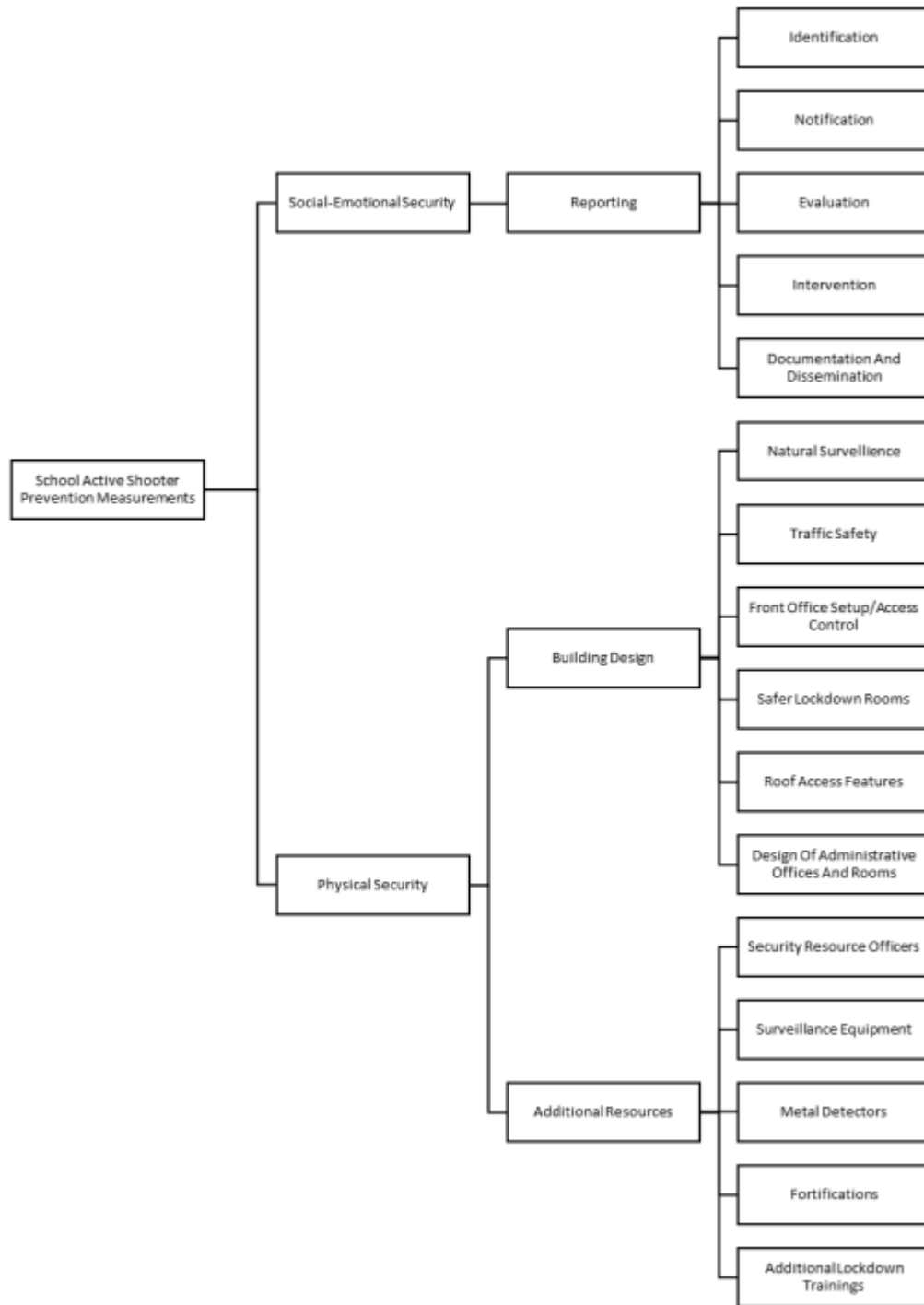


Figure 5. Survey structure (outcome variables)

Of the data collected, a sample was collected for approximately 55 schools. Thus, the study surveyed 47 public and 8 nonpublic schools, which is not in line with the attempted stratified survey. Indiana has 92 counties, and of the surveyed schools, 37 counties were represented,

and one school chose not to disclose. One school reported two counties. This school was counted as a separate entity as it could not be determined whether the school did not exist in two counties.

The hypotheses consisted of the following:

1. The researcher hypothesizes that public schools will score higher on active shooter prevention than nonpublic schools. The null hypothesis is that no scores are affected by school classification.
2. The researcher hypothesizes that schools with a mental health counselor or social workers will score higher in the social-emotional security area than those without. The null hypothesis is that no scores are affected by having these personnel or not.
3. The researcher hypothesizes that large schools will score higher in active shooter prevention than small and medium schools. The null hypothesis is that no scores are affected by population.
4. The null hypothesis is that no variables affect active shooter prevention.

The frameworks used for this study are current policies and procedures associated with active shooter prevention as discussed in the literature, mentioning how school active shooter prevention is a reactive process as opposed to a proactive process. This concept aligns with the diffusion of innovation theory in which innovation may slowly be adopted by a group or society (Dearing, 2009). The dissemination of this innovation may show gaps based on parameters like age, population, or socioeconomic area (Zhang et al. 2015). This theory aligns with how active shooter prevention can be adopted by schools, despite proactive measures becoming more common. As stated by Kaminski (2011), the diffusion of innovation reveals how modifications occur to improve adoption of an idea. This theory corresponded to the hypotheses in which scores were thought to be affected by demographics like population, personnel, or classification. Thus, this theoretical framework supports school active shooter prevention measurements as they are an innovation of practices and procedures that are occasionally affected by demographics.

As with any voluntary survey, errors may have occurred. To account for error, questions were intended to be as clear as possible, and ambiguous questions were provided with an opportunity to answer “I Don’t Know.” Questions were anonymized and generalized to reduce biased reporting.

Data was gathered over the course of two months. The questions outlined in the appendix were distributed via anonymous links to K-12 serving Indiana principals. Responses from principals who participated but left incomplete answers were deleted from the study. Data was dated to show the policies in place at the time of its recording. (See Table 1.) Data was collected via Qualtrics.

**Table 1.** Data gathering timeline

Data Process	Time (weeks)	Completion Date
Survey pilot creation	2–3	12/10/18
Survey pilot testing	4–5	1/7/19
Survey changes implemented	1–2	1/14/19
IRB approval waiting period	3–4	2/19/19
Survey distribution	4–8	3/11/19
Data entering and cleaning	1–2	3/11/19
Data analysis	1–2	3/22/19
Thesis defense	N/A	4/8/19

Survey responses were voluntary. The survey is composed of qualitative demographics questions and quantitative questions. The demographics questions were composed of the following:

- qualitative
  - area type (school location)
  - public or nonpublic (school classification)
  - county area (school county)
  - mental health counselor/social worker or none (school personnel)
- quantitative
  - grant applications (grant funding)
  - number of attendees (school size)
  - grades served (school type)

See Appendix A for the full list of demographics questions. The categories as listed here are further explored in what follows.

The quantitative questions correspond to both physical security measurements and social-emotional security measurements that can aid in the prevention of active shooter safety measurements. Data was analyzed after all responses were secured (see Figure 5).

Given the survey structure, a factor analysis measures the scale of how schools in Indiana compare to one another in active shooter prevention. This factor analysis allows comparisons between physical building security and social-emotional security in policy and current definitions.

The research design allowed for comparisons in school policies regarding active shooter prevention and those that exceed or fall below those standards. Thus, several tests were run to compare scores to demographic data and ascertain significance as mentioned in the research questions. First, a multiple regression analysis was run to determine whether one could predict total score based on a few factors (school location, school classification, school personnel, and school type). Two independent t-tests were run, one of which sought to determine

whether there was a group mean difference in social-emotional environment scores between having or not having a mental health counselor or social worker. The second *t*-test determined whether there was a group mean difference between public and nonpublic schools. An analysis of variance (ANOVA) compared school type and the total active shooter prevention score. Finally, correlations determined whether there was a relationship between population and score.

A forced-entry multiple regression was run because there were multiple subject variables with no specified order. The regression was run to determine whether total active shooter prevention score could be predicted from school location (School\_Local), school type (School\_Type), school classification (School\_Class), and whether the school has a mental health counselor/social worker or not (School\_MHSW).

By surveying different schools in a single state, Indiana K-12 schools can educate themselves on where they stand regarding active shooter safety. Using Indiana Department of Education reference information regarding firearm possession, school safety, cyberbullying, nonpublic accredited schools, etc., the survey represents how policy shapes these procedures. Indiana and other states can use these policies and subsequent responses to measure how well schools prevent ASIs as a result. A truncated survey focusing on two areas of active shooter prevention was created and tested to allow schools to measure their active shooter prevention.

The nondemographics questions were based on federal and state policies as they refer to current school procedures regarding ASI prevention. They were used as subject variables to compare whether schools differed in their active shooter prevention measurements.

## RESULTS

Surveys with extreme outlier data remained in the sample size as the rest of the data was complete. A respondent's choice to not disclose the population size or county was marked as missing data. Therefore, the final sample size was approximately 55 K-12 schools in Indiana. Per the central limit theorem, the dataset, though small, assumes normality. Tests for homogeneity of variance and linearity were run per the analysis required.

Many of the demographics asked for at the beginning of the survey were independent variables for analysis. The independent variables are listed below with their frequencies. (See Figure 6.)

1. From the list below, please select what neighborhood best represents the school's current location. (QD1\_SchoolLocal)

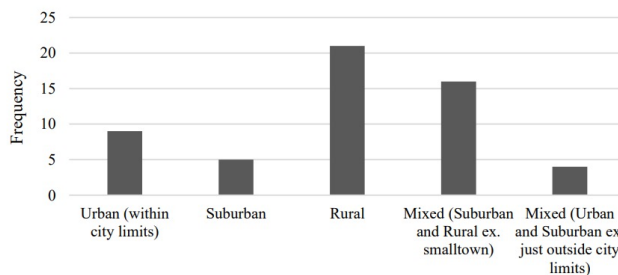


Figure 6. School frequency by location

- A. Urban (within city limits) = 9 schools
- B. Suburban = 5 schools
- C. Rural = 21 schools
- D. Mixed (Suburban and Rural ex. small town) = 16
- E. Mixed (Urban and Suburban ex. just outside city limits) = 4

Neighborhood types were based on a National Assessment of Educational Progress data analysis as reported by the National Center of Statistics and the Federal Office of Management and Budget based on the school's proximity to an "urbanized area" (National Center for Education Statistics, 2019, p. 1). Accordingly, there are four categories—city, suburb, town, and rural—and they were established in 2007 and continue to be upheld as "urban centric locale codes" (National Center for Education Statistics, 2019). However, the 2010 US census provided data that shows that there are two types of urbanized areas known as "urban clusters" (Berg, 2012). Thus, the researcher determined that having two categories, Urban (city limits) and Suburban (just outside of city limits), was necessary to accurately define a school location. Additionally, the categories were expanded to include definitions and avoid confusion.

2. What is the approximate population of your school (including students, faculty, and staff)? (QD2\_SchoolPop)
  - A. Small populations = 16 schools
  - B. Medium populations = 20 schools
  - C. Large populations = 16 schools

This response was self-reported by the principal and then coded into population size categories. The population size categories were modeled after a 1988 study of small, medium, and large secondary schools. The small schools were made up

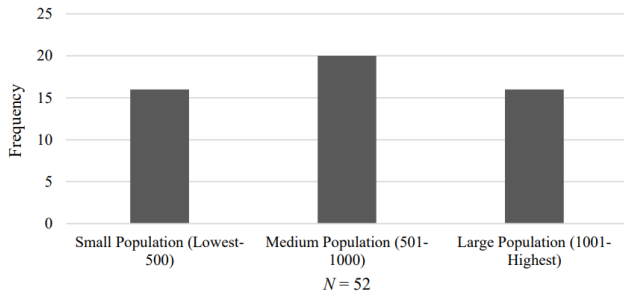


Figure 7. School population by category

of populations under 500, medium schools were between 501 and 1000, and large schools were populations of 1000 and above (Boswell & Carr, 1988). (See Figure 7.)

3. From the list, please select the grades that your school services. (QD3\_SchoolType)

Grades K-12 were all listed individually. Categories were assigned later based on grade level selected:

- i. K-12 (kindergarten–12th grade) = 19 schools
- ii. elementary (kindergarten–5th grade) = 4 schools
- iii. middle (5th–8th grades) = 8 schools
- iv. high (9th–12th grades) = 12 schools
- v. elementary and middle (kindergarten–8th grade) = 7 schools
- vi. middle and high (5th grade–12th grade) = 5 schools

The school categories were based on the US education system and the categorization of K-12 schools. These categories are given grade levels and ages that typically pertain to this system (Corsi-Bunker, n.d.). The categories do not correspond to grade level as 5th grade and 6th grade are often used in both middle school and elementary categories. (See Figure 8.)

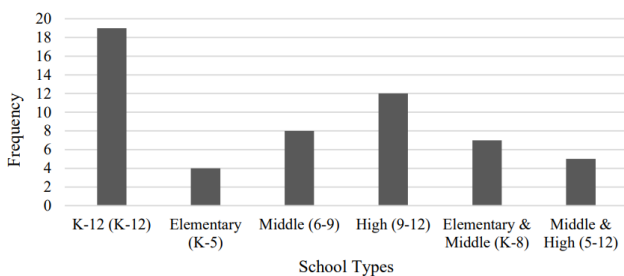


Figure 8. School grade level serviced

4. Select how the State of Indiana classifies your school. (QD4\_SchoolClass)

- A. Public = 47 schools
- B. Nonpublic = 8 schools

The school classification comes directly from Indiana state regulations on what makes an accredited school, of which there are two types: public and nonpublic. School principals were expected to know their school's classification when answering the survey (US Department of Education, 2009). In this study, a stratified sample was sought but was not attained in the interest of keeping the sample size as large as possible. In a sample of 55, the number of public schools should have been 46, and the nonpublic schools should have been 9, in keeping with the percentages of school classification reported by the Indiana Department of Education. This research was composed of 47 public schools and 8 nonpublic schools.

5. Does the school employ a mental health counselor or social worker? (QD6\_MHSW).

This question did not seek to differentiate between mental health counselors and social workers, because having either could affect the social-emotional security of a school. According to the National Association of School Psychologists, school counselors and school social workers make up part of school-based mental health services. This question revealed that 33 schools of the 55 surveyed have a mental health counselor or social worker.

These subject variables' answers were used to determine whether they predicted, influenced, or affected the dependent variables of total score (SC0), physical security score (SC1), and social-emotional security score (SC4). (See Figures 9, 10, and 11.)

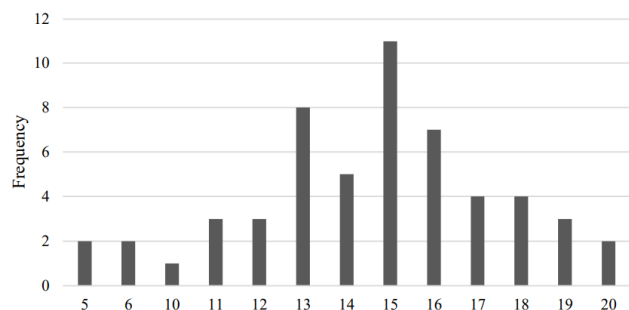


Figure 9. Total score by frequency

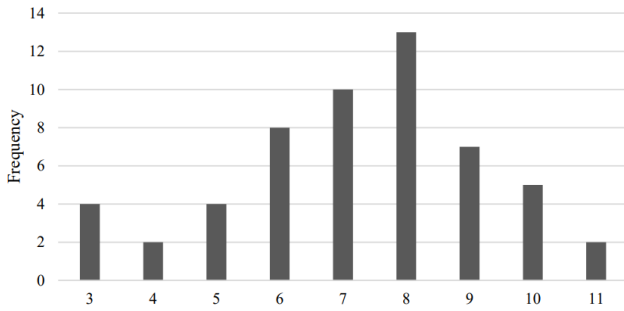


Figure 10. Physical security score by frequency

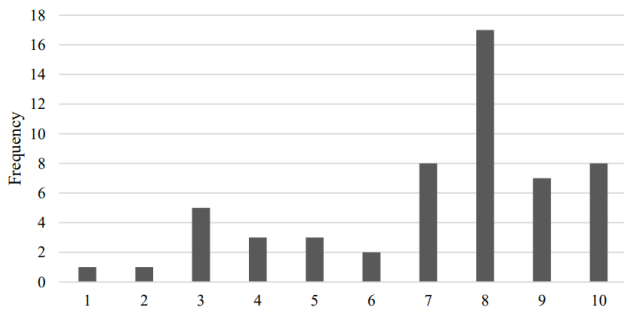


Figure 11. Social-emotional security score by frequency

The total score of the active shooter prevention consisted of two parts, physical security and social-emotional security. Though the scored portion of the survey could account for 23 points, the highest score reached on the survey was 20. It should also be noted that schools could score at least a 0, but the minimum score reported was a 5. The scores are relatively normally distributed.

The physical security of a school was composed of two types, additional resources and building design,

which consisted of seven and six scored questions, respectively. Respondents could have received scores ranging from 0 to 13. The range for these scores was 3 to 11. Thus, no respondent received a perfect score. These scores are relatively normally distributed.

Table 2 illustrates the scoring maximum, minimum, mean, and standard deviation of the scores taken by the subjects. As shown in the table, the maximum differs from the ideal for both total and physical security. This implies that no participant was able to have a perfect score on school active shooter prevention, or the subcategory of physical security. The ANOVA showed as not significantly predicting total score  $F(4,50) = 1.04$  with  $p > .05$ . (See Table 3.)

The research team ran an independent  $t$ -test as the researcher intends to compare the subject variable of public and nonpublic schools (QD4\_SchoolClass) and the outcome variable (SC0) to determine whether the two groups are on average statistically significant from each other. The subject variable is manipulated in two ways, but with two separate groups. Thus, the  $t$ -test is independent, not dependent. Levene's test was run to determine whether equal variances are assumed. Levene's test was nonsignificant, leading the researcher to read the independent  $t$ -test as such. (See Table 4.)

On average, public schools experienced higher scores on active shooter prevention ( $M = 14.66, SE = .49$ ) than nonpublic schools ( $M = 12.50, SE = 1.18$ ). There is a moderate effect,  $r = .23$ . Due to the moderate effect, the small sample size, and the exploratory nature of this research, this mean difference was determined to be statistically significant ( $t(53) = 1.68, p = .1$ ). The use of exploring relationships is measured as  $1 > p > 0.05$  (Figueiredo Filho et al., 2013). Additionally, another independent

Table 2. Descriptive statistics of scores

	N	Minimum	Maximum	Mean	Std. Deviation
Total security	55	5.00	20.00	14.35	3.42
Physical security	55	3.00	11.00	7.22	2.02
Social-emotional security	55	1.00	10.00	7.13	2.35

Table 3. Multiple regression of total score

	Unstandardized Coefficients		Unstandardized Coefficients			Collinearity Statistics	
	B	Std. Error	Beta	t	Sig.	Tolerance	VIF
(Constant)	16.755	2.369		7.072	.000		
School_Local	-.176	.329	-.076	-.536	.595	.925	1.081
School_Type	.196	.276	.100	.708	.482	.927	1.079
School_Class	-2.483	1.353	-.258	-1.835	.072	.933	1.072
School_MHSW	.295	.488	.085	.604	.549	.928	1.077

**Table 4.** Independent *t*-test of public versus nonpublic schools and total score

		<i>T</i>	<i>df</i>	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
							Lower	Upper
Total score	Equal variances assumed	1.68	53	.099	2.16	1.29	-.42	4.74

**Table 5.** Independent *t*-test of mental health counselor/social worker or not versus social-emotional security score

		<i>t</i>	<i>df</i>	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
							Lower	Upper
Social-emotional security	Equal variances assumed	-.14	53	.89	-.09	.65	-1.40	1.22

**Table 6.** School population categories ANOVA

		Sum of Squares	<i>df</i>	Mean Square	<i>F</i>	Sig.
Total score	Between groups	16.59	2	8.30	.67	.515
	Within groups	605.18	49	12.35		
	Total	621.77	51			
Physical Security	Between groups	20.13	2	10.06	2.62	.083
	Within groups	187.95	49	3.84		
	Total	208.08	51			
Social-emotional security	Between groups	.59	2	.30	.05	.951
	Within groups	292.18	49	5.96		
	Total	292.77	51			

*t*-test was run to compare the predictor variable of mental health counselors and social workers or not (QD6\_MHSW) and the outcome variable total social-emotional security score (SC4) to determine whether the two groups are on average statistically significant from each other. The subject variable is manipulated in two ways, but with two separate groups. Thus, the *t*-test is independent, not dependent. Levene's test was run to determine if equal variances are assumed. Levene's test was nonsignificant, leading the researcher to read the independent *t*-test as such.

On average, schools without a mental health counselor or social worker experienced slightly higher scores on social-emotional security ( $M = 7.18, SE = .50$ ) than nonpublic schools ( $M = 7.09, SE = .41$ ). This difference was not significant ( $t(53) = -.139, p > .05$ ). There is no effect,  $r = .02$ . (See Table 5.)

The research team ran a one-way ANOVA to see if there is a mean difference in school active shooter prevention scoring (total score, physical security, and

social-emotional security) based on school population. The school population variable was coded into categories representing small, medium, and large populations. This test was chosen as the outcome variable is categorical and there are three or more groups within the continuous predictor variable.

Levene's statistic measures the homogeneity of variance. In this case, one does not seek significance as homogeneity is not violated if the variance is evenly covered among all groups. This Levene's statistic (2,49) has a nonsignificant *p*-value ( $p > .05$ ). As shown in Table 6, there was no significant average difference on total score based on the population categories,  $F(2,49) = .125, p > .05$ . This finding represents a medium or larger effect size between total score and population. There was no significant average difference on social-emotional security score based on the population categories,  $F(2,49) = .951, p > .05$ . This represents a more medium to large effect between physical security score and population. Finally, there was no significant average difference on

**Table 7.** Social-emotional security scores based on school type

	Sum of Squares	Df	Mean Square	F	Sig.
Between groups	59.49	5	11.90	2.44	.05
Within groups	238.62	49	4.87		
Total	298.11	54			

physical security score based on the population categories,  $F(2,49) = .45, p > .05$ .

The research team ran a one-way ANOVA to see if there is a mean difference in school active shooter prevention scoring in the social-emotional security scores based on school type. The school population variable was coded into categories representing school types as defined by the grades they service. This test was chosen as the outcome variable is categorical and there are three or more groups within the continuous predictor variable. This Levene's statistic (5,49) has a nonsignificant  $p$ -value ( $p > .05$ ).

As shown in Table 7, there was a significant average difference in social-emotional security score based on the school type categories,  $F(5,49) = 2.44, p = .05$ . Thus, school types do have a significant effect on social-emotional security scores. Effect size calculations showed that there was a medium effect size ( $\omega^2 = .12$ ) for school types on social-emotional security scores.

To determine whether the groups are different, significantly or not, the researcher ran post hoc tests to compare each mean against the others. In this analysis, the researcher chose to run Tukey's at the suggestion of a statistical consultant as the data was better fit to this test given the sample size and type of test. Post hoc tests showed that being a middle school (grades 5 to 8) significantly increased social-emotional security scores as compared to being a K-12 school (Tukey,  $p = .05$ ). There was no significant mean difference between any of the other school types on social-emotional security scores.

The researcher ran a zero-order correlation between school population and social-emotional security score to see if a relationship existed. There was a statistically significant, moderate, negative relationship between

school population (School\_Pop) and social-emotional security score,  $r(52) = -.29, p = .04$ . This zero-order correlation suggests that the larger the school, the lower the score on this specific area of active shooter prevention. See Table 8.

Analysis shows how averages and scores were affected by subject variables determined through demographics. Data was cleaned before being included. The next section discusses the analysis of school active shooter prevention in the state of Indiana regarding these results.

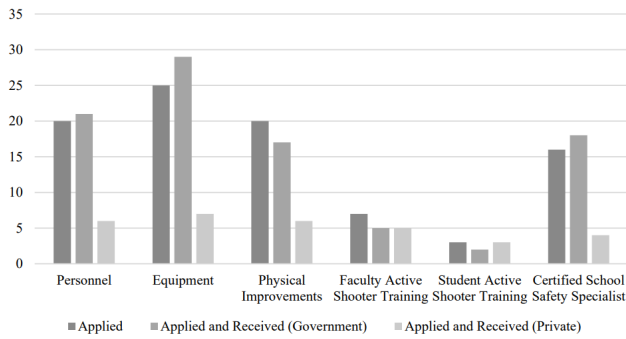
## DISCUSSION

The results indicate that a school's status, whether public or nonpublic, impacts its score on active shooter school prevention. This suggests that schools in Indiana may not be equally preventing active shooters. There was a moderate effect between public and nonpublic schools. Nonpublic schools may lack state funding in general, though they may receive similar funding through other means. This trend can be seen in the grant funding demographics question in Figure 12. The figure shows that public schools make up most grant applications in the public sector. Nonpublic schools appear to apply for more private funding, but the two are not mutually exclusive. Of the grant funding types that were reviewed (government and private), both obviously differ in frequency. Thus, it may not be just the type of grant that matters for application, but rather the application purpose. Grant funding is important for preventing ASIs as it can provide funds for training, resources to help with a school's social-emotional security, and funds to improve building conditions. Additionally, grant funding is still sought to supplement costs that may or may not be associated with active shooter prevention. Of the 55 participants, only two did not apply for grant funding in the last five years.

Results show that schools having a mental health counselor or social worker does not significantly affect scoring on social-emotional security as they may not have a direct impact on the promotion or utilization of threat assessment reporting in schools. Though the social-emotional security category was difficult to define,

**Table 8.** Correlations between social-emotional security score and population

		School_Pop	Social-emotional security score
Social-emotional security score	Pearson correlation	-.29*	1
	Sig. (2-tailed)	.04	
	N	52	55



**Figure 12.** Breakdown of grant funding applications

accurate measurement criteria was given that could prevent an ASI. The data used to represent this category includes questions regarding threat assessments completed by both students and teachers. The average social emotional score for a school ( $M = 7.13$ ) was out of 10. This category could expand to include more criteria regarding social-emotional security as it relates to active shooter prevention by incorporating learning styles or behavioral assessments (Indiana Department of Education, 2018a).

Post hoc tests show the statistical difference in mean scores on school type, suggesting that school type (K-12) may impact the focus of active shooter prevention in schools. This is shown in how middle schools scored higher on social-emotional security active shooter prevention in comparison to other groups within K-12 schools. Demographics contained within middle schools could cause the discrepancy.

Though there was no significant mean difference across school population categories, a moderate negative significant relationship was shown in school population to social social-emotional security. This is possibly explained as monitoring the environment of a school could be more of a priority or potentially a requirement. Though schools with larger populations are investing in physical security, there does not seem to be as much emphasis on social-emotional security (Chute & Mack, 2018). Further analysis should be done to fully explore the relationship between school population and scoring on social-emotional security. States can improve their promotion of certain active shooter prevention measurements by offering incentives or reforming the measurements to better suit their needs (Kaminski, 2011). This is an area that requires further research.

As shown in the 2016 NYPD report, reporting is most effective when done through sources that recognize concerning behavior (i.e., teachers, peers, parents), which is useful only if the parties receive training or instruction. As shown in Figure 12, training is less sought after than other areas for grant funding, implying that there is not

as great a push for training regarding active shooter prevention than other costlier funding allocations (personnel, equipment, physical improvements).

A discrepancy in the grant funding data shows that certifying a school safety specialist, which includes a registration fee and a training session, is more sought after than active shooter training. This may be due to the permanence of a specialist as opposed to the impermanence of training. However, low cost and uniform versions of active shooter training offer a solution to this problem as well as encourage thorough, accessible education. Additionally, of the grant funding types mentioned, active shooter training was the only area that specifically referred to active shooters.

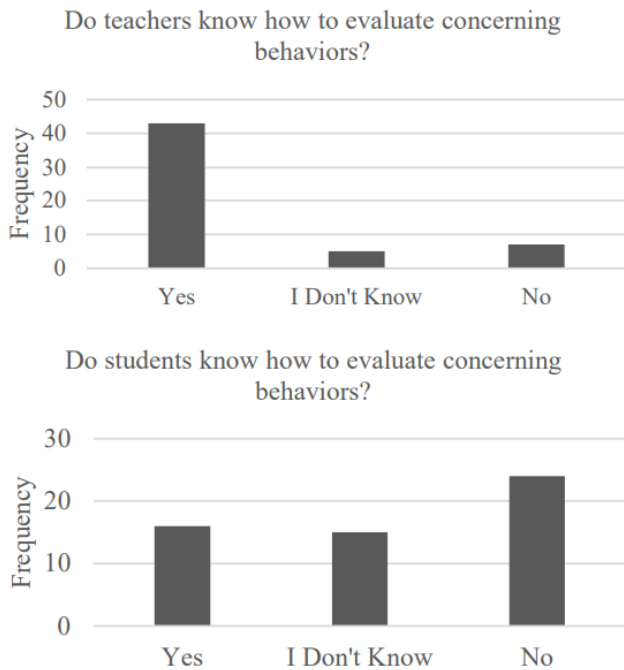
## CONCLUSION

These results, collected from the state of Indiana, could potentially be generalized to a national audience, indicating that hiring staff and making building modifications are the primary uses of grant funds to improve school safety for both public and nonpublic schools. Building modifications and training practices, which can be the least expensive and most consequential actions taken, are the least requested use of grant funds. Nonpublic schools do not seem to be overlooked by grant funding.

Social-emotional security is an area of school safety that seems to be left out of official surveys (US Department of Homeland Security, 2018b). Additionally, training focuses on the physical aspect of active shooter training, running through the scenario as opposed to the prior incidents (Zraick, 2019). Social-emotional security should also be built into active shooter training as it is essential for the prevention of ASIs. Learning how to identify concerning behavior could potentially improve social-emotional security scores and should be included in future research. This research suggests that school classification affected total score in a marginally significant way. This conclusion requires further analysis to determine why nonpublic schools have lower scores than public schools.

Recommendations for preventing ASIs in schools recognize that promoting grant funding for training as opposed to equipment and personnel is critical. Improved training would benefit the school and prevent miseducation. Low-cost and safer options could be made available at the behest of school officials. States and school corporations should also broaden training to include social-emotional security of a school along with physical training. Finally, future studies should bring in more participants like teachers, students, and school resource officers. This would help generalize results to the national level. Additional studies should explore the discrepancy





**Figure 13.** Comparison between teacher and student reporting: evaluate

between teachers and students. Studies should also work toward a greater sample size, a fully stratified study, and comparing school classifications in greater numbers if possible. The small sample may have influenced results and should be considered going forward.

Further analyses could be run for this data, particularly regarding reporting scores. Teachers, in some cases, had predominantly higher frequencies related to reporting on some questions compared to their student counterparts. Further studies should investigate these differences using this data set or expanding on it. Figure 13 shows the differences in how principals viewed teachers' knowledge for evaluating concerning behaviors versus students' knowledge for evaluating concerning behaviors. Principals reported that they had more confidence in a teacher's ability to evaluate concerning behaviors than a student's ability. Adding participants to this survey and comparing their results to the principals' could result in valuable perception and professional data.

Further recommendations include inputting physical measurements into social-emotional security. Schools should consider not only using publicly available bullying data, but also collecting student, parent, and teacher social-emotional security surveys. Software like Class-Dojo could be used to measure social-emotional security data without intruding on a classroom environment or intruding on a school day (Saeger, 2017).

Ultimately, active shooter prevention is a topic that continues to change with policy additions. States continuously improve their own active shooter prevention approaches through participation and experimentation. Thus, school active shooter prevention in the state of Indiana will remain proactive as opposed to reactive, ensuring safety for all students, faculty, visitors, and staff.

## REFERENCES

- Active shooter: Recommendations and analysis for risk mitigation.* (2016). City of New York Police Department.
- Barnett, E., & Casper, M. (2001). A definition of "social environment." *American Journal of Public Health, 91*(3), 465. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1446600/pdf/11249033.pdf>
- Berg, N. (2012, March 26). *U.S. urban population is up... but what does 'urban' really mean?* CityLab. <https://www.citylab.com/equity/2012/03/us-urban-population-what-does-urban-really-mean/1589/>
- Brown, H. (2018). Correlations versus causation. In *The Economics of Public Health* (pp. 41–55). Palgrave Pivot.
- CBC/Radio Canada. (2021, December 2). *Teen charged with murder, terrorism in Michigan school shooting as death toll rises to 4.* Retrieved February 9, 2022, from <https://www.cbc.ca/news/world/michigan-school-shooting-charges-1.6269907>
- Centers for Disease Control and Prevention. (2018). *1992–2015 school-associated violent death surveillance system (SAVD-SS).* <https://www.cdc.gov/ViolencePrevention/youthviolence/schoolviolence/SAVD.html>
- Cyber bullying.* (2018). Attorney General of the State of Indiana. <https://www.in.gov/attorneygeneral/2629.htm>
- Davies, P., & Martin, M. (2014). Children's coping and adjustment in high-conflict homes: The reformulation of emotional security theory. *Child Development Perspectives, 8*(4), 242–249. doi:10.1111/cdep.12094
- Dearing, J. W. (2009). Applying diffusion of innovation theory to intervention development. *Research on Social Work Practice, 19*(5), 503–518. doi:10.1177/1049731509335569
- DeSocio, J., & Hootman, J. (2004). Children's mental health and school success. *Journal of School Nursing, 20*(4), 189–196. doi:10.1177/10598405040200040201
- Dorn, M., Atlas, R., Schneider, T., Dorn, C., Nguyen, P., & Statterly, S. (2014). *Seven important building design features to enhance school safety and security* [Press release]. <https://www.doe.in.gov/sites/default/files/safety/seven-importantbuilding-design-features-enhance-school-safety-and-security-issa-2014.pdf>
- Fabbri, W. P. (2014, September 29). *FBI's view to improving survival in active shooter events.* *Journal of Emergency Medical Services.* Retrieved from <https://www.jems.com/administration-and-leadership/fbi-s-view-improving-survival-active-sho/>
- Federal Bureau of Investigation. (2017). *Quick look: 250 active shooter incidents in the United States from 2000 to 2017.*

- <https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics>
- Federal Bureau of Investigation. (2017a). *Making prevention a reality: Identifying, assessing, and managing the threat of targeted attacks*. <https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view>
- Federal Bureau of Investigation. (2017b). *Violence prevention in schools*. <https://www.fbi.gov/file-repository/violence-prevention-in-schools-march-2017.pdf/view>
- Federal Bureau of Investigation. (2018). *Quick look: 250 active shooter incidents in the United States from 2000 to 2017*. <https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics>
- Federal Bureau of Investigation. (2018). *Active shooter incidents in the United States in 2016 and 2017*. Retrieved February 6, 2022, from <https://www.fbi.gov/file-repository/active-shooter-incidents-us-2016-2017.pdf/view>
- Federal Bureau of Investigation. (2021). *Active shooter incidents 20-year review, 2000-2019*. Retrieved February 6, 2022, from <https://www.fbi.gov/file-repository/active-shooter-incidents-20-year-review-2000-2019-060121.pdf/view>
- Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. SAGE.
- Figueiredo Filho, D. B., Paranhos, R., Rocha, E. C. D., Batista, M., Silva, J. A. D., Jr., Santos, M. L. W. D., & Marino, J. G. (2013). When is statistical significance not significant? *Brazilian Political Science Review*, 7(1), 31–55.
- Gilbert, A. K. (2018). *Long term security auditing of large event venues* (Publication No. 108446720 [Master's thesis, Purdue University]).
- Herron, A., & Hwang, K. (2019, March 22). *Active-shooter training in Indiana school went wrong. Here's how experts say it should go*. <https://www.indystar.com/story/news/education/2019/03/22/indiana-teachers-shooter-drill-alice-training-lockdown/3244182002/>
- Hobbs, S., Zhu, Y., & Chokey, A. (2018, April 24). *New detail: How the Parkland school shooting unfolded*. <https://www.sun-sentinel.com/local/broward/parkland/florida-school-shooting/sfl-florida-school-shooting-timeline-20180424-htmlstory.html>
- Hogue, R. (2018, July 30). *General resource for school safety*. Indiana State Police.
- Huttler, D. (2019). Physical security and why it is important. *SANS Institute Reading Room*. <https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120>
- Indiana Department of Education. (n.d.). *Bullying defined*. <https://www.doe.in.gov/sites/default/files/student-services/types-bullying-main-page-2.pdf>
- Indiana Department of Education. (2016, February 14). *Climate surveys*. <https://www.doe.in.gov/safety/climate-surveys>
- Indiana Department of Education. (2018, September 11). *School building physical security and safety*. <https://www.doe.in.gov/safety>
- Indiana Department of Education. (2018, October 22). *2019 legislative priority*. <https://www.doe.in.gov/sites/default/files/legaffairs/school-safety-fact-sheet.pdf>
- Indiana Department of Education. (2018, November 14). *Find school and corporation data reports*. <https://www.doe.in.gov/accountability/find-school-and-corporation-data-reports>
- Indiana Department of Education. (2018a). *2018 Indiana school safety recommendations*.
- Indiana Department of Education (2018b). *Audit checklist for schools*. <https://www.doe.in.gov/safety>
- Indiana Department of Education. (2018c). *Compass*. <https://compass.doe.in.gov/dashboard/overview.aspx>
- Indiana Department of Education. (2018d). *Reference guide of Indiana laws related to school safety*. <https://www.doe.in.gov/sites/default/files/safety/laws-reference-2018.pdf>
- Indiana Department of Education. (2018e). *School safety requirements and best practices*. <https://www.doe.in.gov/sites/default/files/safety/doe-school-safety-requirements-and-suggested-practices-v2.pdf>
- Indiana Department of Homeland Security. (n.d.) *Introduction to metal detectors in schools*. <https://www.doe.in.gov/sites/default/files/safety/rem-sa-centermetal-detectors-schools.pdf>
- Indiana Department of Homeland Security. (2018). *School safety information and resources*. <https://www.in.gov/dhs/4043.htm>
- Indiana State Police. (2018a). *Active shooter preparedness*. <https://www.in.gov/isp/3191.htm>
- Indiana State Police. (2018b). *Unarmed response to active shooter events: Resources for schools*. <https://www.in.gov/isp/3495.htm>
- John Anthony Gardner Davis—Biographical information. (2016). Arthur J. Morris Law Library, University of Virginia School of Law. <http://archives.law.virginia.edu/person/john-anthony-gardner-davis>
- Lhamon, C. E. (2014, October 21). *Dear colleague letter: Responding to bullying of students with disabilities*. Office for Civil Rights, U.S. Department of Education.
- Maher, S. (2018, August 15). *6 months after Parkland shooting, N.H. teens advocate for gun-free school zones*. New Hampshire Public Radio. <http://www.nhpr.org/post/6-months-after-parkland-shooting-nh-teens-advocate-gun-free-school-zones#stream/0>
- Marjory Stoneman Douglas Public Safety Commission. (2019). *Marjory Stoneman Douglas High School Public Safety Commission initial report*. <http://www.fdle.state.fl.us/MSDHS/CommissionReport.pdf>
- McMahon, P. (2018, April 25). *Life and death became a matter of chance in Parkland school massacre*. Sun Sentinel. <https://www.sun-sentinel.com/local/broward/parkland/florida-school-shooting/fl-florida-school-shooting-commission-first-meeting-20180424-story.html>
- Naghavi, M., et al. (2018). Global mortality from firearms, 1990–2016. *JAMA*, 320(8), 792–814. doi:10.1001/jama.2018.10060
- National Association of School Resource Officers. (2018). <https://nasro.org/school-cpted-practitioner-certification/>
- National Center on Safe Supportive Learning Environments. (2018). *ED school climate surveys*. <https://safesupportivelearning.ed.gov/edscls/measures>

- National School Climate Center. (2022, January 3). Retrieved February 6, 2022, from <https://www.schoolclimate.org/>
- National Threat Assessment Center. (2018). *Enhancing school safety using a threat assessment model: An operational guide for preventing targeted school violence*. U.S. Secret Service, Department of Homeland Security. [https://schoolshooters.info/sites/default/files/Enhancing\\_School\\_Safety.pdf](https://schoolshooters.info/sites/default/files/Enhancing_School_Safety.pdf)
- Office of Information Technology, University of Tennessee Knoxville. (2018). *Qualtrics to QuestionPro migration*. <https://oit.utk.edu/research/documentation/qualtrics-to-questionpro/>
- Paparazzo, J., Eith, C., & Tocco, J. (2013). *Strategic approaches to preventing multiple casualty violence: Report on the national summit on multiple casualty shootings*. Office of Community Oriented Policing Services, Department of Justice. [https://schoolshooters.info/sites/default/files/Preventing\\_Multiple\\_Casualty\\_Violence.pdf](https://schoolshooters.info/sites/default/files/Preventing_Multiple_Casualty_Violence.pdf)
- Puskar, K. R., & Bernardo, L. M. (2007). Mental health and academic achievement: Role of school nurses. *Journal for Specialists in Pediatric Nursing*, 12, 215–223. doi:10.1111/j.1744-6155.2007.00117.x
- Reichart, K. E. (2019). *School active shooter prevention measurements* [Master's thesis, Purdue University]. doi:10.25394/PGS.8038706.v1
- Rivara, F. P., Studdert, D. M., & Wintemute, G. J. (2018). Firearm-related mortality: A global public health problem. *JAMA*, 320(8), 764–765. doi:10.1001/jama.2018.9942
- Rosenwald, M. S. (2018, April 29). *159 years before Columbine, the nation's first school shooting happened at UVa*. *The Washington Post*. <https://wjla.com/news/local/159-years-columbine-nations-first-school-shooting-happened-uva>
- Saeger, A. M. (2017). *Using ClassDojo to promote positive behaviors and decrease negative behaviors in the classroom*. <https://rdw.rowan.edu/etd/2443>
- SEL impact. (2019). Collaborative for Academic, Social, and Emotional Learning. <https://casel.org/what-is-sel/>
- Shapiro, E., Barr, L., & Deliso, M. (2021, December 1). *3 killed, 8 hurt in shooting at Michigan high school*. ABC News. Retrieved February 6, 2022, from <https://abcnews.go.com/US/multiple-victims-shooting-michigan-high-school-sheriff/story?id=81472178>
- Silva, J. R., & Greene-Colozzi, E. A. (2022). An exploratory study of failed mass shootings in America. *Security Journal*, 35, 367–399. doi:10.1057/s41284-020-00281-z
- Silver, J., Simons, A., & Craun, S. (2018). *A study of the pre-attack behaviors of active shooters in the United States between 2000-2013*. Federal Bureau of Investigation. <https://schoolshooters.info/sites/default/files/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf>
- Smith, J. L., & Renfroe, D. R. (2016). *Active shooter: Is there a role for protective design?* Applied Research Associates. <https://www.wbdg.org/resources/active-shooter-there-role-protective-design>
- Toppo, G. (2018, February 28). *'Gun free zones' take weapons from kids not cops*. USA Today. <https://www.usatoday.com/story/news/2018/02/28/gun-free-school-zones-draw-trumps-ire-but-advocates-protest/381902002/>
- US Department of Education. (n.d.). *The role of teachers in school safety efforts*. <https://rems.ed.gov/docs/Role%20of%20Teachers%20Presentation%20508c.pdf>
- US Department of Education. (2009). *State regulation of private schools*. <https://www2.ed.gov/admins/comm/choice/regprivschl/regprivschl.pdf>
- US Department of Education. (2017). *Indiana state regulations*. State regulations of private and home schools. <https://www2.ed.gov/about/inits/ed/non-public-education/regulation-map/indiana.html>
- US Department of Education. (2018a). *Laws & guidance*. <https://www2.ed.gov/policy/landing.jhtml?src=pn>
- US Department of Education. (2018b). *School climate and discipline*. <https://www2.ed.gov/policy/gen/guid/school-discipline/index.html>
- US Department of Homeland Security. (n.d.) *Active shooter pocket card*. [https://www.dhs.gov/xlibrary/assets/active\\_shooter\\_pocket\\_card.pdf](https://www.dhs.gov/xlibrary/assets/active_shooter_pocket_card.pdf)
- US Department of Homeland Security. (n.d.) *Emergency action plan guide: Active shooter preparedness*. <https://www.dhs.gov/sites/default/files/publications/active-shooter-emergency-action-plan-112017-508v2.pdf>
- US Department of Homeland Security, US Fire Administration, National Fire Data Center. (1999). *Wanton violence at Columbine high school* (USFA-TR-128). [www.usfa.dhs.gov](http://www.usfa.dhs.gov)
- Vagi, K. J., Stevens, M. R., Simon, T. R., Basile, K. C., Carter, S. P., Carter, S. L. (2018). Crime prevention through environmental design (CPTED) characteristics associated with violence and safety in middle schools. *Journal of School Health*, 88(4), pp. 296-305. doi: 10.1111/josh.12609
- Zhang, X., Yu, P., Yan, J., & Spil, I. T. A. M. (2015). Using diffusion of innovation theory to understand the factors impacting patient acceptance and use of consumer e-health innovations: A case study in a primary care clinic. *BMC health Services Research*, 15, 71. doi:10.1186/s12913-015-0726-2.
- Zraick, K. (2019, March 22). *Indiana teachers were shot with pellets during active-shooter drill, union says*. *New York Times*. Retrieved from <https://www.nytimes.com/2019/03/22/us/indiana-teachers-shot.html>



## **Introduction**

Intro.

Hello,

Thank you for taking this survey on school active shooter prevention measurements. This survey is geared toward Indiana principals or equivalent.

As a reminder, your response is anonymous and voluntary. Any identifiable information will be coded and then destroyed.

You will receive an opportunity to download your responses at completion. Thank you again!

## **Demographics**

QD1. From the list below, please select what neighborhood best represents the school's current location.

- Urban (within city limits)
- Suburban
- Rural
- Mixed (Suburban and Rural ex. smalltown)
- Mixed (Urban and Suburban ex. just outside city limits)

QD2. What is the approximate population of your school (including students, faculty, and staff)?

QD3. From the list, please select the grades that your school services.

- Kindergarten
- 1st Grade
- 2nd Grade
- 3rd Grade
- 4th Grade
- 5th Grade
- 6th Grade

- 7th Grade
- 8th Grade
- 9th Grade
- 10th Grade
- 11th Grade
- 12th Grade

QD4. Select how the State of Indiana classifies your school.

- Public
- NonPublic

QD5. What county is your school located in?

QD6. Does the school employ a mental health counselor or social worker?

- Yes
- I Don't Know
- No

QD6a. How are they funded?

- Through grants  
 Through private means  
 Both

QD7. To your knowledge, has your school applied for any grants in the last 5 years?

- Yes  
 No

QD7a. Click all the following that apply to your school.

	Personnel	Equipment	Physical Improvements	Faculty Active Shooter Training	Student Active Shooter Training	Certified School Safety Specialist
Applied	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applied and Received (Government)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applied and Received (Private)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Additional Resources**

Q1.AR. Do you have more than 1 scheduled lockdown/lockout drill per semester (every two months)?

- Yes
- I Don't Know
- No

Q2.AR. Do you use metal detecting technology?

- Yes
- I Don't Know
- No

Q2a.AR. Which type of metal detector do you use?

- Walk-through Metal Detectors
- Hand Held Metal Detectors
- Both

Q3.AR. Does the school reinforce (protective coatings, adhesives, internal metal, etc.) in windows?



- Yes
- I Don't Know
- No

Q3a.AR. Which type of window is reinforced?

- Internal Facing
- External Facing
- Both

Q4.AR. Does the school have a resource officer?

- Yes
- I Don't Know
- No

Q4a.AR. Please select all that apply to your school resource officer.

- Part-time
- Full time
- Shared with another school
- Monitors more than one building
- Monitors one building

Certified School Safety Specialist through the State of Indiana

Q5.AR. Does the school have any interior or exterior cameras?

- Yes
- I Don't Know
- No

Q5a.AR. Does someone monitor them throughout the school day?

- Yes
- I Don't Know
- No

### **Building Design**

Q1.BD-LR. Can teachers lock their doors from the inside?

- Yes
- I Don't Know
- No

Q2.BD-TS. Are there external barriers in place to prevent cars from driving through/into the school?

- Yes
- I Don't Know
- No

Q3.BD-RAC. Is roof access always locked unless in use by a verified professional?

- Yes
- I Don't Know
- No

Q4.BD-AC. Does the school employ a double access control system (a holding area in which visitors can be visually verified before entering the building)?

- Yes
- I Don't Know
- No

Q5.BD-NS. Does the school have fire doors?

- Yes
- I Don't Know
- No

Q5a.BD-NS. Are the fire doors locked during a lockdown/lockout scenario?

- Yes
- I Don't Know
- No

Q6.BD-AO. Are administration offices near alternate entrances and exits?

- Yes
- I Don't Know
- No

## Reporting

Q1.RPT-IS. Do students receive training on identifying concerning behavior?

- Yes
- I Don't Know
- No

Q2.RPT-IT. Do teachers receive training on identifying concerning behavior?

- Yes
- I Don't Know
- No

Q3.RPT-NS. Do students notify an authority figure about concerning behavior?

- Yes
- I Don't Know
- No

Q4.RPT-NT. Do teachers notify an authority figure about concerning behavior?

- Yes
- I Don't Know
- No

Q5.RPT-ES. Do students know how to evaluate concerning behaviors?

- Yes
- I Don't Know
- No

Q6.RPT-ET. Do teachers know how to evaluate concerning behaviors?

- Yes
- I Don't Know
- No

Q7.RPT-ITVS. Do students know how to properly intervene when another student displays a concerning behavior?

- Yes
- I Don't Know
- No

Q8.RPT-ITVT. Do teachers know how to properly intervene when a student displays a concerning behavior?

- Yes
- I Don't Know
- No

Q9.RPT-DDS. Are student reports of concerning behavior documented and disseminated?

- Yes
- I Don't Know
- No

Q10.RPT-DDT. Are teacher reports of concerning behavior documented and disseminated?

- Yes
- I Don't Know
- No

**Thank you**

Thank You.

Please continue forward to print a copy for your records.

Thank you again for your participation.

Powered by Qualtrics



## Appendix



### Purdue Military Research Institute



#### Purdue Military Research Institute (PMRI) Fellowships

The **Purdue Military Research Institute (PMRI) program**, housed in the College of Engineering, partners with the Army, Navy, Marines, Air Force, and Space Force to support graduate tuition fellowships for U.S. active-duty officers. Purdue President Chiang vigorously supports this in-resident initiative focusing first on PhD candidates, but also considers highly qualified MS applicants and then matches students with Purdue faculty preferably working on DoD funded research projects. Tuition costs and fees applicable to completing the intended degree are without cost for both the Service and the student (students are responsible for books). Costs are borne by the Graduate School and the student faculty advisor. Students receive funding for up to 3 years to complete a PhD or up to 2 years to complete a MS. We fully vet faculty to ensure they are aware of and are willing to support their program cost share as well as the accelerated program timelines. This past Fall, we brought in student # 161 and to date, approx. 98% of PMRI officers have successfully completed their graduate degrees on time.



Purdue President Chiang (back row, center), PMRI officers, faculty and staff members, March 2023

**Purdue’s graduate programs** are recognized among the best in the nation (Graduate Engineering Program ranked #4 nationally) and Purdue University is proud to be a strong partner to those who serve. Our focus is on STEM majors with application to deliberate and innovative DoD research. We believe that PMRI is the largest graduate program for military officers outside of the Air Force Institute of Technology or the Naval Post Graduate School. We are leading the way in reshaping the research universe through discovery and innovation to support the military services. We have also developed a two-semester PMRI Seminar course that features presentations by eminent scientists from the DoD and the Nation to provide the latest perspective on emerging military technology research trends. Our vision is to become a strategic national asset to synergize military research and help our Nation maintain military dominance. Photo at right shows LTC Matt Gettings conducting research at the Purdue Energetics Research Center. He is now an Assistant Professor in the Department of Chemistry and Life Science at the United States Military Academy.

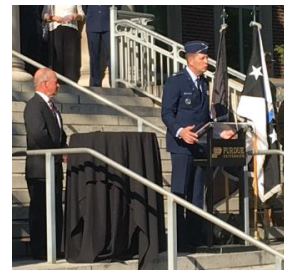


Matt Gettings, LTC U.S. Army, conducting research at the Purdue Energetics Research Center.

#### *Purdue Military Research Institute*

401 N. Grant Street, Knoy Hall, Room 259, Purdue University, West Lafayette, IN 47907-2021 • <https://engineering.purdue.edu/PMRI>

In 2021, Purdue formally entered into the **University Partnership Program** with U.S. Space Force to educate officers through specialized academics and provide Space Force ROTC members with additional educational opportunities. Purdue is also partnered with Space Force’s chief scientist for research operations through deliberate innovation to solve the most urgent technological problems and deliver operational solutions. This extends Purdue’s legacy as the “*Cradle of Astronauts*” and history of space technology and further enhances the future of space research to support the Nation. Purdue Former President Mitch Daniels and General David Thompson, Vice Chief of Space Operations, U. S. Space Force signed a historic University Partnership Program agreement in September 2021 to extend Purdue’s leadership, innovation, and legacy in space (photo right). Purdue and Space Force will partner on education and research to ensure U.S. space superiority, while preparing for the 22<sup>nd</sup> century.



Purdue President Daniels and U. S. Space Force General Thompson sign historic University Partnership Program agreement.

**Summer Intern Program.** The PMRI is working with military service branches to deliver technological solutions and educate and mentor officers in a Joint Service environment at Purdue. The Cadet/Midshipman Summer Undergraduate Research Program for Academy and Purdue ROTC students allows future military leaders to work in the lab beside and learn from PMRI officers who are solving the military’s most complex problems (photo right). The program mirrors civilian student opportunities where possible, though our military students will have visits averaging only 4-5 weeks due to their requirement to attend other summer training. Many of these students have enjoyed success with co-authorship of papers, patent disclosures, and some have joined Purdue Graduate programs. Most importantly, the program provides a win/win for all involved...our Nation, Purdue, and for the Service and officer.



Military service academy and ROTC cadets participating in the Summer Undergraduate Research Program.

**Exciting new strategic initiatives include:**

- Increased opportunities for DoD civilian scientists to earn advanced academic degrees at Purdue University to ensure the Services have the right work force to serve the Nation.
- On-line technical courses will be developed to support military enlisted education.
- An Advisory Board of political leaders, eminent scientists and military leaders is being assembled to provide independent strategic advice and recommendations that will directly benefit the DoD through world class education of military officers gaining graduate degrees at Purdue and through building deliberate innovation technologies to provide leap-ahead capabilities to the DoD.
- South China Sea Staff Ride. This Purdue innovative summer course provides students a comprehensive intellectual and experiential opportunity to study how technology and innovation leads to a US strategic policy of regional stability in the South China Sea.
- Military officers will use deliberate innovation techniques while working together in coordinated research opportunity PhD/MS degrees to solve the military’s most complex and urgent technological problems.
- Partner in research with additional agencies such as the Defense Threat Reduction Agency, Joint PEO Armaments and Ammunition, DoD Deployed Warfighter Protection (DWFP) Program, and Congressionally Directed Medical Research Programs.

**Contact Information**

Eric Dietz, Professor, Computer and Information Technology Department, Director, Purdue Military Research Institute | Cell: (765) 494-8130, [jdietz@purdue.edu](mailto:jdietz@purdue.edu)  
 Dave Hankins | Senior Project Manager, Colonel, USAF/Ret, Purdue Military Research Institute | Cell: (765) 427-8621, [dhankins@purdue.edu](mailto:dhankins@purdue.edu)



The Purdue Military Research Institute (PMRI) began in the Fall of 2014 to focus on synergistic collaboration with our military partners by offering access to some 1,900 faculty conducting world-class research in numerous research areas of significant interest to the Department of Defense. The PMRI partners with the Army, Navy and Marines, Air Force, and Space Force in three focus areas: merit-based fellowships for active-duty military members that cover all costs for graduate degree programs (except for books and incidental costs around graduation); summer intern program for undergraduates from the military academies, Purdue ROTC, and select student veterans from other US universities/colleges; and faculty exchange program.

In a world of rapidly increasing technology and surges in threat, PMRI seeks to develop defense and security leaders who, beyond excellence in military leadership, are highly capable problem solvers in a variety of STEM and non-STEM disciplines. Since 2014, over 170 military officers have successfully completed their advanced academic degrees at Purdue with a 99+% on-time graduation rate.

Through the *Innovation through Teamwork* conference, we aim to maximize a US strategic national defense advantage by expanding the partnership between the defense, academic, and innovation ecosystems. This conference will bring together defense and security program faculty, students, and external stakeholders to convene an annual event highlighting PMRI research, engagement, and impact.

**ISBN: 978-1-61249-995-6. The papers in this volume and further materials from the conference are available free of charge at: [docs.lib.purdue.edu/pmri](https://docs.lib.purdue.edu/pmri)**