ONE STEP AHEAD:

A CRITICAL INFRASTRUCTURE PROTECTION RESEARCH AND STRATEGY PUBLICATION

Spring 2025

Insights of the

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY®

ONE STEP AHEAD

A CRITICAL INFRASTRUCTURE PROTECTION RESEARCH AND STRATEGY PUBLICATION

Editorial Office:
Institute for Homeland Security
Criminal Justice Center
Sam Houston State University
PO Box 2296
Huntsville, TX 77340
Email: IHS@ihsonline.org
www.ihsonline.org

Message from the Director

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY®

Partners,

On behalf of the team here at the Institute for Homeland Security, I am pleased to present the 3rd edition of our publication One Step Ahead: A Critical Infrastructure Protection Research and Strategy Journal.

In staying One Step Ahead in research, our academic and professional partners from the critical infrastructure protection (CIP) world create innovative, value-added knowledge that meets the needs of our constituents. The following papers stand out as our "best in show" because of their exploration of unseen threats and emerging technological challenges. These papers are representative of our Core Purpose: We Stay One Step Ahead, transforming knowledge to protect critical infrastructure. It is our hope that the information herein stands to fill research gaps in the CI protection space. As it is through the dissemination of our research that we seek to sustain existing relationships and build new connections with the homeland security professional.

For a complete searchable listing of our sponsored research projects, please go to our website at www.ihsonline.org and select Sponsored Research tab. Finally, if you are interested in submitting a research proposal select the Research Proposal tab and tell us about your topic. Our team will review your submission and work with you to develop your submission. Thank you for being part of our goal to stay One Step Ahead!

Michael J. Aspland
Executive Director

Mission

The SHSU Institute for Homeland Security provides innovative, value-added knowledge tailored to the needs of industry and public institutions, to protect critical infrastructure supporting Texas and the nation's economy.

Our Four Pillars

Texas Nexus

We believe in a secure and unified Texas, connecting our private industry partners with public institutions through productive conversation.

One Step Ahead

Our focus is to stay ahead in an ever-changing security environment by providing innovative solutions that support business continuity and critical infrastructure protection.

Complement to Complete

We aim to fill the gaps and meet the needs of critical infrastructure sectors alongside our institutional partners.

Disruptive but Helpful

We believe in serving our private industry partners and public institutions in ways not done before.

Message from the Editor

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY®

THE YEAR AHEAD: TURNING INSIGHT INTO ACTION

Greetings,

As we look ahead, the Institute for Homeland Security (IHS) at Sam Houston State University is focused on deepening our commitment to people-centric, evidence-based research. Our goal is simple: to transform insight into tools, strategies, and solutions that address the challenges faced by those working to safeguard and sustain critical infrastructure.

At IHS, research is never abstract. Every project begins with a real-world question—asked by the people closest to the issue—and ends with a product designed to inform action. Whether we are evaluating the effectiveness of training, identifying patterns in organizational performance, or developing resources that improve readiness and resilience, our work is meant to equip decision makers with evidence and utility.

This past year, our team supported several infrastructure-focused collaborations that yielded tangible improvements in operational communication and preparedness. That effort wasn't just about producing findings—it was about creating usable knowledge that made a difference for the people involved. It's a reflection of what drives us: the belief that rigorous, responsive research can and should support those on the front lines.

As we move into the new year, we're continuing to seek out partnerships and proposals that align with this mission. Through the Research tab at IHSOnline.org, you'll find our proposal submission form—simple to complete and reviewed weekly by our research coordination team.
We welcome new questions, new collaborators, and new perspectives. The more precisely we can define the problems facing our communities and industries, the more effectively we can build the evidence base for solving them.

Thank you for being part of our network. We look forward to the work ahead.

Warm regards,

Ryan Randa, PhD
Deputy Director | Research
Institute for Homeland Security

Contents

RISK OF STATE-SPONSORED INTELLECTUAL PROPERTY THEFT AND PROTECTION

Nick Reese and Thomas Morin

Abstract

Intellectual property (IP) is a cornerstone of innovation and economic strength, yet it faces growing threats from state-sponsored theft. This paper explores the significance of IP theft for U.S. national security and economic stability, focusing on the legal frameworks, case studies, and methods used by state actors. It provides actionable recommendations for critical infrastructure owners and advisors to mitigate risks and enhance protections.

I. Introduction

In December of 2024, Chinese cyber actors made history. Their widespread intrusion into the American telecommunications system made their 2008 attack on the Office of Personnel Management (OPM) look minor in comparison. The attack was notable due to its breadth and that it was executed against critical infrastructure. However, many national security experts had a different take. Many looked at what China did as an indicator of its newfound cyber prowess standing in contrast to some previous attacks that were easily discovered and easily remediated. This time, Chinese actors displayed a level of sophistication that indicates they are no longer the ham-handed cyber actors of old. The Typhoons are getting stronger. China watchers and critical infrastructure personnel should be equally concerned by the Salt Typhoon attack in December 2024, but it would be a mistake to focus only on the tactical aspects of the attack itself. There is another group, a much larger group of people, that should also be concerned.

The U.S. innovation ecosystem is one of the most robust in the world attracting science, technology, engineering, and mathematics (STEM) talent from all over the world. The U.S. has a long history of long research and development (R&D) projects that create technologies that come to market and improve the lives of individuals and the efficiency of organizations across sectors. R&D is vital. It's also slow and expensive. That is why the intellectual property (IP) of companies, universities, and governments is so valuable. Far more than risking a loss of market share, in a geopolitical era dominated by the competition for the research, development, monetization, and operationalization of emerging technologies, IP is strategically important. The ability to shortcut the R&D path and develop a geostrategically important emerging technology could be decisive globally, and that fact is not lost on China nor their cyber actors.

The sophistication of the Salt Typhoon attack should cause concern among critical infrastructure operators but it should also raise flags with companies, universities, and governments who un-

The authors would like to thank Sam Houston State University and the Institute for Homeland Security for their support of this important work and dedication to emerging technology education and research for critical infrastructure.

dertake or sponsor technology R&D. The most valuable R&D does not necessarily exist inside a national laboratory or a highly classified defense or intelligence facility. It exists on the laptops of entrepreneurs, students, and engineers for private companies, and those people are targets. The theft of IP presents a direct threat to the economic and homeland security of the U.S. and will, if unchecked, grow into a national security threat. State sponsored IP theft is taking place in the cyber domain as well as the physical domain as the Chinese Ministry of State Security (MSS) is planning and executing intelligence operations inside the U.S. homeland that are directly targeting American citizens and institutions to achieve that edge in emerging technology development. With laws on the books to prosecute and punish IP theft, the U.S. law enforcement community must focus on this compatible issue to mitigate the loss of IP to state sponsored attacks on U.S. soil. As technologies like artificial intelligence (AI), quantum information science (QIS), and space technologies grow to higher levels of maturity, the U.S. must protect its national security and economic assets the way it protects its nuclear arsenal and surrounding technologies.

IP theft is a strategic action intended to give the executing nations a global advantage in emerging technology development, operationalization, and monetization. It also represents a growing issue that crosses the public, private, and academic sectors as well as homeland security and defense authorities. State-sponsored IP theft disrupts this balance by targeting sensitive technologies for geopolitical and economic gains. This paper focuses on U.S. legal frameworks, case studies of state-sponsored theft, and actionable recommendations. Sections include a methodology of research for relevant literature, an analysis of case studies, methods of IP theft, and strategic solutions.

II. Methodology

The research for this paper was conducted through a comprehensive review of relevant and reputable sources, including news outlets known for their investigative reporting on cybersecurity and IP theft, publications from federal (FBI, DHS, etc.) and international government agencies (the EU. etc), as well as peer-reviewed academic articles and research papers. Special attention was also given to relevant laws and regulations like the U.S. Economic Espionage Act, global legal infrastructure like the Trade-Related Aspects of Intellectual Property Rights (TRIPS), as well as other bilateral agreements. These sources were selected to provide a balanced and credible foundation for understanding the scope and methods of state-sponsored intellectual property theft, its impact on industries, and the legal and policy responses addressing the issue. Some priority was given to theoretical perspectives on IP theft as state actors often view IP theft as a strategy to gain economic and military advantages, using it to close technological gaps and assert dominance. Special attention was given to triangulating information across these sources to ensure accuracy and relevance.

III. Methods of Executing IP Theft

States have been attempting to and succeeding at collecting secret information on their adversaries since the beginning of organizational civilization. While the history of espionage is outside the scope of this paper, the dynamic shift between what is considered important enough to steal and the methods by which that information is stolen has shifted recently in ways that should be understood by critical infrastructure personnel, law enforcement, and homeland security professionals across the U.S. This section will examine the methods by which state actors execute their IP theft and will pull from the case studies from the previous section. The intent is to build the foundation for a risk and vulnerabilities framework that can be used by U.S. private sector entities, universities, and critical infrastructure organizations to more effectively plan their defense against IP theft. State actors employ a mix of cyber tools, espionage, and insider recruitment to access IP. Social

engineering tactics and academic partnerships often mask their intent. Advanced technologies such as AI and drones facilitate surveillance and data exfiltration, while joint ventures and research collaborations are leveraged to gain unauthorized access to proprietary knowledge. These coordinated strategies highlight the need for organizations to adopt multifaceted defense mechanisms to safeguard their intellectual property.

Most organizations are aware of the threat posed by cyber threats and many take steps to protect their cyber domain. However, cyber protections are only as useful as the understanding of who is attacking and what they want. Generic cybersecurity practices such as multi-factor authentication, minimum password requirements, file encryption, and firewalls provide a basic level of security for the organization's cyber footprint overall. While these minimum standards are not compulsory outside of a few regulated industries, they remain good practice and should be implemented widely. However, when facing a state-sponsored cyber actor with state-level resources, the minimum cybersecurity practices will not be sufficient to meet the threat. At the same time, not every private sector entity can afford the cybersecurity tools and staff required to run some of the most advanced cyber defenses in places like the federal government or the financial industry. This is what makes the identification of the "crown jewels" so critical. Every organization should understand fully the most valuable information they possess and have an understanding of who might want it and for what purpose. This view on cybersecurity changes the standard view by assuming that a cyber breach may occur, but even in the event of a breach, the most valuable data and/or systems are protected with additional layers.

Cyber espionage has been common for decades, but today's threats include powerful zero day exploits with large teams charged with their deployment and their targets are not limited to other governments. The innovation ecosystem of the U.S. requires a different view of cyber espionage because Chinese actors are not bound by the same restrictions as U.S. intelligence agencies. Next, we will explore the methods by which Chinese actors target private companies for the benefit of their domestic innovation ecosystem in the cyber domain.

Cyber Espionage

Cyber events attributed to China or China-backed actors have been prominent in the cyber landscape since at least 2015 when China hacked the federal Office of Personnel Management (OPM).[1] What has changed is the sophistication and brazen characteristics of Chinese cyber espionage against US targets. In late 2024, US officials announced two hacks attributed to China in the breach of the US telecommunications network[2] and a hack of the US Department of Treasury in December 2024.[3] It will come as a surprise to few readers that China is also willing and able to use this cyber capability against IP theft targets.

The difference between the OPM, Treasury, and telecommunications hacks and hacks against IP targets is one of cybersecurity sophistication on the part of the target. Federal government agencies and critical infrastructure entities are mostly aware that they are targets for cyber events that are backed by nation-state actors with nation-state resources. This is not the "bored teenager in his basement" image that has been popular in years past but an image of teams of individuals

1 Fruhlinger, Josh; *OPM Hack Explained: Bad Security Practices Meet China's Captain America; 2020;* https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

2 Lyngaas, Sean; *White House Official: 8 Telecom Providers Hacked by Chinese*: December 4, 2024; https://www.cnn.com/2024/12/04/politics/us-telecom-providers-chinese-hack/index.html

3 Tucker, Eric; *Chinese Hackers Accessed Workstations and Documents in a "Major" Cyber Incident, Treasury Says*; December 31, 2024; https://apnews.com/article/china-hacking-treasury-department-8942106afabeac96010057e05c67c9d5

working together to create the perfect social engineering, delivery, packaging, and exfiltration scheme around an extremely valuable zero day exploit. Federal agencies have a difficult enough time defending against this kind of concentrated effort. Small technology firms and startups make for easy and attractive targets under this model.

Central to the US's ability to continue to lead in emerging technology development is its ability to help the startup and innovator ecosystems defend their IP from state-sponsored cyber threats. What has traditionally been viewed as a matter for the private sector to deal with, technology IP on a variety of topics such as AI, quantum computing, and space resides with small technology companies. That IP should be considered information with national and homeland security implications and should receive the attention it deserves. The cyber domain is a welcoming one for actors that want to be persistent and enjoy some degree of anonymity. Cyberattacks against organizations with valuable technological IP will not stop so the US must take more seriously the need to protect it.

Non-Traditional Collectors

On June 27, 2017, at the 28th meeting of the Standing Committee of the 12th National People's Congress, a major new law was passed in China. The Chinese National Intelligence Law is a sweeping piece of legislation that gives its intelligence services broad authorities to conduct operations abroad and at home. For the purposes of this paper, Article 7 of the National Intelligence Law is relevant. Article 7 states in full (translation from Brown University):

Any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence work known to the public. The State protects individuals and organizations that support, assist and cooperate with national intelligence work.[4]

This provision means that Chinese citizens, regardless of their employment or direct affiliation with the government, are compelled to participate in intelligence operations in concert with intelligence organizations if they are asked to do so. This is an important provision of the law because it opens the door to the use of non-traditional collectors by opening the field of potential human collectors beyond traditional or known intelligence operators.

Traditionally, intelligence operators arrive in their assigned country posing as diplomats. This is called "official cover" in the business and means that they are under diplomatic protections with an official diplomatic passport. This cover provides a layer of protection for the intelligence professional should they be discovered and possibly arrested for espionage. It also creates confusion among the host law enforcement agencies about who is a real diplomat and who is actually conducting espionage. A common duty among intelligence organizations regardless of national allegiance is trying to identify the intelligence operators of your adversaries. Intelligence organizations go to great lengths to have a picture of who works for an opposing intelligence organization so that surveillance may be put into place should that person or persons ever come to your country. The goal is to know an operative is entering your country before they arrive through the visa or customs processes and to make a decision to put them under surveillance or to refuse them entry.

Non-traditional collectors create a problem with this system. Because of the 2017 National Intelligence Law, the Chinese Ministry of State Security (MSS), the Chinese foreign intelligence organization, is not limited to possibly known intelligence officers. They can choose from a pool of Chinese citizens who may have never had any affiliation with the Chinese government, military,

4 Public Law of the People's Republic of China; *National Intelligence Law of the People's Republic of China*; 2017; https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf

or intelligence apparatus. If that person, perhaps a senior academic researcher, can be trained in basic counter intelligence tactics, they will be extremely difficult for US authorities to identify and track. Intelligence analysts look for connections, even tenuous connections, between potential operators and the Chinese government or the Chinese Communist Party (CCP) to build a case that the individual may be working for the Chinese government. Without any such connection, US authorities have, and will continue to, struggle to identify unaffiliated individuals who have been sent to the US to collect IP under the 2017 National Intelligence Law.

This approach is more effective because even if a non-traditional collector is identified and caught, the penalties have traditionally been light. For example, a non-traditional collector might be charged with lying to a federal official and have their visa cancelled. From the perspective of the MSS, this is a perfectly acceptable risk because the individual in question was never going to be sent back to the US after this operation anyway.

In addition, this approach causes cultural and political tensions as accusations of racial profiling arise.[5] This creates a conflict with the culture of open innovation that sits at the core of many universities and technology companies.

In 2020, FBI Director Christopher Wray called counterintelligence and espionage the "greatest long term threat" to the US economy and called IP theft one of the greatest transfers of wealth in human history.[6] A 2017 estimate put the cost of Chinese IP theft from US sources at between $225 and $600 billion per year.[7] According to the Georgetown Security Studies Review, the FBI opens a new China-related counterintelligence case every 10 hours. This increase represents a 1,300% increase in Chinese economic espionage (IP theft) cases in the last ten years.[8]

The threat posed by IP theft is well documented and not in question. The Chinese government has the domestic tools to execute effective cyber and human-enabled operations that play outside of the boundaries of normal espionage operations. While the US does recognize the problem and has launched initiatives to counter the threat such as the China Initiative and the Disruptive Technologies Strike Force, it is increasingly falling to state and local governments and private and academic organizations to protect themselves from threats. The first step is identification of the problem and education about the scope of the issue. Next, authorities and leaders need to know what to look for and where to look. In the next section, we will cover specific case studies related to IP theft in a university and in the energy sector as a way to illustrate the problem in a real world context.

IV. Case Studies of State-Sponsored IP Theft

IP theft in universities:
State-sponsored actors frequently target universities due to their cutting-edge research, collaborative academic environments and comparatively lax security protocols. Academic partnerships, international student exchanges, and open-access publishing can serve as conduits for unauthorized access to IP. Research in fields such as biotechnology, quantum computing, and advanced materials is particularly vulnerable. This case underscores the dual challenge of fostering academic collaboration while safeguarding sensitive innovations.

5 Financial Times; *America is Struggling to Protect Intellectual Property*; https://www.ft.com/content/1d13ab71-bffd-4d63-a0bf-9e9bdfc33c39
6 IBID
7 IBID
8 Bryja, Tom; *Winning the Race: The Case for Counterintelligence Against Chinese Espionage*; January 17, 2024; https://georgetownsecuritystudiesreview.org/2024/01/17/winning-the-race-the-case-for-counterintelligence-against-chinese-espionage/

The case of Charles Lieber, former Chair of Harvard University's Chemistry and Chemical Biology Department, underscores the complex risks posed by state-sponsored IP theft in institutions. Lieber was a globally recognized nanoscientist, renowned for his groundbreaking research on nanotechnology, which was heavily funded by U.S. government grants from agencies such as the Department of Defense the National Institutes of Health.[9] However, unbeknownst to his academic peers and federal authorities, Lieber has entered into a secret agreement with China's Wuhan University of Technology (WUT) under the Thousand Talents Program,[10] a Chinese government initiative designed to attract top global talent to advance China's technological and economic objectives.[11] While these programs are often framed as legitimate academic collaborations, they have been criticized for their role in facilitating the unauthorised transfer of sensitive technologies. Lieber's case came to light in 2020 as part of the U.S. Department of Justice's (DOJ) China Initiative, which sought to investigate and address state-sponsored economic espionage and illicit academic partnerships.[12]

Lieber's involvement with WUT and the Thousand Talents Program was concealed from both Harvard University and U.S. federal grant authorities. Under his contract with WUT, Lieber was paid up to $50,000 per month, received $158,000 annually in living expenses, and was granted $1.5 million to establish a research lab in China.[13] In return, he agreed to publish articles, mentor young researchers, and facilitate collaborations with WUT.[14] Critically, Lieber failed to disclose his participation in this program and the income he received on his tax filings and in federal research funding disclosure-both required by U.S. law. Although the case did not produce direct evidence that Lieber transferred classified information or IP to China, it exemplified how foreign governments use academic partnerships to access advanced knowledge and research conducted in the U.S. Lieber's false statements to federal investigators and failure to report foreign income led to his arrest in January 2020 and his conviction in December 2021 on charges of making false statements, failing to report foreign bank accounts and tax fraud.

The Lieber case had significant consequences for the academy and national security communities, highlighting the vulnerability of universities to foreign influence and economic espionage. It reinforced the importance of strict compliance with disclosure requirements for federally funded researchers and prompted universities to reexamine their policies on foreign collaborations. In the wake of this case, federal agencies, including the National Institutes of Health (NIH) and the Department of Energy (DOE), issued stronger guidance on disclosure and tightened oversight of foreign research funding. Nevertheless, the case underscored the broader theory of nontraditional collectors, where adversaries use seemingly legitimate avenues like academic partnerships to gain access to sensitive information. The Lieber case remains a cautionary example, driving ongoing debates over how to balance academic openness with national security, particularly as

9 US Department of Justice Press Release; January 28, 2020; https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

10 Federal Bureau of Investigation; *The China Threat*; https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans

11 United States Senate Permanent Subcommitted on Investigations; *Threat to US Research Enterprise: China's Talent Recruitment Plans*; https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf

12 US Department of Justice: *Information about the Department of Justice's China Initiative and Compilation of China Related Prosecutions since 2018;* https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related

13 US Department of Justice Press Release; January 28, 2020; https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

14 IBID

adversarial nations continue to target U.S. institutions to advance their strategic goals. In the wake of the Lieber case, the U.S. government faced criticism over the DOJ's China Initiative, with some arguing that it disproportionately targeted Chinese researchers and collaborators, ultimately ending the initiative.[15] This criticism reflects the challenging nature of the non-traditional collector threat, particularly in the university environment. The vast majority of students in universities are there for legitimate purposes making it difficult and politically treacherous to execute programs to identify and eliminate non-traditional collectors.

Since the Lieber case, China's Thousand Talents program has been widely exposed as a front for IP theft.[16] The exposure has caused Chinese operational planners to shift their tactics to ensure the continued availability of IP. Universities are attractive targets for IP theft given their open learning environments and culture of cross border collaboration. However, many universities hold extremely valuable IP on topics and technologies that are in early stages of development. Such information should be closely guarded by university administrators as a potential national security threat. The Lieber case highlights the need for universities to implement programs that require disclosure of foreign activities to university officials to ensure their IP is safeguarded. Universities should also form close partnerships with state, local, and federal law enforcement agencies to ensure connectivity in the event of an incident. Many university officials are aware of the cybersecurity threats to their data and IP but live human non-traditional collectors are also a threat. Programs to safeguard IP should be built accordingly and not limited to cybersecurity protocols.

IP theft in the energy industry:
The energy sector, encompassing oil, gas, renewable energy, and grid technologies, is a prime target for state-sponsored IP theft due its role in national security and economic stability. Advanced energy technologies, such as those enabling energy storage or smart grids, can often be the focus of theft, as they provide strategic advantages in both economic and geopolitical contexts. Cyber intrusions, insider threats, and illicit technology transfer through joint ventures are common methods employed to exfiltrate critical energy-sector IP.

The 2014 cyber espionage campaign known as Operation Cloud Hopper was orchestrated by a Chinese state-sponsored hacking group identified as Advanced Persistent Threat 10 (APT10).[17] This group targeted US companies and several critical industries including the energy sector to steal valuable intellectual property and trade secrets.[18] APT-10's activities were aligned with China's Made in China 2025 initiative which aims to reduce reliance on foreign technologies and establish dominance in key sectors, including energy.[19] The US government has stated that these thefts posed not only economic threats but also risks to national security given the strategic importance of energy infrastructure and technology.[20]

15 Lucas, Ryan; *The Justice Department is Ending its Controversial China Initiative*; February 3, 2022; https://www.npr.org/2022/02/23/1082593735/justice-department-china-initiative

16 Federal Bureau of Investigation; *The China Threat*; https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans

17 Sayegh, Emil. "Spotlight on Apt10." *Forbes*, Forbes Magazine, 22 Feb. 2023, www.forbes.com/sites/emilsayegh/2023/02/21/spotlight-on-apt10/.

18 IBID

19 Center for Strategic and International Studies; *Made in China 2025;* June 1, 2015 https://www.csis.org/analysis/made-china-2025

20 "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

APT10 gained unauthorized access to the networks of energy companies by exploiting vulnerabilities in Managed Service Providers (MSPs) - third party information technology (IT) service providers frequently used by corporations to manage their IT infrastructure.[21] The hackers employed spear-phishing emails to trick employees into revealing login credentials, which were then used to breach MSPs and, subsequently, their client's networks.[22] Once inside, the hackers exfiltrated sensitive data, including research on energy systems, proprietary designs, and information on supply chains.[23] Operation Cloud Hopper exemplified how adversaries leveraged cyber espionage to attack energy companies indirectly through the supply chain dependencies Operation Cloud Hopper had profound consequences for the energy industry and broader US policy. The breach prompted a reevaluation of cybersecurity practices across energy companies in third party providers, with increased focus on supply chain security and stricter compliance requirements.[24] The theft also contributed to deteriorating US-China relations culminating in the 2018 indictment of two Chinese nationals associated with APT10 by the US Department of Justice.[25] Given the nature of this state-sponsored cyber espionage campaign, Operation Cloud Hopper underscores the urgency of international collaboration to combat cyber espionage. The case remains a pivotal example of the intersection between state sponsored cyber crime and economic competition, illustrating the need for robust defensive strategies to protect IP in critical sectors like energy.

IP Theft in Texas:

From 2012 on (with varying levels of activity), the Russian state sponsored cyber espionage group known as Energetic Bear or Dragonfly orchestrated a sophisticated series of attacks targeting energy companies across the United States and Europe.[26] These operations sought to gather intelligence on critical infrastructure and steal proprietary data, posing serious threats to national security and economic stability. Energetic Bear's activities were part of Russia's broader geopolitical strategy to exert influence over global energy markets by undermining competitors and gaining insights into advanced energy technologies.[27] The group's focus on the energy sector highlights the strategic importance of this industry to Russia as many energy exports constitute a significant share of its economy.[28] Notably Texas - a critical hub of the US energy industry - was reported as one of the regions targeted due to its concentration of energy companies and infrastructure.[29]

Energetic Bear employed a multi-faceted approach to compromise energy companies including fishing emails, watering hole attacks and malware such as Havex.[30] Watering hole attacks involved

21 Sayegh, Emil. "Spotlight on Apt10." *Forbes*, Forbes Magazine, 22 Feb. 2023, www.forbes.com/sites/emilsayegh/2023/02/21/spotlight-on-apt10/.

22 IBID

23 IBID

24 Richmond, Nathaniel. "Operation Cloud Hopper Case Study." *SEI Blog*, 4 Mar. 2019, insights.sei.cmu.edu/blog/operation-cloud-hopper-case-study/.

25 "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

26 Bing, Chris. "The Old Foe, New Attack and Unsolved Mystery in the Recent U.S. Energy Sector Hacking Campaign." *CyberScoop*, 12 July 2017, cyberscoop.com/us-nuclear-hack-russia-energetic-bear-fireeye-phishing-watering-hole/.

27 "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a.

28 Iea. "Russia - Countries & Regions." *IEA*, www.iea.org/countries/russia.

29 Mara Hvistendahl, Micah Lee. "Russian Hackers Have Been inside Austin City Network for Months." *The Intercept*, 7 Jan. 2021, theintercept.com/2020/12/17/russia-hack-austin-texas/.

30 Rodillas, Del. "Why Havex Is a Game-Changing Threat to Industrial Control Systems – Part 1." *Unit 42*, 17 July 2014, unit42.paloaltonetworks.com/havex-game-changing-threat-industrial-control-systems-part-1/.

compromising websites frequently visited by energy sector employees, planting malware to infect visitors' devices. Once inside the network, hackers access sensitive information, including operational data, blueprints for energy infrastructure, and research on industrial control systems (ICS).[31] The Havex malware was particularly notable for its ability to map and compromise ICS systems, potentially allowing attackers to disrupt operations and connect sabotage.[32] While no confirmed cases of operational disruption occurred, the theft of critical data is significantly increased risk for targeted companies, including those in Texas, where several energy firms were reportedly compromised.[33] The stolen information could have been used to develop competing technologies, compromised systems, or prepare for future attachment energy infrastructure.

The Energetic Bear campaign exposed critical vulnerabilities in the energy sector, particularly concerning supply chain security and Industrial control systems. In Texas, where the energy sector plays a vital role, these attacks highlighted the importance of robust cybersecurity measures to protect critical infrastructure. The US government responded by increasing regulatory requirements and emphasizing the need for public private collaboration on cybersecurity.[34] The attacks also reinforced the theory of cyber enabled economic warfare, which posits that state-sponsored actors use cyber espionage to undermine competitors' economic advantages. Additionally, these events underscored the risks of cascading consequences and interconnected energy networks, as any disruption in Texas - home to extensive oil and gas infrastructure - could have national and even global repercussions.[35] The Energetic Bear case remains a critical example of how state sponsored cyber activities can impact both economic competitiveness and national security.

Analysis of patterns and implications:
Both universities and the energy sector face distinct but overlapping vulnerabilities. Universities often serve as entry points for initial reconnaissance or data collection, which can later be exploited by malicious actors targeting industry partners. In the energy sector, stolen IP can undermine competitive advantages, compromise infrastructure security, and disrupt innovation. In both cases, the IP theft was sponsored by state actors bringing state-level resources to the operation. Cyber has traditionally been the domain of choice, but increased cybersecurity measures across the sector have given rise to other methods of theft. These trends highlight the need for sector-specific strategies to counteract state-sponsored theft while ensuring operational and research integrity.

In the academic world and in critical infrastructure, growing and maintaining an attractive innovation ecosystem for new technologies is a critical element of continued growth and a way to attract new ideas. If these sectors are unable to protect themselves from state-sponsored IP theft, innovators will not be inclined to build new technologies in these environments. Research and Development is a long and sometimes expensive process, so incentives to shortcut it are high. Competitive advantages will be lost by both academia and industry if this problem is not properly mapped and addressed. The issue becomes one of security of the homeland if it proliferates beyond just a few cases as state actors are conducting sanctioned operations inside the US home-

31 "Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a.

32 IBID

33 Symantec. *Dragonfly: Cyberespionage Attacks against Energy Suppliers*,2014, docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers.

34 "Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a.

35 "U.S. Energy Information Administration - EIA - Independent Statistics and Analysis." *EIA*, www.eia.gov/state/analysis.php?sid=TX.

land. The decentralized nature of this problem requires individual organizations to take action commensurate with their mission and priorities. Organizations should prioritize plans for mitigating and reporting IP theft according to the realities on the ground.

Patterns of Theft

Both the Lieber case and the Energetic Bear campaign reveal distinct yet overlapping patterns of intellectual property theft. In the Lieber case, the theft revolved around leveraging academic collaborations to siphon off advanced research, with the Thousand Talents Program acting as a conduit for recruiting US based scientists to share proprietary knowledge.[36] By embedding these relationships in ostensibly legitimate exchanges, the perpetrators exploited transparency norms in academia to mask malicious intent.[37] Energetic Bear, on the other hand, relied on cyber espionage techniques like phishing and watering hole attacks to access sector networks.[38]

Despite differing operational methods, both cases targeted sectors critical to national security- biotechnology and energy- highlighting a consistent pattern of adversaries focusing on cutting edge technologies and critical infrastructure. These case studies underscore the trend of exploiting systemic vulnerabilities in high-value industries for strategic economic and military gains.

Implications

The implications of these thefts extend far beyond financial losses to the victim organizations. The Lieber case demonstrated how state-sponsored programs like the Thousand Talents Program weaponized academic openness to advance technological development in foreign adversary nations, potentially undermining US leadership in key Industries such as nanotechnology. Similarly, Energetic Bear's cyber attacks on the US energy sector revealed the fragility of critical infrastructure, demonstrating how stolen industrial control system (ICS) data could be used for future sabotage or to develop competing technologies. Both incidents underscore the potential for economic espionage to serve as a tool of geopolitical influence, allowing foreign adversaries to accelerate their technological progress while weakening the US's competitive edge and security resilience.

Risk Factors from Case Studies

Key risk factors enabled the success of these thefts in both case studies. In the Lieber case, the decentralized oversight of academic partnerships and inadequate vetting processes allowed the Chinese government to exploit university research programs.[39] Furthermore, Lieber's failure to disclose his affiliations reflected broader systemic gaps in enforcing compliance with federal funding requirements. For Energetic Bear, the risk factors were rooted in the cyber vulnerabilities of the energy sector, particularly its reliance on aging ICS infrastructure and insufficient cyber security

36 US Department of Justice Press Release; January 28, 2020; https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

37 "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases." *Office of Public Affairs | Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases | United States Department of Justice*, 28 Jan. 2020, www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

38 *Dragonfly: Cyberespionage Attacks against Energy Suppliers*, Symantec, 2014, docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers.

39 "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases." *Office of Public Affairs | Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases | United States Department of Justice*, 28 Jan. 2020, www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

defenses.[40] The targeting of Texas-based energy firms, a hub for oil and gas industries, highlights how regional concentrations of high value assets can amplify risk exposure. These cases illustrate how a combination of institutional complacency, lack of oversight and inadequate cybersecurity can create fertile ground for intellectual property theft.

- Decentralized Oversight of Academic Partnerships
- Inadequate Vetting Processes
- Cyber Vulnerabilities
- Aging Infrastructure
- Insufficient Cyber Defenses
- Lack of Cohesive Strategy
- Lack of Information Sharing

V. Risk Factors and Vulnerabilities for US Businesses

Cybersecurity Defenses in Critical Infrastructure

The case studies of Energetic Bear, the Lieber case, and APT10 illustrate critical risk factors that expose U.S. businesses to IP theft and cyber espionage. One of the most prominent vulnerabilities is the lack of robust cybersecurity defenses in critical infrastructure sectors. Energetic Bear, a Russian state-sponsored threat actor, exploited outdated ICS in the U.S. energy sector, using phishing emails and watering hole attacks to gain access to sensitive operational technology.[41] Many energy firms, those in Texas being no exception, rely on legacy systems that prioritize reliability over security, creating exploitable gaps that allow adversaries to conduct reconnaissance and potentially disrupt operations.[42] Similarly, APT10, a Chinese cyber-espionage group, leveraged weaknesses in managed service providers (MSPs) to infiltrate U.S. corporations, particularly in healthcare, finance, and defense sectors.[43] These cases underscore the growing threat of supply chain vulnerabilities, where businesses unknowingly inherit security risks from third-party service providers.

Exploitation of Academic and Corporate Partnerships

Beyond technical vulnerabilities, the exploitation of academic and corporate partnerships serves as a major risk factor.

40 "Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a.

41 Bing, Chris. "The Old Foe, New Attack and Unsolved Mystery in the Recent U.S. Energy Sector Hacking Campaign." *CyberScoop*, 12 July 2017, cyberscoop.com/us-nuclear-hack-russia-energetic-bear-fireeye-phishing-watering-hole/.

42 "How Renewable Energy Can Make the Power Grid More Reliable and Address Risks to Electricity Infrastructure." United States Joint Economic Commitee.,19 Jan. 2024, www.jec.senate.gov/public/index.cfm/democrats/2024/1/how-renewable-energy-can-make-the-power-grid-more-reliable-and-address-risks-to-electricity-infrastructure#:~:text=The%20aging%20U.S.%20electrical%20grid,replacing%20in%20the%20coming%20decades.

43 "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

The Lieber case exemplifies how foreign governments leverage talent recruitment programs, such as China's Thousand Talents Program, to extract cutting-edge research from top U.S. institutions.[44] By providing financial incentives and exploiting weak disclosure requirements, these programs facilitate the illicit transfer of intellectual property, often without immediate detection. APT10 used a different but related tactic—compromising MSPs —to gain access to trade secrets and sensitive research from multiple corporations at once.[45] These cases reveal how businesses and universities, eager to engage in global collaboration, may unintentionally expose proprietary data to foreign adversaries through inadequate oversight and compliance enforcement.

Insider Threats

Another significant risk is the human element and insider threats, which play a crucial role in both cyber and physical theft of intellectual property. While Energetic Bear and APT10 relied on cyber-based intrusions, Lieber's case demonstrated how individual actors within research institutions can become conduits for foreign adversaries. Insider threats—whether intentional, as in Lieber's case, or unintentional, such as employees falling for phishing scams—remain a persistent vulnerability across industries.[46] Many businesses and institutions lack comprehensive security awareness training, making employees susceptible to social engineering tactics that facilitate cyber intrusions. Additionally, the increasing sophistication of state-sponsored cyber operations means that traditional security measures, such as firewalls and endpoint detection, are often insufficient without proactive threat intelligence and real-time monitoring.

This study identified these three major risk factors, which should be operationalized by organizations in the form of a cohesive IP theft risk mitigation strategy and workforce training. These factors serve as a foundation for organizations to build policies and strategies to guide their organizations in the time of increased threat from state-sponsored actors. The threats posed come from both cyber actors and human collectors making risk mitigation difficult. However, organizations can begin mitigating these threats through strategic planning and training their workforce to recognize the threats. The primary recommendations of this paper are:

- Strategic planning to create risk-informed policies
- Workforce training
- Mapping of the primary targets of IP theft inside Texas

Undertaking these efforts will ensure the integrity of the innovation ecosystem in Texas and beyond facilitating ongoing technological and economic development. IP theft is a threat to organization and to the homeland if left unchecked. It is currently pursued on a small scale by law enforcement necessitating action by individual organizations. This research will help organizations take the first critical steps toward a safe and secure innovation ecosystem.

44 US Department of Justice Press Release; January 28, 2020; https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

45 "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

46 "Defining Insider Threats: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats.

VI. Recommendations for Critical Infrastructure Owners and Operators

To mitigate the risks posed by state-sponsored IP theft and cyber espionage, critical infrastructure owners and advisors must adopt a multi-layered security approach that integrates both technical and organizational safeguards. One of the most immediate priorities is strengthening cybersecurity defenses through continuous monitoring, threat intelligence sharing, and zero-trust architecture. The Energetic Bear campaign demonstrated how nation-state actors exploit outdated ICS in the energy sector to gain unauthorized access.[47] To counteract this, organizations should implement network segmentation, ensure endpoint detection and response (EDR) capabilities, and regularly update systems to close exploitable security gaps. Additionally, participation in industry-specific cyber intelligence-sharing initiatives, such as the Electricity Information Sharing and Analysis Center (E-ISAC), could enable organizations to stay ahead of evolving threats(*).

Beyond technical controls, enhancing third-party risk management is crucial, as demonstrated by APT10's infiltration of managed service providers (MSPs) to access sensitive corporate and government data.[48] Organizations should conduct rigorous security assessments of all vendors and cloud service providers, requiring compliance with robust cybersecurity frameworks such as the NIST Cybersecurity Framework or the Department of Energy's Cybersecurity Capability Maturity Model (C2M2)(*). Contracts with third-party providers should include strict security requirements, including continuous monitoring, multi-factor authentication, and incident response plans. Furthermore, the push for data sovereignty measures, where critical infrastructure companies limit reliance on foreign cloud providers and enforce stronger encryption standards, can significantly reduce exposure to adversarial cyber operations.

Another vital recommendation is strengthening insider threat programs and enforcing stricter disclosure requirements for research and technology partnerships. The Lieber case underscores how foreign adversaries exploit talent recruitment programs to extract sensitive research from U.S. institutions.[49] Critical infrastructure organizations should adopt enhanced vetting procedures for employees and collaborators, particularly those engaged in proprietary research and development. The implementation of continuous monitoring systems for anomalous data access and exfiltration, along with mandatory disclosure of foreign funding for research initiatives, can prevent intellectual property leakage. Furthermore, industry leaders should work closely with academic institutions to ensure that federally funded research remains protected under various regulatory structures.

Understanding where we are most vulnerable is the first step toward effective mitigation. We also recommend that individual organizations create internal maps of where their critical IP resides organizationally and within their virtual environment. To guide this, the State of Texas should create a geographic map of the most vulnerable regions to state-sponsored IP theft and marshal resources to those locations. Creating better security and resilience is always a goal for critical infrastructure and that should extend to IP protection. Understanding the geographic and organizational vulnerabilities is an important step to creating effective risk management.

47 "Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical.

48 "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *Office of Public Affairs, United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

49 US Department of Justice Press Release; January 28, 2020; https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

Lastly, investing in workforce training and incident response readiness is essential to creating a resilient security culture. Employees remain a primary attack vector, whether through phishing attempts, social engineering, or direct recruitment by foreign adversaries. Organizations should conduct regular security awareness training tailored to evolving threats, with a focus on detecting social engineering tactics and recognizing cyber intrusion indicators. Additionally, developing and testing incident response playbooks through red team/blue team exercises ensures that organizations can rapidly contain and mitigate cyber incidents. Close collaboration with government agencies such as CISA, the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), and the FBI's Counterintelligence Division can provide critical infrastructure owners with the necessary support to strengthen their defenses against state-sponsored threats.

By implementing these recommendations, critical infrastructure owners and advisors can build a more secure and resilient operational environment, reducing the likelihood of successful IP theft and cyber espionage campaigns conducted by foreign adversaries.

Authors Biographies

Nick Reese is the founder and CEO of Triantha and a Strategic Advisor to the Space ISAC. He is a former federal government space policy maker and an adjunct professor at the NYU Center for Global Affairs.

Thomas Morin is an Emerging Technology Consultant and curriculum developer at Triantha. He is a graduate of the NYU Center for Global Affairs and is an expert in the geopolitical implications of emerging technology


Nick Reese


Thomas Morin

Suggested citation: **Reese, N., & Morin, T.** (2025). Risk of state-sponsored intellectual property theft and protection. *One Step Ahead*, *July 2025*, 1–14. The Sam Houston State University Institute for Homeland Security. OSF | Risk of State-Sponsored Intellectual Property Theft and Protection

THE GROWING ROLE OF ARTIFICIAL INTELLIGENCE IN TOMORROW'S URBAN HYDROLOGICAL INFRASTRUCTURE

Liya Abera

Abstract

Urban hydrological infrastructure is vital for sustainable water management in cities, yet it faces significant challenges from climate change, rapid urbanization, and aging infrastructure. These challenges exacerbate water scarcity, increase flood risks, and strain existing infrastructure, underscoring the urgent need for innovative and adaptive solutions. Artificial Intelligence (AI) has emerged as a transformative tool, offering advanced capabilities in predictive maintenance, flood risk modeling, water quality monitoring, and urban planning. This study aims to explore AI's growing role in managing urban hydrological infrastructure. A qualitative approach was employed, utilizing a systematic review and bibliometric analysis to synthesize knowledge and identify trends in the field. Scopus was selected as the primary database due to its extensive coverage of multidisciplinary research. Keywords such as "urban hydrology," "artificial intelligence," "machine learning," "water management," "extreme events," and "flood prediction" were used, yielding a dataset of 2,098 relevant documents. The analysis identified five primary clusters of AI applications within urban hydrological infrastructure. These include AI in flood prediction and early warning systems, AI in urban water demand forecasting, AI in real-time water quality monitoring, AI in optimization of stormwater management systems, and AI in urban flood risk assessment and mapping. The originality of this research lies in its explorative analysis of AI's role in enhancing the efficiency, resilience, and sustainability of urban water systems. Furthermore, it offers practical insights for policymakers, engineers, and urban planners, paving the way for integrating cutting-edge technologies into urban water management. This study also contributes to the growing discourse on sustainable urban development, demonstrating how AI can revolutionize hydrological infrastructure to meet the demands of an increasingly complex and dynamic world.

Keywords: Artificial Intelligence (AI), Climate Change, Resilient Infrastructure, Stormwater Management, Sustainable Water Systems, Urban Flood Risk Assessment, Urban Hydrological Infrastructure.

1. Introduction

Urban hydrological infrastructure plays a critical role in managing water resources within densely populated areas. It comprises a complex network of systems, including stormwater drainage,

Liya Abera, Stantec, Raleigh, North Carolina

wastewater treatment, water supply networks, and flood control measures (Fletcher *et al.,* 2024). These systems are designed to ensure the sustainable and equitable distribution of water resources while mitigating the risks associated with water scarcity, flooding, and pollution. However, urban hydrological infrastructure faces unprecedented challenges in the 21st century. Aliu et al., (2024) and Ebekozien et al., (2024) highlight that climate change intensifies extreme weather events, resulting in more frequent and severe droughts, floods, and heatwaves. Rising global temperatures exacerbate water scarcity issues, while increased precipitation in some regions contributes to more frequent and intense flooding events (Otto *et al.,* 2023). Urbanization compounds these challenges as land-use changes and the proliferation of impervious surfaces disrupt natural hydrological processes, leading to increased runoff, reduced infiltration, and heightened flood risks (Abraham *et al.,* 2023; Neog *et al.,* 2024; Soori *et al.,* 2024).

Additionally, aging infrastructure, inadequate maintenance, and rapid population growth strain existing urban water systems (Abera, 2022). Moreover, many cities in both developed and developing countries struggle to meet rising water demands while addressing issues related to aging infrastructure, pollution, and the adverse effects of climate change. These interrelated challenges underscore the urgent need for innovative and sustainable solutions to ensure urban water systems' long-term resilience and sustainability. Advancing the integration of emerging technologies, such as artificial intelligence (AI), could provide transformative approaches to address these issues and enhance the management of urban hydrological infrastructure.

According to Shahin *et al.,* (2024) and Sharifi *et al.,* (2024), AI encompasses a wide range of computer-based disciplines focused on creating intelligent systems capable of performing tasks traditionally carried out by humans. In water resources management, AI has made notable advancements, mainly through the adoption of sophisticated models such as Artificial Neural Networks (ANNs), Support Vector Machines (SVMs), Decision Trees (DTs), Random Forests (RFs), Gradient Boosting Machines (GBMs), and hybrid methodologies (Ye *et al.,* 2021; Samadi, 2022; Soori *et al.,* 2024). Early applications of ANNs were crucial in improving river flow predictions, particularly in areas with limited historical data (Yang *et al.,* 2019). These networks excelled at identifying complex, nonlinear relationships between climatic inputs and hydrological outputs, paving the way for broader AI utilization in water management. As challenges in hydrology grew more intricate, techniques such as SVMs and fuzzy logic systems became indispensable (Zhu *et al.,* 2022). These methods effectively addressed uncertainties like fluctuating rainfall patterns and varying soil moisture levels, scenarios where traditional models often struggled due to limited or inconsistent data. AI's capacity to handle large datasets and predict extreme meteorological events, including floods and droughts, has significantly enhanced disaster preparedness. For example, in the Mississippi River Basin, USA, Ganges-Brahmaputra-Meghna Basin, South Asia, and several others, AI-driven flood risk prediction and mitigation strategies have been instrumental in enhancing early warning systems, optimizing resource allocation and improving the resilience of vulnerable communities against extreme hydrological events. Similarly, AI models have demonstrated exceptional efficacy in groundwater management in regions facing water scarcity. These models help forecast groundwater levels and recharge rates, promoting more sustainable resource utilization.

Furthermore, AI has revolutionized water quality management by enabling real-time monitoring and contaminant assessment, as seen in the Ganges River in India, the Mississippi River in the USA, the Danube River in Europe, the Mekong River in Southeast Asia, and the Nile River in Africa. These systems have significantly improved the ability to track pollution sources, assess turbidity levels, and monitor ecosystem health. AI-powered Smart Microclimate Control Systems (SMCS) have transformed resource management in the agricultural sector. By optimizing factors such as temperature, humidity, and soil moisture, these systems have boosted crop yields while improving water-use efficiency (Haider *et al.,* 2024). These diverse applications highlight AI's critical role in

addressing the multidimensional challenges posed by climate change, growing water demands, and environmental variability.

In light of its potential, this review seeks to explore the growing role of AI in managing urban hydrological infrastructure through a qualitative approach, providing an in-depth understanding of the subject via detailed analysis of secondary data. Furthermore, the study offers practical insights and recommendations based on its findings. Ultimately, this research contributes to the expanding discourse on integrating advanced technologies into urban water systems, paving the way for more adaptive and sustainable infrastructure to meet the demands of a rapidly changing world.

2. Review of Existing Studies

2.1. Historical Overview of AI Applications in Urban Hydrological Infrastructure

The use of AI in urban hydrological infrastructure started in the early 1980s, coinciding with advancements in computational power and the development of early machine learning algorithms. During this period, AI applications primarily focused on rule-based and expert systems to simulate water flow and predict hydrological behavior. For instance, researchers utilized these systems to simulate rainfall-runoff processes, allowing urban planners to predict flood risks in specific regions. These rule-based systems were limited in scalability and adaptability but marked the initial steps toward automating complex hydrological computations (Maisonobe, 2022). By the late 1980s, Artificial Neural Networks (ANNs) emerged as a groundbreaking AI tool. Early applications of ANNs aimed to improve hydrological forecasting by capturing nonlinear relationships between climatic variables and water flow dynamics. In urban contexts, ANNs were applied to model stormwater drainage systems, providing more accurate predictions of flood events in cities. This period also witnessed the integration of AI with Geographic Information Systems (GIS), enabling spatial analysis of urban hydrological systems to better understand drainage patterns and areas prone to flooding (Zhao *et al.,* 2021).

The mid-1990s marked a significant expansion in the scope of AI applications in urban hydrology, driven by advancements in computing and data availability. During this time, Support Vector Machines (SVMs) and Fuzzy Logic systems were introduced to manage the uncertainties inherent in hydrological data (Yang *et al.,* 2019). These AI models enhanced the accuracy of flood prediction, groundwater recharge estimation, and pollutant transport modeling. For instance, SVMs were employed in urban areas to predict the impacts of heavy rainfall on stormwater systems, offering insights into flood mitigation strategies. Fuzzy Logic systems became particularly valuable for decision-making in water quality management, allowing for real-time assessment of urban water bodies affected by industrial and domestic pollutants (Maisonobe, 2022). Simultaneously, hybrid AI models combining ANNs, SVMs, and Fuzzy Logic gained traction. These models proved highly effective in managing urban water systems by addressing challenges like the variability of precipitation and the impact of impervious surfaces on runoff. This era also saw increased collaboration between AI and remote sensing technologies, which enhanced urban hydrological data collection and analysis (Fletcher *et al.,* 2024).

The 2010 era paved the way for a new era of AI applications characterized by the rise of big data and advanced machine learning techniques. With the proliferation of sensors and IoT devices, urban areas began generating vast amounts of real-time hydrological data, enabling the application of sophisticated AI models. Gradient Boosting Machines (GBMs), Random Forests (RFs), and Deep Learning models emerged as dominant tools during this period. These models handled large, high-dimensional datasets, allowing for improved flood forecasting, water demand prediction, and stormwater management. Deep Learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), were used for time-series analysis of rainfall and river flow

patterns, enabling urban planners to make more informed decisions (Panahi *et al.,* 2021). One notable advancement was the integration of AI with smart water grid systems, which utilized real-time data from sensors installed in urban water distribution networks to optimize water allocation, detect leaks, and monitor water quality (Maisonobe, 2022). In the 2020s, the focus has shifted toward sustainability and resilience as climate change and rapid urbanization have intensified challenges such as water scarcity, flooding, and infrastructure aging. To address these issues, AI-driven solutions are increasingly being used for adaptive water management and disaster preparedness. Presently, AI models now incorporate Nature-based Solutions (NbS) to design urban landscapes that mitigate flood risks while promoting biodiversity (Aghimien *et al.,* 2024). For example, AI algorithms are used to model the effectiveness of green roofs, permeable pavements, and urban wetlands in managing stormwater runoff. Furthermore, AI has been instrumental in advancing the circular economy of water. By predicting wastewater composition and optimizing its treatment, AI enables the recovery of resources such as nutrients and energy, contributing to sustainable urban water management (Zhu *et al.,* 2022). Table 1 summarizes the evolutionary milestones of AI in urban hydrological infrastructure.

Table 1. Evolutionary Milestones of AI in Urban Hydrological Infrastructure

Period	Key milestone
The early 1980s	The use of rule-based and expert systems for hydrological modeling began, marking the initial steps toward automating complex hydrological computations.
The late 1980s	ANNs emerged as a significant tool for improving hydrological forecasting and modeling stormwater drainage systems.
Mid-1990s	The introduction of SVMs and Fuzzy Logic systems helped manage uncertainties in hydrological data, enhancing flood prediction and water quality management.
The 2010s	The rise of big data and advanced machine learning techniques, including Gradient Boosting Machines (GBMs), Random Forests (RFs), and Deep Learning models, improved real-time analysis and decision-making in urban water management.
The 2020s	AI-driven solutions have increasingly focused on sustainability and resilience, incorporating NbS and advancing the circular economy of water.

2.2. Challenges in Urban Hydrological Infrastructure and the Role of AI

One of the most pressing issues is aging infrastructure. In many urban areas, particularly in developing nations, water distribution networks, drainage systems, and treatment facilities have surpassed their designed lifespans (Ferreira et al., 2022). These systems suffer from inefficiencies such as leaks, contamination, and reduced capacity to handle current demands. Also, AI-driven predictive maintenance systems are revolutionizing this space by analyzing sensor data to detect early signs of wear or potential failures (Otto et al., 2023). Machine learning models can also forecast pipeline bursts or drainage blockages, allowing cities to proactively address issues, minimize disruptions, and extend the lifespan of their infrastructure. Urbanization further exacerbates these challenges. As cities expand, water demand increases and the increase in impervious surfaces (such as concrete and asphalt) leads to higher runoff, reduced groundwater recharge, and increased flood risks (Pokhrel et al., 2022). AI offers a solution by simulating water flow and modeling the impact of urban development on existing hydrological systems. These tools use geospatial data and advanced algorithms to identify areas prone to flooding or water scarcity, helping urban planners design more resilient and adaptive infrastructure (Ferreira et al., 2022).

Climate change compounds these problems by intensifying extreme weather events, including floods and droughts (Sharifi et al., 2024). As such, urban hydrological systems are often overwhelmed by heavy rainfall or strained by prolonged dry spells, with traditional models failing to predict the increasing variability of climatic conditions. AI excels in processing large datasets from weather stations, satellites, and historical records to provide accurate forecasts and risk assessments (Zhu et al., 2022). AI-driven flood prediction models, for example, integrate meteorological data with real-time hydrological measurements, enabling early warning systems that save lives and reduce economic losses. Water quality management is another significant challenge in urban areas, where industrial discharges, untreated sewage, and runoff pollute water bodies. Traditional water quality monitoring methods rely on extensive manual sampling, which is time-consuming and often ineffective in detecting real-time contamination (Saheb et al., 2019). AI-powered monitoring systems use sensors and machine learning algorithms to instantly analyze water parameters like turbidity, pH, and contaminant levels. These systems help authorities identify pollution sources, assess ecosystem health, and ensure safe and sustainable water supplies (Ferreira et al., 2022). However, adopting AI solutions is not without its challenges. Many cities cannot afford the infrastructure or skilled workforce required to deploy and maintain AI technologies (Haider et al., 2024). Researchers focus on developing cost-effective AI tools to overcome resource-constrained challenges. Cloud-based platforms and open-source machine learning frameworks are making AI more accessible and reducing the financial and technical hurdles to adoption.

3. Research Methodology

This review aims to explore the growing role of Artificial Intelligence (AI) in the management of urban hydrological infrastructure. The review was achieved using a qualitative approach, which allows for an in-depth understanding of the subject through detailed secondary data analysis. According to Byrd (2020), qualitative research is a method designed to explore and understand phenomena within their natural context. As part of the qualitative approach, this study employed a systematic literature review to ensure a deep understanding of the existing body of knowledge. Systematic literature reviews align with the principles of qualitative research by enabling a structured and transparent process for synthesizing information from diverse sources (Rathnayaka *et al.,* 2022). Some steps involved in conducting a systematic literature review include identifying, selecting, evaluating, and synthesizing relevant research from academic databases, journals, conference proceedings, and other scholarly sources. This process typically begins with formulating clear research questions or objectives, followed by developing a detailed search strategy to locate relevant studies. To ensure transparency and reproducibility, these reviews adhere to a structured approach guided by predefined criteria and protocols for screening, inclusion, exclusion, and data extraction. Finally, the synthesized findings are analyzed and reported in a manner that provides insights into the research topic. A quantitative approach was also employed to strengthen the study and provide a broader perspective. The quantitative analysis was achieved via a bibliometric analysis method, which systematically evaluates the scholarly literature using quantitative metrics to analyze trends, patterns, and networks within the research field (Sajovic and Boh Podgornik, 2022).

VOSviewer software is a widely recognized tool for visualizing and analyzing bibliographic data. According to Zhao *et al.,* (2021), and was thus adopted in this study. The search strategy focused on identifying relevant studies by targeting titles, abstracts, and keywords to ensure a holistic capture of relevant literature. The final search string employed was (TITLE-ABS-KEY) (“urban hydrology” OR “artificial intelligence” OR “machine learning” OR “water management” OR “extreme events” OR “flood prediction”) AND (PUBYEAR > 2010 AND PUBYEAR < 2024) AND (LIMIT-TO [SUBJAREA, “ENGI”, “ENV”, “COMP”, “AGRI”, “EART”, “SSCI”]) AND (LIMIT-TO [DOCTYPE, “j”] OR LIMIT-TO [DOCTYPE, “cp”]) AND (LIMIT-TO [LANGUAGE, “English”]). Subject areas included “ENGI”

(Engineering), "ENV" (Environmental Science), "COMP" (Computer Science), "AGRI" (Agricultural Science), "EART" (Earth and Planetary Sciences), and "SSCI" (Social Sciences). The Scopus database was assessed for this study due to its extensive coverage of peer-reviewed literature, multidisciplinary scope, and advanced tools for bibliometric analysis. Document types were restricted to journals (j) and conference proceedings (cp). The study considered publications from 2010 to 2024 to ensure the results reflected recent advancements. The search, conducted in late December 2024, resulted in bibliometric data downloaded in comma-separated values (CSV) format, yielding 2,098 documents.

4. Results and Discussion

4.1. Document Types and Distribution

The bibliometric analysis of the 2,098 documents revealed significant trends and patterns. These documents were classified into two primary categories: journal articles and conference papers. As illustrated in Figure 1, journal articles accounted for 71% of the total publications, while conference papers comprised the remaining 29%. This distribution highlights the prominence of peer-reviewed journal articles in advancing research within this field, although conference proceedings serve as a critical platform for disseminating emerging findings and fostering collaborations.

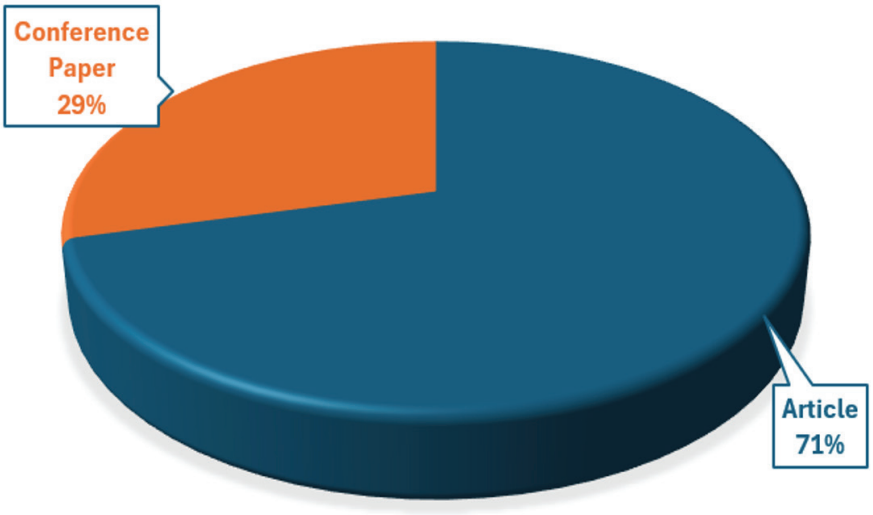


Figure 1: Documents by type

4.2. Analysis of Co-occurrence of Keywords

A co-occurrence map was created to analyze the frequency and relationships of keywords based on the bibliographic data collected for the study. These keywords were extracted from the titles, abstracts, and keyword sections of the articles reviewed. While VOSviewer typically uses a default ranging co-occurrence threshold of five keywords, various studies have adopted different thresholds, from two (Baier-Fuentes *et al.,* 2018) to as many as 40 (Saheb et al., 2019). For this study, a minimum threshold of four co-occurrences was selected to ensure a balance between obtaining widespread results and avoiding redundant keywords. The analysis revealed 8,485 keywords across 2,098 articles, with 565 keywords meeting the threshold of four co-occurrences. According to Van Eck and Waltman (2013), the proximity of keywords in the map indicates their frequency of co-occurrence, with larger nodes representing more frequently occurring keywords. The network visualization map in Figure 2 shows the five distinct clusters of co-occurring keywords related to

AI in urban hydrological infrastructure. The lines connecting the nodes reflect the strength of their relationships, with thicker lines representing stronger co-occurrence connections.

Cluster 1: AI in Flood Prediction and Early Warning Systems

The red cluster focuses on AI applications in flood prediction and early warning systems, a critical component of urban hydrological resilience. Key terms such as "floods," "forecasting," "streamflow," "runoff," and "numerical model" highlight AI's role in advancing predictive accuracy. Flood events are becoming more frequent and severe due to climate change, requiring innovative solutions to improve forecasting and minimize damage. AI techniques, including machine learning (ML) models like artificial neural networks (ANNs), support vector machines (SVMs), and decision trees, have been widely adopted for hydrological predictions. For instance, a study by Albahri *et al.,* (2024) employed ANNs to predict river discharge levels with unprecedented accuracy, enabling authorities to prepare for and respond to flooding effectively. Deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have further enhanced flood forecasting (Panahi *et al.,* 2021). These models can process large datasets, including historical rainfall patterns, real-time meteorological data, and topographical maps, to provide more reliable predictions. Research by Yang *et al. (2019) demonstrated that using RNNs in real-time streamflow forecasting significantly improves* the lead time for early warnings. Moreover, integrating AI with Internet of Things (IoT) devices such as water level sensors and weather stations allows for continuous data collection and analysis, enabling authorities to monitor conditions in real time. For example, the FloodAI project developed a system that combines IoT data with AI algorithms to provide real-time flood risk alerts, reducing response times and enhancing community preparedness (Abraham *et al.,* 2023).

Additionally, AI-driven simulations have enabled researchers to model complex hydrological interactions, such as rainfall-runoff processes and river flow dynamics (Albahri *et al.,* 2024). Studies like those by Yang *et al.,* (2019) also highlight how AI models outperform traditional hydrological models in handling nonlinear and chaotic water systems. This capability is crucial for urban areas where multiple variables, including impervious surfaces and aging infrastructure, exacerbate flood risks. By integrating predictive modeling with early warning systems, AI empowers urban planners and policymakers to implement proactive measures, such as evacuations, resource allocation, and structural adaptations. The red cluster, therefore, emphasizes the transformative potential of AI in mitigating flood impacts and safeguarding urban communities.

Cluster 2: AI in Urban Water Demand Forecasting

The green cluster represents AI's application in urban water demand forecasting, as highlighted by keywords like "water use," "decision support systems," and "resource management." Accurate forecasting is vital for sustainable water resource allocation in rapidly urbanizing regions. According to Shahin et al., (2024), traditional forecasting methods often fall short of accounting for the variability introduced by population growth, climate change, and urban development. Conversely, AI leverages advanced algorithms to analyze historical data and predict future water demand with relatively higher precision. For instance, Mu et al., (2020) utilized long short-term memory (LSTM) networks to forecast water demand in urban areas, demonstrating a significant reduction in prediction errors compared to conventional methods. Similarly, decision support systems (DSS) powered by AI have been implemented to optimize water supply networks. Research by Soori et al., (2024) showed how AI-enabled DSS could dynamically adjust water allocation to meet fluctuating demands, minimizing wastage and enhancing reliability. AI has also been applied to develop predictive maintenance strategies for water infrastructure, ensuring that leaks and inefficiencies are addressed before they escalate.

Furthermore, AI-based models are instrumental in scenario planning, allowing urban planners to simulate various demand scenarios under different conditions, such as droughts or rapid urbanization (Soori et al., 2024). Such advancements have practical implications for cities facing water scarcity. AI enhances the efficiency of water supply systems and supports sustainable development goals by helping promote equitable resource distribution. The green cluster highlights the indispensable role of AI in ensuring the long-term sustainability of water resources.

Cluster 3: AI in Real-Time Monitoring of Water Quality

The blue cluster emphasizes AI's role in real-time water quality monitoring, as evident from keywords such as "water quality," "wastewater treatment," and "water pollution." Ensuring the safety and quality of urban water supplies is a growing challenge, particularly in regions grappling with industrial pollution and aging infrastructure (Pokhrel et al., 2022). Thus, AI technologies have revolutionized water quality monitoring by enabling the rapid detection of contaminants and optimizing wastewater treatment processes. Machine learning algorithms have been widely applied to analyze sensor data and classify water pollutants. Zhu et al., (2022) demonstrated the use of support vector machines (SVMs) in identifying water contaminants with high accuracy. This approach reduces the reliance on labor-intensive and time-consuming laboratory tests, enabling faster decision-making. Deep learning models, such as CNNs, have also been employed to process remote sensing data for large-scale water quality assessment. AI-powered wastewater treatment systems have also been developed to optimize treatment processes. These systems adjust operational parameters, such as aeration rates and chemical dosages, based on real-time data, improving efficiency and reducing costs (Sakkaravarthy et al., 2024). For example, Aquaai Corporation, an AI-based platform based in California, leverages ML algorithms to monitor and manage wastewater treatment plants, ensuring compliance with regulatory standards (Reference). By integrating AI with IoT and cloud computing, real-time monitoring systems can provide actionable insights to utilities and regulators. This enables proactive interventions, such as issuing advisories or implementing stricter pollution controls. The blue cluster thus highlights AI's potential to enhance the safety, efficiency and sustainability of urban water systems.

Cluster 4: AI in Optimization of Stormwater Management Systems

The yellow cluster highlights AI's transformative potential in optimizing stormwater management systems, a critical aspect of mitigating urban flooding, reducing water pollution, and enhancing the resilience of drainage infrastructure. The presence of keywords such as "stormwater management," "optimization," "drainage infrastructure," and "urban flooding" underscores this focus. As urbanization and climate change increase the frequency and intensity of extreme weather events, effective stormwater management has become a top priority for cities worldwide (Panahi et al., 2021). AI offers innovative tools to optimize these systems, driving improvements in their efficiency, adaptability, and sustainability. One of the significant applications of AI in stormwater management is predictive modeling. AI algorithms such as ANNs, LSTM networks, and SVMs can analyze vast datasets, including historical rainfall patterns, land use maps, and soil permeability, to predict stormwater runoff peak discharge and volume (Yang et al., 2019). These models outperform traditional hydrological models in accuracy and computational efficiency. For instance, a study by Cea and Costabile (2022) demonstrated that AI-based systems could predict runoff more effectively under complex urban conditions, enabling planners to better design drainage systems that mitigate flood risks. Another critical use of AI is real-time monitoring and optimization of stormwater systems. Internet of Things (IoT) sensors embedded in stormwater infrastructure collect data on water flow, sediment levels, and equipment performance. AI algorithms process this data to detect anomalies, such as blockages or equipment failures, and recommend timely interventions. AI also contributes to sustainable stormwater management by optimizing the design and placement of green infrastructure (GI) solutions like rain gardens, bioswales, and permeable pavements (Sharifi

et al., 2024). Using geospatial data and hydrological models, AI tools identify optimal locations for GI installations, maximizing water infiltration and pollutant filtration while minimizing costs. Pokhrel et al., (2022) demonstrated how AI-driven planning tools increased the efficiency of GI projects, significantly reducing urban flooding and improving water quality.

Furthermore, AI enables cities to integrate long-term climate change scenarios into stormwater planning. Adaptive management strategies, supported by AI, can evaluate the impact of changing rainfall patterns and rising temperatures on stormwater systems and recommend infrastructure upgrades to maintain their effectiveness. For example, research by Labonnote (2024) showcased how AI could model climate change impacts, helping cities future-proof their stormwater management systems. Therefore, the yellow cluster underscores AI's versatile role in stormwater management, from predictive analytics and operational optimization to sustainability and public engagement.

Cluster 5: AI in Urban Flood Risk Assessment and Mapping

The purple cluster represents the application of AI in urban flood risk assessment and mapping, a crucial area of study for mitigating the impacts of urban flooding on infrastructure, communities and ecosystems. Centered on keywords like "risk assessment," "groundwater," and "mapping," this cluster emphasizes the role of AI in evaluating urban flood risks and generating detailed, data-driven maps to guide urban planning and disaster preparedness strategies. Flood risk assessment involves evaluating both hazard exposure and the vulnerabilities of urban areas. AI enables more accurate and dynamic assessments by analyzing extensive datasets, including topography, hydrology, rainfall patterns, land use, and socioeconomic indicators (Cea and Costabile, 2022). Machine learning algorithms, such as Random Forest (RF) and Gradient Boosting Machines (GBM), are particularly effective in identifying flood-prone areas. Studies like that of Neog et al., (2024) highlight how these algorithms outperform traditional statistical methods in flood risk classification, providing more granular insights into the factors driving urban flooding. Integrating remote sensing data is one key advancement AI brings to flood risk mapping. When coupled with AI, high-resolution satellite imagery and LiDAR data allow for the creation of precise flood maps.

Deep learning models like CNNs can analyze spatial data to detect features like riverbanks, floodplains, and impervious surfaces. For example, a study by Panahi et al., (2021) determined the use of CNNs to map flood extents with unparalleled accuracy, supporting emergency response and long-term planning. AI also enhances real-time flood monitoring and forecasting, which are essential risk mitigation components. AI algorithms can accurately predict flood events by processing data from IoT sensors, weather stations, and social media feeds. For instance, Samadi (2022) explored how AI-driven predictive systems integrated real-time hydrological data to issue timely warnings, reducing human and economic losses during urban flood events.

Additionally, AI facilitates the creation of dynamic flood vulnerability indices by incorporating socioeconomic data, such as population density, infrastructure resilience, and access to emergency services (Ye, 2021). This multidimensional approach helps urban planners prioritize interventions and allocate resources more effectively. Finally, research by Dixon et al., (2021) showcased how AI-based models identified high-risk zones, aiding in targeted urban flood mitigation strategies. Therefore, the purple cluster stresses the versatility and power of AI in transforming urban flood risk assessment and mapping.

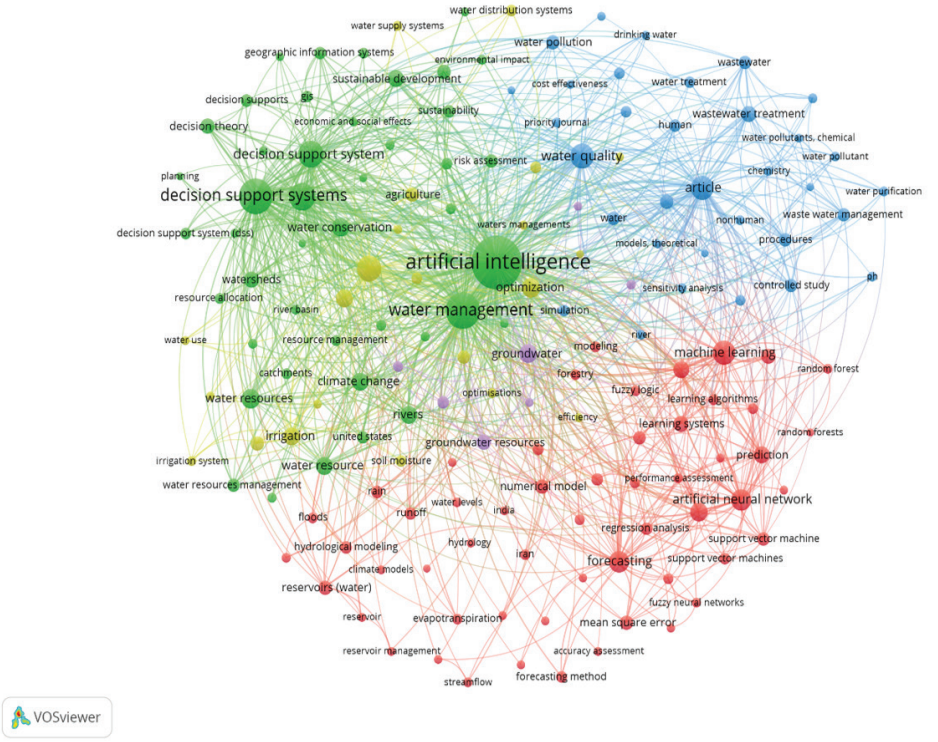


Figure 2: Overlay visualization map for co-occurring keywords

5. Practical Applicability of the Findings

This study's findings highlight AI's transformative potential in urban water and flood management systems, presenting significant opportunities for private industry professionals across various sectors, including construction, engineering, technology, and urban planning.

One of the key findings from this study is the critical role AI plays in flood prediction and early warning systems. The ability to predict floods with greater accuracy allows cities to take proactive measures, such as reinforcing vulnerable infrastructure, implementing flood barriers, or ensuring timely evacuations. For professionals, AI-based flood prediction models provide valuable data to inform infrastructure design, resource allocation, and adaptive strategies. The study emphasizes that by integrating AI with IoT devices, such as water level sensors and weather stations, real-time data collection can be significantly enhanced, leading to more effective flood management. Companies may consider leveraging these technologies to improve flood preparedness and response strategies. For example, AI-driven predictive flood models, like those used by NOAA and the FloodAI project, can be implemented by private sector organizations to improve flood risk management and reduce disaster-related losses. Also, engaging with local governments and utilities to promote the widespread adoption of these technologies could have far-reaching benefits in terms of cost savings and enhanced public safety.

Another important finding from the study is AI's potential to optimize water demand forecasting, a critical component of sustainable water management. AI-based forecasting models enable utilities and infrastructure sectors to allocate resources better, reduce waste, and improve operational efficiency. Therefore, private industry professionals in water utilities and infrastructure may prioritize the integration of AI into water demand forecasting processes, enabling them to create smart water management systems that can dynamically adjust water distribution based on real-time demand forecasts, ultimately improving sustainability and reducing costs. Additionally, they may

consider collaborating with AI technology providers to develop tailored solutions that meet the specific needs of their water systems. Companies that adopt AI-driven water demand forecasting will be better positioned to address future challenges related to population growth, climate change, and urbanization.

The study also highlights the value of AI in real-time water quality monitoring, a crucial application for ensuring safe and clean water supplies. The ability to monitor water quality in real time allows for the rapid detection of contaminants, thereby improving regulatory compliance and reducing the reliance on traditional, time-consuming laboratory tests. AI-powered systems can detect pollutants and optimize water treatment processes, ensuring water quality remains within safe limits. Companies like Aquaai and IBM's Green Horizons are already using AI for water quality monitoring, demonstrating the potential benefits of these systems for water utilities and industrial sectors. Therefore, private sector professionals involved in water utilities and environmental monitoring should prioritize the implementation of AI-driven water quality monitoring technologies to ensure better water safety and efficiency. By implementing AI systems, these companies can improve the speed and accuracy of water quality assessments and treatment adjustments, ultimately leading to more efficient and sustainable water management practices.

In addition, the study emphasizes the role of AI in optimizing stormwater management systems. As urbanization and extreme weather events increase, the risk of urban flooding becomes more pressing, making efficient stormwater infrastructure essential. AI models, such as ANNs LSTM networks, can process vast amounts of environmental data to predict stormwater runoff and optimize drainage system performance. Cities like Philadelphia and Seattle have already demonstrated the effectiveness of AI in stormwater management, and private companies can learn from these examples to improve their stormwater systems. Based on the study's findings, a recommendation is for private sector professionals to adopt AI technologies for stormwater management. By doing so, they can optimize drainage systems and integrate green infrastructure solutions, which are increasingly recognized for their effectiveness in managing stormwater and improving urban resilience to climate change. Companies should also consider investing in AI-driven models to forecast runoff and optimize stormwater systems, ensuring that urban areas are better equipped to handle extreme weather events.

Finally, the study highlights AI's value in urban flood risk assessment and mapping. AI models can process large datasets from remote sensing technologies, such as satellite imagery and LiDAR, to create highly accurate and detailed flood risk maps. These maps are essential for identifying flood-prone areas, prioritizing mitigation efforts, and designing flood-resistant infrastructure. Private industry professionals in urban planning and infrastructure design can benefit from AI-based flood risk assessment tools by using them to improve resource allocation and inform flood mitigation strategies. Collaborating with governmental agencies to enhance the accuracy of flood hazard maps can also improve disaster preparedness efforts and contribute to more sustainable urban development.

6. Conclusions and Areas of Future Studies

The integration of AI into urban hydrological infrastructure has gained significant traction over the past decade, driven by the increasing demand for smarter and more efficient water management systems in cities. With the growing challenges of climate change, rapid urbanization, and water scarcity, there is an urgent need for innovative solutions that can optimize water resource use, reduce flooding risks, and ensure the safety and sustainability of urban environments. AI, with its ability to analyze large datasets, make accurate predictions, and automate decision-making processes, offers tremendous potential to address complex challenges in urban water management. A systematic review approach, supported by bibliometric studies, revealed 2,098 documents

from 2010 to date on AI's role in urban water management, underscoring the growing interest and potential for innovation in this field. These studies highlight the transformative impact AI could have in enhancing the efficiency and resilience of urban water systems. Overall, this study uncovered that five clusters of AI applications have emerged within this domain. These include AI in flood prediction and early warning systems, AI in urban water demand forecasting, AI in real-time monitoring of water quality, AI in optimization of stormwater management systems, and AI in urban flood risk assessment and mapping. These clusters represent key areas where AI is making a significant impact, contributing to more sustainable, responsive, and resilient urban water management practices.

Practically, these insights provide valuable direction for industry professionals and policymakers aiming to integrate AI into urban hydrological infrastructure. The emergence of AI in flood prediction, water demand forecasting, stormwater management, water quality monitoring, and flood risk assessment indicates a clear shift toward more data-driven, efficient, and proactive approaches in managing urban water systems. These findings suggest that AI can play a pivotal role in enhancing decision-making processes, reducing operational risks, and improving resource allocation within these sectors. For urban planners, engineers, and other stakeholders, the application of AI offers an opportunity to modernize existing infrastructure, making it more resilient to the growing challenges posed by climate change and urbanization. Furthermore, AI's potential for optimizing resource use, improving sustainability, and mitigating flood risks can help cities better prepare for extreme weather events while ensuring the continued provision of essential water services. As AI technology continues to evolve, future studies should focus on refining these AI applications, enhancing their integration with other technologies such as IoT and big data analytics, and evaluating their long-term impact on urban resilience. Moreover, there is a need for collaboration between academia, industry, and government agencies to ensure the widespread adoption and effective implementation of these technologies, which will ultimately contribute to more sustainable and adaptive urban water management systems.

Despite the contributions of this study, several limitations must be acknowledged. First, the reliance on bibliometric data, while comprehensive, may not capture the full spectrum of AI applications in urban hydrological infrastructure, particularly those emerging in newer or less-publicized studies. The documents analyzed may also reflect a concentration of research in specific regions or institutions, potentially overlooking advancements in AI applications from other areas or industries. Future studies might want to empirically investigate AI applications through case studies, field experiments, or surveys to provide a deeper understanding of the global adoption and deployment of these technologies. Additionally, while the study focuses on the major clusters of AI applications, it does not explore in-depth the specific challenges or barriers faced by professionals when attempting to implement these technologies in real-world urban settings. Factors such as cost, data privacy concerns, and the need for specialized expertise may hinder the widespread adoption of AI but were not extensively examined in this review. Future research could consider examining case studies or conducting interviews with industry professionals to identify these practical challenges and provide more context to the findings.

Declaration of Competing Interest

The author declares that I have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abera, L.E., 2022. Determining Implementation Barriers for Green Stormwater Infrastructure (GSI) Practices for Urban Flood Control (Doctoral dissertation, The University of Mississippi).

Abraham, S.T. and Thazhathethil, B.V., 2023. Tourism Disaster Management through Chatbots as an Alternative Tool of Communication. Revista Turismo & Desenvolvimento (RT&D)/Journal of Tourism & Development, (41). https://doi.org/10.34624/rtd.v41i0.30195

Aghimien, D., Aliu, J., Chan, D.W., Aigbavboa, C. and Awuzie, B., 2024. Making a case for nature- based solutions for a sustainable built environment in Africa. Sustainable Development. https://doi.org/10.1002/sd.2935

Albahri, A.S., Khaleel, Y.L., Habeeb, M.A., Ismael, R.D., Hameed, Q.A., Deveci, M., Homod, R.Z., Albahri, O.S., Alamoodi, A.H. and Alzubaidi, L., 2024. A systematic review of trustworthy artificial intelligence applications in natural disasters. Computers and Electrical Engineering, 118, p.109409. https://doi.org/10.1016/j.compeleceng.2024.109409

Baier Fuentes, H., Cascón Katchadourian, J., Martínez Sánchez, M.Á. and Herrera Viedma, E., 2018. A bibliometric overview of the international journal of interactive multimedia and artificial intelligence. DOI: 10.9781/ijimai.2018.12.003

Byrd, R., 2020. Qualitative research methods. *Virtual Class, Memphis. Recuperado em*, *17*. https://www.memphis.edu/jrsm/syllabi/syllabi_pages/syllabi_pdfs/2020_fall/jrsm7085.001.m50.byrd.fall2020.pdf

Cea, L. and Costabile, P., 2022. Flood risk in urban areas: Modelling, management and adaptation to climate change. A review. Hydrology, 9(3), p.50. https://doi.org/10.3390/hydrology9030050

Dixon, B., Johns, R. and Fernandez, A., 2021. The role of crowdsourced data, participatory decision-making and mapping of flood related events. Applied Geography, 128, p.102393. https://doi.org/10.1016/j.apgeog.2021.102393

Ebekozien, A., Aigbavboa, C., Samsurijan, M.S., Radin Firdaus, R.B. and Salman, A., 2024. Appraising flood resilience technologies role in developing cities: how prepared is the professional stakeholder?. International Journal of Construction Management, 24(7), pp.683-692. https://doi.org/10.1080/15623599.2023.2203501

Ferreira, C.S., Duarte, A.C., Kasanin-Grubin, M., Kapovic-Solomun, M. and Kalantari, Z., 2022. Hydrological challenges in urban areas. In Advances in Chemical Pollution, Environmental Management and Protection (Vol. 8, No. 1, pp. 47-67). Elsevier. https://doi.org/10.1016/bs.apmp.2022.09.001

Fletcher, T.D., Burns, M.J., Russell, K.L., Hamel, P., Duchesne, S., Cherqui, F. and Roy, A.H., 2024. Concepts and evolution of urban hydrology. Nature Reviews Earth & Environment, pp.1-13. https://doi.org/10.1038/s43017-024-00599-x

Haider, S., Rashid, M., Tariq, M.A.U.R. and Nadeem, A., 2024. The role of artificial intelligence (AI) and Chatgpt in water resources, including its potential benefits and associated challenges. *Discover Water*, *4*(1), p.113. https://doi.org/10.1007/s43832-024-00173-y

Labonnote, N., 2024. AI-driven sustainable cities: A Nordic-inspired requirement framework. In SHS Web of Conferences (Vol. 198, p. 03001). EDP Sciences. https://doi.org/10.1051/shsconf/202419803001

Maisonobe, M., 2022. The future of urban models in the Big Data and AI era: a bibliometric analysis (2000–2019). AI & society, pp.1-18. https://doi.org/10.1007/s00146-021-01166-4

Mu, L., Zheng, F., Tao, R., Zhang, Q. and Kapelan, Z., 2020. Hourly and daily urban water demand predictions using a long short-term memory based model. Journal of Water Resources Planning and Management, 146(9), p.05020017. https://doi.org/10.1061/(ASCE)WR.1943-5452.0001276

Neog, D.R., Singha, G., Dev, S. and Prince, E.H., 2024. Artificial Intelligence and Its Application in Disaster Risk Reduction in the Agriculture Sector. In Disaster Risk Reduction and Rural Resilience: With a Focus on Agriculture, Water, Gender and Technology (pp. 279-305). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-6671-0_15

Otto, F.E., Zachariah, M., Saeed, F., Siddiqi, A., Kamil, S., Mushtaq, H., Arulalan, T., AchutaRao, K., Chaithra, S.T., Barnes, C. and Philip, S., 2023. Climate change increased extreme monsoon rainfall, flooding highly vulnerable communities in Pakistan. Environmental Research: Climate, 2(2), p.025001. https://doi.org/10.10.1088/2752-5295/acbfd5

Panahi, M., Jaafari, A., Shirzadi, A., Shahabi, H., Rahmati, O., Omidvar, E., Lee, S. and Bui, D.T., 2021. Deep learning neural networks for spatially explicit prediction of flash flood probability. Geoscience Frontiers, 12(3), p.101076. https://doi.org/10.1016/j.gsf.2020.09.007

Pokhrel, S.R., Chhipi-Shrestha, G., Hewage, K. and Sadiq, R., 2022. Sustainable, resilient, and reliable urban water systems: Making the case for a “one water” approach. Environmental Reviews, 30(1), pp.10-29. https://doi.org/10.1139/er-2020-0090

Rathnayaka, B., Siriwardana, C., Robert, D., Amaratunga, D., & Setunge, S. (2022). Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. *International Journal of Disaster Risk Reduction*, *78*, 103123. https://doi.org/10.1016/j.ijdrr.2022.103123

Saheb, T. and Saheb, M., 2019. Analyzing and visualizing knowledge structures of health informatics from 1974 to 2018: a bibliometric and social network analysis. *Healthcare informatics research*, *25*(2), pp.61-72. DOI: https://doi.org/10.4258/hir.2019.25.2.61

Sajovic, I., & Boh Podgornik, B. (2022). Bibliometric analysis of visualizations in computer graphics: a study. *Sage Open*, *12*(1), 21582440211071105. https://doi.org/10.1177/2158244021107110

Sakkaravarthy, S., Jano, N.A. and Vijayakumar, A., 2024. Overcoming Challenges in Traditional Wastewater Treatment Through AI-Driven Innovation. In The AI Cleanse: Transforming Wastewater Treatment Through Artificial Intelligence: Harnessing Data-Driven Solutions (pp. 53-81). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-67237-8_3

Samadi, S., 2022. The convergence of AI, IoT, and big data for advancing flood analytics research. Frontiers in Water, 4, p.786040.

Shahin, M., Chen, F.F., Maghanaki, M., Firouzranjbar, S. and Hosseinzadeh, A., 2024. Evaluating the fidelity of statistical forecasting and predictive intelligence by utilizing a stochastic dataset. The International Journal of Advanced Manufacturing Technology, pp.1-31. https://doi.org/10.1007/s00170-024-14505-8

Sharifi, A., Beris, A.T., Javidi, A.S., Nouri, M.S., Lonbar, A.G. and Ahmadi, M., 2024. Application of artificial intelligence in digital twin models for stormwater infrastructure systems in smart cities. Advanced Engineering Informatics, 61, p.102485. https://doi.org/10.1016/j.aei.2024.102485

Soori, M., Jough, F.K.G., Dastres, R. and Arezoo, B., 2024. AI-Based Decision Support Systems in Industry 4.0, A Review. Journal of Economy and Technology. https://doi.org/10.1016/j.ject.2024.08.005

Van Eck NJ, Waltman L. 2013. VOSviewer manual. Vol. 1. Leiden: Univeristeit Leiden; p. 1–53.

Yang, S., Yang, D., Chen, J. and Zhao, B., 2019. Real-time reservoir operation using recurrent neural networks and inflow forecast from a distributed hydrological model. Journal of Hydrology, 579, p.124229. https://doi.org/10.1016/j.jhydrol.2019.124229

Ye, X., Wang, S., Lu, Z., Song, Y. and Yu, S., 2021. Towards an AI-driven framework for multi-scale urban flood resilience planning and design. Computational Urban Science, 1, pp.1-12. https://doi.org/10.1007/s43762-021-00011-0

Zhao, F., Fashola, O. I., Olarewaju, T. I., & Onwumere, I. (2021). Smart city research: A holistic and state-of-the-art literature review. *Cities*, *119*, 103406. https://doi.org/10.1016/j.cities.2021.103406

Zhu, M., Wang, J., Yang, X., Zhang, Y., Zhang, L., Ren, H., Wu, B. and Ye, L., 2022. A review of the application of machine learning in water quality evaluation. Eco-Environment & Health, 1(2), pp.107-116. https://doi.org/10.1016/j.eehl.2022.06.001

Suggested citation: **Abera, L.** (2025). The growing role of artificial intelligence in tomorrow's urban hydrological infrastructure. *One Step Ahead*, *July 2025*, 15–28. The Sam Houston State University Institute for Homeland Security. OSF | The Growing Role of Artificial Intelligence in Tomorrow's Urban Hydrological Infrastructure

ASSESSING WORKFORCE TRAINING STRATEGIES IN CRITICAL INFRASTRUCTURE: INSIGHTS AND RECOMMENDATIONS

Oluponmile Olonilua
John Ogbeleakhu Aliu

Abstract

Critical infrastructure sectors face growing risks from evolving threats such as cybersecurity attacks, natural disasters and cascading disruptions. Frontline employees play a pivotal role in mitigating these risks and ensuring operational continuity. However, limited research exists on the adequacy of training strategies tailored to the needs of small and medium-sized enterprises (SMEs) within these sectors. This study addresses this gap by examining existing workforce training approaches and highlighting opportunities for SMEs to enhance workforce training. The research employed a systematic literature review to evaluate current workforce training strategies. Relevant academic journals, industry publications and government reports were identified using targeted search terms such as "workforce training," "critical infrastructure," "SMEs" and sector-specific phrases like "energy sector workforce training," "cybersecurity workforce training," and "resilience training for SMEs." Databases including Scopus, Web of Science, and Google Scholar served as primary sources. Six strategies were identified in this review: (1) traditional and core skills training, (2) technology integration and innovation training, (3) emerging threats and risk management training, (4) certification and regulatory compliance training, (5) partnerships with educational institutions and (6) simulation-based and virtual training. This study provides a unique perspective by focusing on the workforce training needs of SMEs within critical infrastructure sectors, an area often overlooked in broader industry discussions. By proposing tailored opportunities for SMEs, the research offers actionable insights that align with the resource constraints and operational challenges faced by smaller organizations.

Keywords: Critical infrastructure, Frontline employees, Resilience education, Risk mitigation, Scenario-based simulations, Training strategies, Workforce preparedness.

Oluponmile Olonilua, Professor, Emergency Management, Homeland Security and Public Administration, Department of Political Science and Public Administration, Barbara Jordan – Mickey Leland School of Public Affairs, Texas Southern University, Houston, Texas 77004. Email: Oluponmile.Olonilua@tsu.edu: ORCID: 0000-0001-5087-3000

John Ogbeleakhu Aliu, Clinical Assistant Professor, Engineering Education Transformations Institute, College of Engineering, University of Georgia, Athens, Georgia, USA; Email: john.o.aliu@gmail.com: ORCID: 0000-0001-5651-4009

1. Introduction

Critical infrastructure is defined by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) as the systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating effect on national security, the economy, public health, or safety (CISA,2022). This encompasses 16 critical infrastructure sectors, including Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials and Waste, Transportation Systems and Water and Wastewater Systems. According to Dawson *et al.,* (2021), these sectors are responsible for ensuring the daily functioning of society and maintaining the stability and security of the nation. The protection and resilience of critical infrastructure are therefore vital to safeguarding public health and the economy, as well as ensuring national security.

With the growing interdependencies across these sectors, the risks faced by critical infrastructure are also expanding. These risks include natural disasters, cybersecurity threats, terrorism and pandemics (Olonilua, 2022). As such, the workforce within these sectors is increasingly recognized as a key element in ensuring operational continuity and resilience during times of crisis. As Remington *et al.,* (2024) note, frontline employees are often the first responders to crises, whether they involve natural disasters, cyberattacks, or other disruptions. As such, they must be equipped with the skills and knowledge necessary to address and mitigate risks, maintain operations and protect public safety. For example, the 2021 Texas winter storm demonstrated the vulnerability of the state's energy infrastructure, with widespread power outages and water supply disruptions (Doss-Gollin *et al.,* 2021). The response to this disaster highlighted gaps in preparedness, particularly regarding workforce training in dealing with extreme weather events. Similarly, the rise in cyberattacks targeting critical infrastructure systems, such as the 2020 SolarWinds hack, underscores the need for workforce readiness to handle cybersecurity threats (Willett, 2023).

Despite the critical role played by frontline employees in ensuring the resilience of critical infrastructure, there are significant challenges related to workforce readiness and skill gaps. These challenges are especially pronounced in small to medium-sized enterprises (SMEs), which often face resource constraints and lack access to advanced training programs (Chuang, 2024). A major issue is the inadequacy of existing workforce training strategies, which often focus primarily on technical skills without addressing the broader needs of crisis management and decision-making under pressure (Cubrich *et al.,* 2022). According to Remington *et al.,* (2024), the evolving nature of threats, such as the increasing frequency and severity of cyberattacks and the impacts of climate change, has created an urgent need for more wide-ranging workforce training programs. For example, many employees in critical infrastructure sectors may be well-versed in routine tasks but may not be adequately trained to respond to large-scale emergencies or to handle complex, multi-faceted crises (Chuang, 2024). The skills gap can result in inefficiencies, slow response times, and, in the worst cases, failures to prevent or mitigate disasters.

Another challenge is the disparity in training resources between large corporations and SMEs. While large organizations can often invest in advanced training technologies, such as scenario-based simulations and virtual training platforms (Sanchez *et al.,* 2023), SMEs often struggle to access these resources. As a result, many frontline employees in smaller organizations are left with outdated or generic training that does not address the unique needs of their specific sector or region. For example, energy sector employees may have training focused on maintaining power lines but may not receive adequate education on responding to cyberattacks targeting the energy grid. Similarly, healthcare workers may be trained for routine procedures but lack crisis manage-

ment training for pandemics or large-scale natural disasters. These training gaps contribute to vulnerabilities in critical infrastructure systems, especially during emergencies.

Therefore, the main objective of this study is to explore the current workforce training strategies within critical infrastructure sectors, with a particular focus on SMEs. This study will focus on the energy, water, transportation and healthcare sectors, as these are among the most vital to public safety and the economy. The study will then propose actionable recommendations to enhance workforce training strategies for SMEs within these sectors. This study will not only contribute to academic knowledge but also offer actionable insights for policymakers, industry leaders and educational institutions to foster stronger collaborations and enhance the training capabilities of SMEs in these key sectors.

2. Related Work

Based on the authors' knowledge, a systematic literature review that examines workforce training strategies within critical infrastructure sectors, particularly focusing on SMEs, has not been conducted yet. While there have been numerous studies on the general importance of workforce training in critical infrastructure, the literature primarily addresses large organizations and does not fully explore the unique challenges faced by SMEs, which are often constrained by limited resources. Several studies have highlighted the significance of workforce preparedness in critical infrastructure sectors such as energy, water, transportation and healthcare. One significant body of research focuses on workforce training in the energy sector, particularly in response to the increasing complexity of the industry. Gurieiev *et al.,* (2020) examined the importance of continuous training for energy sector employees, emphasizing the need for ongoing education due to the rapid technological advancements and the growing sophistication of cybersecurity threats. With energy systems becoming increasingly interconnected and dependent on digital infrastructure (Jasiūnas *et al.,* 2021), traditional training programs are no longer sufficient. The authors argue for the implementation of dynamic, ongoing training models that equip employees with the latest skills and knowledge to address both technical challenges and cyber threats. Furthermore, they highlight the lack of training opportunities for SMEs in the energy sector, which are often overlooked in larger-scale initiatives, despite their critical role in ensuring the resilience of the energy supply chain (Jasiūnas *et al.,* 2021),

Similarly, Bekiaris and Loukea (2019) studied workforce training in the transportation sector, emphasizing the importance of safety protocols and emergency response training for frontline workers. Their research underscores the role of specialized training programs in mitigating the risks associated with transportation accidents and ensuring quick, effective responses in emergencies. The authors discuss the complexity of training programs designed for the transportation workforce, noting that training methods such as simulation-based learning and scenario exercises are highly effective in enhancing employee preparedness (Bekiaris and Loukea, 2019). However, they also point out that SMEs within the transportation sector face significant hurdles in providing such advanced training methods, primarily due to financial and resource constraints. This gap in training availability and access to state-of-the-art learning technologies presents a challenge for smaller organizations attempting to maintain workforce readiness (Ambra *et al.,* 2019). The concept of resilience and its integration into workforce training is another area where substantial research has been conducted. Heath *et al.,* (2020) explored resilience education, specifically how training programs can improve both technical skills and decision-making abilities of employees during crises. Their work highlights the importance of training programs that go beyond conventional skills development and focus on equipping workers with the cognitive tools needed to manage high-stress, high-risk situations. This approach, known as resilience education, has been shown to improve operational continuity during disruptions (Heath *et al.,* 2020). Although their study

emphasizes the role of resilience in large organizations, the authors also acknowledge that SMEs could benefit from resilience-based training, especially as they often operate under heightened pressure during emergencies. However, the resource limitations of SMEs make it difficult for them to implement these advanced training methodologies effectively.

3. Research Methodology

This study adopted an eight-step approach for literature review based on the framework proposed by Okoli and Schabram (2015). The process was systematically structured to ensure that relevant studies were identified, assessed and synthesized. The eight steps are listed below and discussed further:

1. Defining the objective of the review
2. Protocol development
3. Conducting a comprehensive literature search
4. Screening for relevance
5. Assessing the quality of the selected studies
6. Extracting data from the studies
7. Synthesizing the findings from the studies
8. Writing the review

3.1. Defining the Objective of the Review

The primary aim of this literature review is to examine the current workforce training strategies within critical infrastructure sectors, with a specific focus on SMEs. These sectors (energy, water, transportation and healthcare) are integral to public safety and the economy, making workforce preparedness crucial. The following points describe the specific objectives of this study:

- To explore the existing workforce training strategies within critical infrastructure sectors (energy, water, transportation and healthcare) with a focus on SMEs.
- To propose actionable recommendations to enhance workforce training strategies for SMEs in these sectors.
- To contribute to both academic knowledge and practical solutions to strengthen the workforce in critical sectors.

3.2. Protocol Development

This step involves developing a review protocol that aligns with the study's objectives. Okoli and Schabram's (2015) approach was selected due to its systematic and structured methodology, which ensures a consistent and transparent process for conducting a literature review. The protocol for this study outlines key aspects such as the inclusion and exclusion criteria, specific focus areas (e.g., SMEs within critical infrastructure sectors like energy, water, transportation and healthcare) and the methodologies for evaluating relevant studies. By clearly defining the boundaries of the review, the protocol ensures that only studies directly related to workforce training strategies in SMEs are included, providing a focused and relevant body of literature for analysis.

3.3. Conducting a Comprehensive Literature Search

The search covered a wide range of databases, including Scopus, Web of Science, Google Scholar, IEEE Xplore, ScienceDirect, JSTOR, PubMed, SpringerLink, ProQuest and Emerald Insight. These databases were chosen for their broad coverage of relevant topics such as energy, transportation,

healthcare and workforce training. A combination of keywords was used to ensure comprehensive coverage of the topic, including terms like “workforce training,” “critical infrastructure,” “SMEs” and sector-specific phrases like “energy sector workforce training,” “cybersecurity workforce training,” and “resilience training for SMEs.” The search string used was: (“workforce training” AND “critical infrastructure” AND “SMEs” AND (“energy” OR “transportation” OR “healthcare” OR “water”) AND (“cybersecurity” OR “disaster preparedness” OR “resilience”)). This search resulted in 875 articles. After screening for relevance based on inclusion and exclusion criteria, and removing duplicates, 127 articles remained for further review. Non-relevant articles, including those that did not directly address SMEs or workforce training in critical infrastructure sectors, were omitted.

3.4. Screening for Relevance

In this step, the identified articles were screened for relevance based on specific inclusion and exclusion criteria that aligned with the study’s objectives. The inclusion and exclusion criteria are outlined below:

Inclusion criteria:

1. Only peer-reviewed articles published in reputable journals or conferences were considered.
2. Studies that specifically addressed workforce training strategies within critical infrastructure sectors, particularly for SMEs.
3. Articles that discussed issues such as cybersecurity, disaster preparedness, resilience, or other emerging threats pertinent to the energy, water, transportation, or healthcare sectors.
4. Preference was given to studies providing practical insights or case studies on training programs for SMEs within these sectors.

Exclusion criteria:

1. Studies that did not specifically address workforce training or focused solely on large organizations without relevance to SMEs.
2. Articles that lacked empirical data or presented only theoretical models without practical applications.
3. Studies published before 2010, as they may not reflect current practices and challenges.
4. Non-English language articles were excluded due to language proficiency limitations.

This screening process resulted in narrowing down the initial 127 articles to 84 articles that met the inclusion criteria. These 84 articles were then analyzed in detail to extract data that could contribute to the study’s understanding of workforce training strategies in critical infrastructure sectors, with a specific focus on SMEs.

3.5. Assessing the Quality of the Selected Studies

In this step, the quality of the selected studies was carefully assessed to ensure that the findings were credible and relevant to the research objectives. The assessment aimed to determine the reliability, validity and methodological rigor of the studies included in the review. To achieve this, a set of predefined criteria was applied to evaluate each study’s methodological approach, data collection methods, analysis techniques and overall contribution to the understanding of workforce training strategies within critical infrastructure sectors, particularly focusing on SMEs. The quality assessment process involved examining several key factors. First, the methodological

rigor was evaluated, considering whether the studies employed appropriate research designs such as case studies, surveys, or experiments. Studies with clear and well-structured methodologies were given higher weight. Second, the sampling strategy used in the studies was assessed. Studies that included diverse samples from SMEs within the critical infrastructure sectors were preferred, as these would provide a broader understanding of workforce training strategies across different contexts. Third, the clarity and transparency of data collection and analysis processes were examined, ensuring that the studies provided sufficient detail on how data was gathered, analyzed, and interpreted. Additionally, the relevance of the findings to the research objectives was critically evaluated. Studies that directly addressed the challenges SMEs face in workforce training, such as resource constraints or sector-specific threats, were prioritized. Peer-reviewed articles published in reputable journals were considered more reliable than conference papers or grey literature. The quality assessment process resulted in retaining 42 studies that met the high standards for inclusion, ensuring that the literature used in the review was of sufficient quality to support the study's objectives.

3.6. Extracting Data from the Studies

In this step, relevant data was systematically extracted from the selected studies to address the research objectives, focusing on workforce training strategies within critical infrastructure sectors, particularly for SMEs. The data extraction process involved identifying key information such as study characteristics (e.g., author, year, sector), training methods used, challenges faced by SMEs, and the effectiveness of the training programs. To ensure consistency, a standardized data extraction form was developed and organized into a table with eight columns, each representing key attributes necessary to summarize and assess the relevance of the studies. These attributes included details like training strategies, challenges, outcomes and gaps in workforce preparedness. This structured approach facilitated the comparison of findings across sectors and enabled the synthesis of the evidence.

3.7. Synthesis of Studies

In the synthesis of studies, the extracted data was analyzed and combined to address the research objectives, highlighting patterns, trends and insights related to workforce training. The synthesis process involved grouping the studies based on common themes, such as training methods, challenges faced by SMEs and the effectiveness of training programs in enhancing workforce preparedness. Comparative analysis was conducted across the five sectors to identify similarities and differences in workforce training approaches. The findings were synthesized to provide a holistic understanding of the existing strategies and their relevance to SMEs, ultimately informing the study's recommendations for improving workforce training in critical infrastructure sectors. This synthesis allowed for a clearer picture of how training programs can be optimized, especially within resource-constrained environments like SMEs.

3.8. Writing the Review

The process of writing this systematic literature review was conducted in line with the established guidelines for writing research articles, following the methodology outlined by Okoli and Schabram (2015). After the initial search, a total of 875 articles were retrieved using the combination of keywords indicated in Section 3.3. This large number of results was partly due to the absence of effective filters in many of the database search engines based on the previously defined inclusion and exclusion criteria. After two rounds of practical screening, in which articles that did not meet the requirements outlined in Section 3.4 were removed, the selection was reduced to 127 articles. These articles were then further manually reviewed to ensure their relevance to the subject of the review. The manual screening involved eliminating articles that did not reference the key themes

or keywords mentioned in Section 3.3. Simultaneously, articles that did not meet the second rule of the quality appraisal discussed in Section 3.5 were also excluded. Following the quality appraisal process, the final selection consisted of 84 articles that contributed to the literature review, with an additional 42 studies being incorporated into the related work section.

4. Results and Discussion

4.1. Existing Workforce Training Strategies Within Critical Infrastructure Sectors

4.1.1. Traditional and Core Skills Training

Traditional and core skills training remain fundamental in ensuring the proper operation and safety of critical infrastructure systems. In the water sector, training often focuses on the foundational knowledge required for water treatment and distribution. For instance, large utilities such as the Los Angeles Department of Water and Power (LADWP) provide in-depth training on water purification, reservoir management and pipeline maintenance (LADWP, 2024). During these trainings, workers are taught hands-on how to handle critical equipment such as water treatment plants and chemical dosing systems. In the transportation sector, training often revolves around vehicle operation, safety protocols and regulatory compliance. One example is FedEx, which runs a comprehensive training program for its drivers to ensure they understand safety standards, regulatory requirements and customer service. Similarly, in the healthcare sector, traditional certifications such as Basic Life Support (BLS) and Advanced Cardiac Life Support (ACLS) ensure that healthcare professionals possess the core skills necessary to perform emergency medical procedures. For example, Mayo Clinic requires all medical personnel to undergo ACLS and BLS training regularly to maintain readiness in emergency situations (Mayo Clinic, 2021).

For SMEs, traditional and core skills training often takes a more focused approach, depending on the specific needs of the business. According to Perez *et al.,* (2016), smaller enterprises may not have the resources for extensive in-house training programs, so they often rely on third-party training providers or certification programs. In the water sector, for instance, small water utilities may not have the budget for large-scale training, so they often turn to American Water Works Association (AWWA) certification programs, which provide essential skills in water quality management, wastewater treatment and system maintenance (Olson, 2020). In healthcare SMEs, such as small clinics, the staff often relies on third-party certification courses like Basic Life Support (BLS) and Advanced Cardiovascular Life Support (ACLS) provided by the American Heart Association (AHA), ensuring they meet regulatory requirements and can respond to emergencies.

4.1.2. Technology Integration and Innovation Training

With rapid technological advancements, critical infrastructure sectors are evolving by integrating innovative tools and systems. In the water sector, technologies such as smart meters, automated leak detection and remote monitoring systems are revolutionizing utility operations. For instance, the City of Atlanta recently announced plans to utilize artificial intelligence (AI) to manage its aging water infrastructure. This decision comes in response to two significant water main breaks earlier this year. To prevent future incidents, AI-enhanced devices are being installed on water line valves at the affected locations. These devices will provide early warnings, allowing for proactive maintenance and more efficient infrastructure management (Smart Water, 2024). Atlanta's Smart Water Management System also incorporates automated leak detection sensors and real-time water quality monitoring. This technology enables the city to optimize water resource management, minimize losses, and ensure a safe, high-quality water supply. Mayor Andre Dickens highlighted these improvements as a critical step in modernizing the city's water infrastructure (Smart Water, 2024). In the transportation sector, the introduction of autonomous vehicles and AI-powered logistics

platforms has driven companies to train their workforce in new technologies. For instance, Tesla provides training for its technicians on electric vehicle (EV) systems, battery technologies and software updates (Dreher *et al.,* 2024). In the healthcare sector, the adoption of technologies like robotic-assisted surgeries and telemedicine demands that healthcare workers constantly upskill. For example, Cleveland Clinic has developed training programs for surgeons to learn how to operate robotic systems for minimally invasive surgeries, allowing for greater precision and faster recovery times (Cleveland Clinic, 2023).

SMEs are also pushing to leverage these new technologies but often face challenges due to limited resources. According to Bradač Hojnik and Huđek (2023), smaller organizations often make use of affordable digital tools, training platforms and collaborations with larger institutions. In the water sector, small utilities are beginning to adopt smart metering systems and remote monitoring tools. For example, small municipal systems often partner with larger firms or universities to integrate IoT-based water management systems that help track consumption and detect leaks. For training, SMEs regularly rely on online platforms like Coursera or Udemy to educate employees about new tools and technology (Pawar and Lal, 2022). Similarly, smaller transportation companies also integrate telematics systems to monitor vehicle performance but may outsource training on these systems to third-party providers that specialize in fleet management technologies (Dudin *et al.,* 2019). In healthcare, small clinics and private practices adopt technologies like telemedicine platforms but often need affordable and efficient training solutions, which could be obtained through partnerships with larger healthcare providers or certification bodies like the American Telemedicine Association (ATA).

4.1.3. Emerging Threats and Risk Management Training

Emerging threats, particularly cyberattacks and environmental crises, are reshaping the need for risk management training within critical infrastructure sectors. In the water sector, cyberattacks targeting water systems are a growing concern. For instance, a 2021 cyberattack on the Oldsmar, Florida water treatment facility highlighted the vulnerabilities of water utilities to cyber threats (Cervini *et al.,* 2022). In response, the American Water Works Association (AWWA) launched cybersecurity awareness programs aimed at water sector employees to prevent similar breaches. In the transportation sector, emerging risks related to autonomous vehicles and connected infrastructure require specialized cybersecurity training. For example, General Motors and Waymo have begun training their engineers to secure communication between self-driving cars and transportation networks (Chai, 2020). Additionally, airlines like Delta invest in risk management programs for pilots and crew to respond to unexpected challenges such as extreme weather conditions or system failures. In the healthcare sector, cybersecurity threats are also a growing concern. The Universal Health Services (UHS) ransomware attack in 2020 disrupted hospital operations which resulted in reported total pre-tax losses of an estimated $67 million, highlighting the need for cybersecurity training (UHS, 2020). In response, the National Cybersecurity Center of Excellence (NCCoE) has collaborated with healthcare institutions to offer training in secure patient data handling and digital infrastructure protection.

SMEs are also vulnerable to cybersecurity and environmental threats due to limited resources. In the water sector, for example, small water utilities often do not have the in-house expertise to address cybersecurity risks, so they often rely on national training programs or partnerships with cybersecurity firms to ensure they protect their systems. The Cybersecurity and Infrastructure Security Agency (CISA) offers resources specifically geared toward smaller utilities to mitigate cybersecurity threats (CISA,2022). Similarly, in the transportation sector, smaller companies often lack the cybersecurity budgets to create comprehensive protection protocols, so they utilize external providers for cybersecurity training, including platforms like CISA. In healthcare, smaller practices or hospitals may also be targets for cyberattacks due to inadequate security systems.

Following the 2020 Universal Health Services (UHS) attack, many small healthcare providers began looking for cost-effective ways to ensure their staff is trained in cyber hygiene and secure patient data management, with programs offered through entities like Health Information Trust Alliance (HITRUST) or the National Institute of Standards and Technology (NIST) (Sahid, 2024).

4.1.4. Certification and Regulatory Compliance Training

Certification and regulatory compliance are critical to maintaining standards and meeting legal requirements in critical infrastructure sectors. In the water sector, certifications from organizations like the Water Environment Federation (WEF) are essential for ensuring that employees are up to date on the latest environmental standards and operational procedures (Wahl, 2019). For example, the City of New York's Department of Environmental Protection (DEP) requires its employees to hold certifications in water treatment, distribution and wastewater management. In the transportation sector, regulatory compliance training is essential for ensuring vehicle safety and operational standards. For instance, in the aviation industry, the Federal Aviation Administration (FAA) mandates regular certification for pilots, air traffic controllers and maintenance technicians. Also, Delta Airlines has comprehensive training programs that include safety regulations, emergency response procedures and regulatory updates from the FAA (Gonczy, 2015). In the healthcare sector, regulatory training ensures that healthcare providers comply with both local and international healthcare standards. The Joint Commission regularly audits hospitals, and as part of compliance, staff undergo training on best practices, such as infection control and patient safety procedures. The American Heart Association (AHA) offers certification programs that are required for healthcare professionals working in emergency medical services (EMS), including paramedics and emergency room staff (AHA, 2022).

For SMEs, maintaining regulatory compliance is crucial, yet often challenging due to limited resources. However, many third-party certification programs cater to SMEs' needs in critical infrastructure sectors. In the water sector, small utilities typically rely on industry-standard certification programs from the AWWA or State Health Departments, which ensure their employees meet the legal requirements for water treatment and public health (Olson, 2020). In transportation, compliance training is a key part of SME workforce preparation, especially for small logistics companies or delivery services. Programs from organizations like the Federal Motor Carrier Safety Administration (FMCSA) or OSHA are often utilized to train drivers and operational staff in essential regulatory standards such as driver hours-of-service rules and transportation of hazardous materials (Driving, 2020). In healthcare, small clinics and independent practices often focus on certifications for infection control, HIPAA compliance and OSHA regulations to ensure they meet legal standards and industry practices. The American Medical Association (AMA) and Centers for Medicare & Medicaid Services (CMS) provide resources that allow SMEs to comply with federal healthcare regulations while keeping their workforce well-trained (Rondinelli *et al.,* 2023).

4.1.5. Partnerships with Educational Institutions

Collaborations with academic institutions provide critical infrastructure sectors with advanced training programs and innovative research. In the water sector, partnerships with universities enable utilities to stay ahead in water management technologies. For example, The University of California, Berkeley has collaborated with Pacific Gas and Electric (PG&E) to develop training programs focused on sustainable water use and energy efficiency (University of California, 2024). Additionally, in the transportation sector, universities like the Massachusetts Institute of Technology (MIT) have worked with companies like Ford Motor Company and General Motors to advance the development of autonomous vehicle technologies. These partnerships involve research-driven training on AI, machine learning and system integration. In the healthcare sector, hospitals and universities partner to offer specialized programs on the latest medical technologies.

For example, the Mayo Clinic partners with the University of Minnesota to provide specialized training in areas such as robotic surgeries, telemedicine, and advanced diagnostic imaging systems (University of Minnesota Rochester, 2022).

Likewise, SMEs also partner with universities or technical institutions to bridge the training gap caused by constrained resources. These partnerships may also include internship programs or joint research projects that help train staff while improving services. In the transportation sector, smaller companies in logistics often form partnerships with community colleges to provide ongoing driver safety and compliance training. An example is the Community College of Philadelphia, which partners with transportation companies to offer certification courses in commercial driving and logistics management (Aidoo, 2017). Similarly, in healthcare, small clinics and practices partner with universities to offer training in specialized areas such as robotic surgery, telehealth services, or medical billing and coding, often through online learning platforms like Coursera or edX.

4.1.6. Simulation-Based and Virtual Training

Simulation-based and virtual training has become integral to preparing employees for real-world scenarios without the risks associated with live training. In the water sector, utilities like Los Angeles Water and Power (LADWP) use virtual simulation programs to train staff on handling emergencies such as flooding or contamination incidents. These simulations allow employees to practice decision-making in real-time without risking public safety (Zohrabian and Sanders, 2020). In the transportation sector, airlines like Southwest Airlines utilize flight simulators to train pilots and crew members for emergencies, ensuring they can respond effectively to any crisis. For example, pilots train for emergency scenarios like engine failure or severe weather in a highly controlled environment, improving their performance under pressure (Wei *et al.,* 2022). Similarly, rail operators use train simulators to train employees to handle track-related incidents or signaling issues safely (Patel *et al.,* 2023). In the healthcare sector, virtual patient simulators are widely used to train medical professionals in diagnostic procedures and emergency response. The University of California, San Francisco has implemented virtual reality (VR) simulations in medical training, allowing healthcare providers to interact with simulated patients to improve diagnostic and procedural skills (Malone *et al.,* 2024).

Simulation-based training and virtual platforms are particularly beneficial for SMEs, as they provide cost-effective ways to enhance skills without the need for expensive physical infrastructure. In the water sector, SMEs are increasingly adopting virtual simulation tools that allow their employees to practice responding to emergencies such as pipeline bursts or contamination without actual risk. For instance, eWater (Australia) offers virtual training programs designed for small utilities to learn about water treatment and emergency response (Chong *et al.,* 2017). In transportation, small delivery companies and freight firms can use virtual driving simulators to train their staff, cutting down on training costs and improving safety protocols. For healthcare SMEs, virtual patient simulators and telemedicine simulations are cost-effective training tools. For example, the University of California, San Francisco (UCSF) uses virtual patient simulations for clinical staff to practice diagnostic and procedural skills, which smaller practices can access to upskill their workforce affordably (UCSF, 2024).

Table 1: Summary of Workforce Training Strategies in Critical Infrastructure Sectors

Training Strategy	Brief Description	Author(s)	Sectors
Traditional and Core Skills Training	This encompasses foundational training programs that equip employees with the essential knowledge and skills necessary for their roles. This includes technical expertise in areas such as water treatment processes, energy production methods, and patient care protocols. Additionally, it covers core competencies crucial for effective job performance, such as: • *Safety Training*: OSHA compliance, hazard recognition, emergency response procedures. • *Technical Skills*: Equipment operation and maintenance, troubleshooting, specialized skills relevant to specific roles (e.g., electrical, mechanical). • *Core Competencies*: Communication, teamwork, problem-solving, critical thinking, decision-making and adaptability.	Gonczy (2015); Ambra *et al.,* (2019); Brown *et al.,* (2020); Gurieiev *et al.,* (2020); Blanchard *et al.,* (2023)	Energy, Water, Transportation, Healthcare
Technology Integration and Innovation Training	This training focuses on equipping employees with the skills and knowledge to effectively utilize and adapt to emerging technologies that are rapidly transforming critical infrastructure sectors. This includes: • *Cybersecurity Training*: Phishing awareness, incident response, data protection, and defense against cyber threats. • *Automation and Robotics Training*: Training on the operation and maintenance of automated systems, including robotics and AI-powered technologies. • *IoT Training*: Understanding and utilizing the Internet of Things (IoT) in infrastructure management, such as smart grid technologies, sensor networks and data analytics.	Naranjo-Valencia *et al.,* (2018); Wahl (2019); Apa *et al.,* (2021); (Jasiūnas *et al.,* 2021); Sanchez *et al.,* (2023)	Energy, Water, Transportation, Healthcare

Training Strategy	Brief Description	Author(s)	Sectors
Emerging Threats and Risk Management Training	This training prepares workers to identify, assess, and mitigate the impact of emerging threats and risks that can significantly impact critical infrastructure operations. This includes: • *Threat Assessment*: Identifying potential threats such as natural disasters (e.g., earthquakes, floods), cyberattacks, pandemics, and terrorism. • *Risk Mitigation*: Developing and implementing strategies to reduce the likelihood and impact of these threats, such as emergency response plans, business continuity plans, and disaster recovery procedures.	Ambra *et al.,* (2019); Brown *et al.,* (2020); Chai (2020); (Jasiūnas *et al.,* 2021); AHA (2022); Sanchez *et al.,* (2023)	Healthcare, Energy
Certification and Regulatory Compliance Training	This training ensures that workers meet industry standards and comply with relevant regulations. This involves: • *Industry Certifications*: Obtaining professional certifications relevant to their roles (e.g., electrician licenses, operator certifications) to demonstrate expertise and meet industry standards. • *Regulatory Compliance Training*: Training on relevant laws, regulations, and safety standards to ensure compliance with government regulations and industry best practices. This is particularly crucial in sectors like water, transportation and healthcare, which are subject to stringent regulations.	Ambra *et al.,* (2019); Olson (2020); (Jasiūnas *et al.,* 2021); Blanchard *et al.,* (2023); Sanchez *et al.,* (2023)	Water, Transportation, Healthcare

Training Strategy	Brief Description	Author(s)	Sectors
Partnerships with Educational Institutions	This involves collaborative efforts between industry and academia to enhance workforce development. Key initiatives include: • *Apprenticeships and Internships*: Providing on-the-job training and mentorship opportunities for students, fostering practical skills and industry experience. • *Joint Training Programs*: Developing and delivering specialized training programs in collaboration with universities and technical colleges, leveraging academic expertise and industry needs. • *Guest Lectures and Workshops*: Facilitating knowledge exchange by inviting industry professionals to speak at academic institutions and vice versa.	Naranjo-Valencia *et al.,* (2018); Ambra *et al.,* (2019); Bekiaris and Loukea (2019); Rondinelli *et al.,* (2023); Sanchez *et al.,* (2023)	Energy, Water, Transportation, Healthcare
Simulation-Based and Virtual Training	This leverages technology to create realistic training environments that replicate real-world scenarios, allowing employees to learn and practice skills in a safe and controlled setting. This includes: • *Simulators*: Utilizing sophisticated simulators to replicate complex systems and scenarios, such as power plant simulators, flight simulators, and medical simulations. • *E-learning Platforms*: Providing online courses and training modules that offer flexibility and accessibility for employees. • *Virtual Reality (VR) Training*: Immersive training experiences that enhance learning and retention by providing a realistic and engaging environment for skill development.	Bekiaris and Loukea (2019); Apa *et al.,* (2021); Elendu *et al.,* (2024); Sahid (2024)	Healthcare, Transportation, Energy

4.3. Workforce Training Challenges and Opportunities for SMEs in Critical Infrastructure Sectors

Small and medium-sized enterprises (SMEs) within critical infrastructure sectors face a unique set of challenges when it comes to workforce training. These challenges often stem from limited resources, both financial and human, as well as the complexity of meeting industry standards and regulatory requirements (Gamage *et al.,* 2020; Doss-Gollin *et al.,* 2021). One of the most significant challenges SMEs faces is limited financial resources, which makes it difficult for them to invest in comprehensive workforce training programs. Unlike large organizations, SMEs often do not

have the budget for dedicated in-house training teams or advanced simulation tools (Dudin *et al.,* 2019; Pawar and Lal, 2022). This constraint can hinder their ability to implement strategies such as technology integration and innovation training (e.g., adopting AI or digital technologies) or simulation-based and virtual training (e.g., using virtual labs for emergency preparedness).

Another challenge is the lack of specialized expertise within SMEs. Many critical infrastructure sectors require a high level of technical knowledge, especially in areas like cybersecurity and regulatory compliance. According to Gurieiev *et al.,* (2020), SMEs often struggle to provide their employees with the necessary technical skills or to offer emerging threats and risk management training, particularly as they may not have dedicated cybersecurity experts in-house. Moreover, SMEs may find it difficult to keep up with evolving technologies and industry standards, such as the certification and regulatory compliance training required in sectors like healthcare and transportation (Jasiūnas *et al.,* 2021). As discussed earlier, compliance with industry regulations is crucial for ensuring safety and operational efficiency. However, for SMEs, the complexity and cost of compliance training, particularly with constantly changing regulations, pose a significant burden (Shashidhar and Varol, 2023). For example, small water utilities may not have the resources to invest in extensive training programs required to meet the standards set by organizations like the American Water Works Association (AWWA). Similarly, in the healthcare sector, small clinics may struggle to keep their staff updated on the latest certification and regulatory compliance training required for infection control and patient safety protocols (Heath *et al.,* 2020).

4.4. Recommendations for Enhancing Workforce Training in SMEs

To enhance workforce training and development, SMEs can consider forming strategic partnerships with universities, technical institutions and industry associations (Apa *et al.,* 2021). Such collaborations provide access to cutting-edge research, specialized training programs and innovative technologies. For example, SMEs in sectors like water treatment and transportation could partner with local universities to access affordable or even subsidized training programs. The University of California, Berkeley, has formed partnerships with local SMEs in the clean energy sector, providing access to advanced research facilities and expertise in sustainable technologies (University of California, 2024). Similarly, the University of Nevada, Reno has partnered with local water utilities to focus on applied research in water and wastewater treatment technologies (Brown *et al.,* 2020). These partnerships not only enhance the technical capabilities of SMEs but also foster innovation and competitiveness within their industries.

Another opportunity for SMEs to enhance workforce training is through simulation-based and virtual training. These cost-effective solutions offer scalable ways to deliver high-quality training without the need for expensive physical setups. For example, small water utilities can use virtual training platforms to simulate emergencies, such as contamination or pipe bursts, allowing staff to practice their responses in a controlled environment (Sanchez *et al.,* 2023). In the healthcare sector, virtual patient simulators and telemedicine simulations can provide affordable and accessible training for small clinics, helping to improve diagnostic and procedural skills. These simulation-based approaches allow SMEs to train their workforce efficiently while managing limited resources.

Lastly, flexible, modular training programs are a practical solution for SMEs with budget constraints. These programs allow businesses to tailor training to the specific needs of their workforce while providing the flexibility for employees to learn at their own pace. Programs that can be delivered online or in short bursts are particularly beneficial, as they enable SMEs to balance workforce development with financial limitations (Ambra *et al.,* 2019). For example, Stanford Online offers a digital transformation and technology integration program consisting of self-paced courses that professionals can complete over time. This model allows SMEs to keep their employees up to date with the latest technologies and digital strategies without the need for long-term, full-time training

commitments. By embracing these training solutions, SMEs can enhance their workforce capabilities and remain competitive in an ever-evolving market (Cubrich *et al.,* 2022).

5. Practical Applicability of Findings

Having reviewed the various workforce training strategies, the findings provide actionable solutions that SMEs in the energy, water, transportation and healthcare sectors can adopt to address workforce preparedness gaps, improve resilience and enhance operational efficiency. One key strategy is targeted workforce development through partnerships with universities, technical institutions and industry associations. SMEs can leverage these collaborations to access tailored, affordable training programs that meet their workforce needs. For example, in the water sector, small utility companies could collaborate with universities to gain subsidized training in water treatment technologies and quality monitoring. The University of North Carolina's Environmental Finance Center has partnered with small utilities to deliver workshops and online training that build workforce capacity and ensure regulatory compliance (Santana, 2022). Similarly, in the transportation sector, small logistics firms can collaborate with community colleges to offer certification programs for commercial driving and supply chain management. The Community College of Philadelphia exemplifies this model by working with SMEs to upskill employees in logistics and transportation operations (Community College of Philadelphia, 2024).

The adoption of cost-effective training models, such as virtual and simulation-based programs, can also offer SMEs scalable solutions to upskill their workforce without significant infrastructure investments. In the healthcare sector, small clinics and rural hospitals can use simulation tools like Laerdal's SimMan to train nurses and medical staff in emergency response and telehealth operations, ensuring ongoing professional development at a reduced cost (Bliss *et al.,* 2022). Similarly, in the energy sector, small renewable energy firms can adopt simulation-based maintenance training for technologies such as solar microgrid systems. Organizations like the International Renewable Energy Agency (IRENA) promote affordable simulation-based training specifically designed for SMEs operating in renewable energy markets. To bridge technology and innovation gaps, SMEs can focus on workforce training that integrates emerging technologies. For example, in the water sector, small companies can train their workforce in IoT-enabled water distribution monitoring to improve efficiency and reduce leakages. LeakFinder, a small water management company based in Westbury, New York, successfully implemented such training in collaboration with technology providers. For example, they have collaborated with Echologics to implement advanced leak detection technologies and training. This partnership has enabled LeakFinder to enhance their capabilities in identifying and managing leaks more efficiently (Echologics, 2023). In the energy sector, small solar installation firms can train employees to operate advanced systems, such as microgrid management tools, with the support of institutions like the National Renewable Energy Laboratory (NREL), which offers hands-on workshops tailored to SMEs.

Finally, improved access to certification and regulatory training is another critical area for SMEs, as it enhances compliance with industry standards and builds sector credibility. In the healthcare sector, small diagnostic laboratories can train lab technicians to achieve ISO 15189 certification, ensuring adherence to international quality standards. Organizations like the American Society for Quality (ASQ) offer tailored certification pathways for SMEs (American Society for Quality, 2024). Likewise, in the transportation sector, small trucking companies can collaborate with state transportation agencies to train drivers on fleet safety certifications and environmental compliance, aligning their operations with sustainability-focused regulations like the Clean Air Act. Moreover, workforce training strategies that address emerging threats and risk management can strengthen SMEs' resilience against disruptions.

6. Policy-Level Implications for Workforce Training in SMEs

Given the critical role of SMEs in the energy, water, transportation and healthcare sectors, targeted policy interventions can enhance workforce training and preparedness. Governments play a pivotal role in ensuring that SMEs have access to the necessary resources, training programs and financial incentives to develop a skilled and resilient workforce. One key policy consideration is increased government funding for SME workforce training through direct subsidies, training grants and low-interest loans. As mentioned earlier, many SMEs struggle with the financial burden of continuous workforce development, particularly in high-tech sectors requiring specialized skills. Government-backed funding mechanisms, such as sector-specific training grants or workforce development tax credits, could incentivize SMEs to invest in employee training without compromising operational budgets. For example, in the energy sector, the U.S. Department of Energy (DOE) has provided funding for workforce training in renewable energy technologies, a model that could be expanded to other critical infrastructure sectors.

Also. currently, workforce training requirements vary widely across sectors and regions, leading to inconsistencies in skill levels and preparedness. Establishing baseline national training requirements—particularly for SMEs operating in safety-sensitive industries such as healthcare and transportation—could ensure a minimum competency level across the workforce. However, such standardization must be flexible enough to accommodate the unique needs and capacities of smaller enterprises. A tiered approach, where SMEs can adopt training modules relevant to their specific operations while meeting overarching national standards, may be an effective compromise. Tax incentives and grants could further promote industry-academic collaborations in workforce training, promoting partnerships between SMEs and educational institutions. By offering tax deductions or direct grants for SMEs that engage in training partnerships with universities, technical colleges and industry associations, governments can help bridge the skills gap while reducing financial barriers for small businesses. For instance, countries like Germany and Singapore have successfully implemented co-funded vocational training programs where businesses receive government support for employee upskilling. A similar approach could be tailored for SMEs in critical infrastructure sectors, ensuring they have access to cutting-edge workforce development resources. Additionally, governments could support public-private training initiatives that address emerging workforce challenges, such as the integration of digital tools, automation and climate-resilient technologies. This could involve funding collaborative research initiatives between SMEs, universities and technology providers, as well as establishing innovation hubs that offer subsidized training in advanced industry practices.

By implementing these policy measures, governments can help SMEs build a future-ready workforce, enhance sectoral resilience and ensure that critical infrastructure sectors remain operationally efficient in the face of evolving challenges.

7. Contributions of the Research

This research makes several unique contributions. While previous studies primarily focus on large organizations, this study uniquely highlights the challenges and opportunities specific to SMEs. SMEs play a crucial role in maintaining critical infrastructure, yet they often lack access to advanced training resources (Dawson *et al.,* 2021). By addressing this gap, the study brings much-needed attention to the workforce training needs of SMEs, which are frequently overlooked in both research and policy discussions. A key advancement of this study is its systematic evaluation of workforce training strategies across multiple critical infrastructure sectors, including energy, water, transportation and healthcare. Unlike prior research that often examines training approaches in isolation, this study takes a cross-sectoral perspective, identifying common challenges and best practices that can be adapted to different sectors. Beyond identifying training gaps, this research goes a step further by offering

tailored and actionable recommendations for SMEs. Many workforce training studies highlight deficiencies without providing feasible solutions, but this study proposes scalable, cost-effective training strategies that align with the resource constraints faced by smaller enterprises. This is further summarized in Section 4.4. This study also advances the field by shifting the focus from infrastructure resilience to workforce resilience. While much of the existing literature discusses the physical and technological aspects of protecting critical infrastructure, this research highlights the pivotal role of frontline employees in ensuring operational continuity during crises. By integrating insights from disciplines such as engineering, business management and crisis management, the study offers a holistic perspective on workforce training, ensuring that employees are equipped to handle evolving threats such as climate change impacts, cybersecurity breaches and cascading disruptions.

8. Conclusions

This review highlights the diverse workforce training strategies currently utilized within critical infrastructure sectors, emphasizing their relevance to improving employee skills, resilience and adaptability in the face of evolving challenges. Six strategies were identified in this review: (1) traditional and core skills training, (2) technology integration and innovation training, (3) emerging threats and risk management training, (4) certification and regulatory compliance training, (5) partnerships with educational institutions and (6) simulation-based and virtual training. Small and medium-sized enterprises (SMEs), which often face resource constraints, stand to benefit significantly from adopting these strategies. Through collaborations with universities, leveraging affordable simulation-based tools, or accessing government-sponsored training programs, SMEs can address workforce gaps while maintaining operational efficiency. Despite these opportunities, challenges persist, particularly in funding, awareness and accessibility, underscoring the need for tailored interventions and policy support. This study demonstrates the practical applicability of workforce training initiatives, providing actionable insights for SMEs to enhance their workforce preparedness. By adopting innovative training models and forming strategic partnerships, SMEs can not only meet regulatory demands but also build a skilled workforce capable of thriving in increasingly complex and interconnected environments. Future research could explore longitudinal impacts of training programs across different sectors and further investigate cost-effective solutions for SMEs in underserved regions, ensuring that critical infrastructure sectors remain resilient and secure.

Acknowledgement

The authors would like to thank the Homeland Security Institute, and The Department of Computer Science at Sam Houston State University, for funding and support in developing this whitepaper.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Aidoo, F. S. (2017). The Other ‘Philadelphia Plan’: Community Philanthropy and Corporate Investment in Critical Infrastructure for Back-to-the-city Movements, 1950-1985 (Doctoral dissertation, Harvard University). https://www.proquest.com/dissertations-theses/other-philadelphia-plan-community-philanthropy/docview/2451165177/se-2?accountid=14537

Ambra, T., Caris, A., & Macharis, C. (2019). Towards freight transport system unification: reviewing and combining the advancements in the physical internet and synchromodal transport research. International Journal of Production Research, 57(6), 1606-1623. https://doi.org/10.1080/00207543.2018.1494392

American Heart Association. (2022). Retrieved from https://www.heart.org/
American Society for Quality. (2024). Certifications. https://www.asq.org/cert
Apa, R., De Marchi, V., Grandinetti, R., & Sedita, S. R. (2021). University-SME collaboration and innovation performance: the role of informal relationships and absorptive capacity. The Journal of Technology Transfer, 46, 961-988. https://doi.org/10.1007/s10961-020-09802-9
Bekiaris, E., & Loukea, M. (2019). Skills and Training Requirements for the Future Transportation Sector of Europe. Наука и техника, (6), 476-481. https://cyberleninka.ru/article/n/skills-and-training-requirements-for-the-future-transportation-sector-of-europe
Blanchard, P. N., & Thacker, J. W. (2023). Effective training: Systems, strategies, and practices. SAGE Publications. https://www.amazon.com/Effective-Training-Systems-Strategies-Practices/dp/1071927809
Bliss, J. P., Etherton, K. C., Hodge, D., & Winner, J. (2022, September). Performance Based Evaluation of Cricothyroidotomy Simulators for Training. In Proceedings of the International Symposium on Human Factors and Ergonomics in Health Care (Vol. 11, No. 1, pp. 26-31). Sage CA: Los Angeles, CA: SAGE Publications. https://apps.dtic.mil/sti/trecms/pdf/AD1195808.pdf
Bradač Hojnik, B., & Huđek, I. (2023). Small and Medium-Sized Enterprises in the Digital Age: Understanding Characteristics and Essential Demands. Information, 14(11), 606. https://doi.org/10.3390/info14110606
Brown, M., Karimova, F., Love, N., Pagilla, K., Bott, C., He, Z., ... & Merther, S. (2020). University–utility partnerships: Best practices for water innovation and collaboration. Water Environment Research, 92(3), 314-319. https://doi.org/10.1002/wer.1252
Cervini, J., Rubin, A., & Watkins, L. (2022, March). Don't drink the cyber: Extrapolating the possibilities of Oldsmar's water treatment cyberattack. In International conference on cyber warfare and security (Vol. 17, No. 1, pp. 19-25). Academic Conferences International Limited. https://doi.org/10.34190/iccws.17.1.003
Chai, L. (2020). Self-driving cars closer to reality. RoboGlobal White Paper, 1-13. https://f.hubspotusercontent40.net/hubfs/7764048/White%20Papers/Autonomous%20Vehicles.pdf
Chong, N., Bach, P. M., Moilleron, R., Bonhomme, C., & Deroubaix, J. F. (2017). Use and utility: exploring the diversity and design of water models at the science-policy interface. Water, 9(12), 983.https://doi.org/10.3390/w9120983
Chuang, S. (2024). Employee perspectives on effective crisis leadership skills in small and medium-sized enterprises. Human Resource Development International, 1-22. https://doi.org/10.1080/13678868.2024.2399488
Cleveland Clinic. (2023). Robotic Surgery and Minimally Invasive Urologic Oncology Fellowship (RSMIUO). Retrieved from https://my.clevelandclinic.org/departments/urology-kidney/medical-professionals/urology-fellowships/robotic-laparoscopic
Community College of Philadelphia. (2024). Power up your business. https://www.ccp.edu/degrees-programs/continuing-education-noncredit/power-up-your-business
Cubrich, M., Sodhi, K., Petruzzelli, A., & Doverspike, D. (2022). Who rescues the rescuers? Multilevel challenges facing first responder organizations. Crisis and chaos and organizations: The coronavirus and lessons for organizational theory, 65-96. https://www.researchgate.net/profile/Marc-Cubrich/publication/364677361_Who_Rescues_the_Rescuers_Multilevel_Challenges_Facing_First_Responder_Organizations/links/6357056b8d4484154a2d8a3b/Who-Rescues-the-Rescuers-Multilevel-Challenges-Facing-First-Responder-Organizations.pdf
Cybersecurity and Infrastructure Security Agency (CISA), Homepage | https://www.cisa.gov/, accessed multiple times 2022

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

Doss-Gollin, J., Farnham, D. J., Lall, U., & Modi, V. (2021). How unprecedented was the February 2021 Texas cold snap?. Environmental Research Letters, 16(6), 064056. https://doi.org/10.1088/1748-9326/ac0278

Dreher, R., Jüngst, J., & Komp, F. (2024). Vocational Education Training (VET) for Electrical-Driven Cars: Development of a Training Concept for the Aftersales Market (Project DIAKOM-E). In Automotive Aftermarket: Global and Interdisciplinary Perspectives (pp. 139-166). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-62419-3_8

Driving, D. F. (2020). National Safety Council. Accident Analysis & Prevention, 37(6), 1066-1073. https://www.nsc.org/getmedia/37c659be-6b37-4a0e-88d9-ad96c72ec0ab/adid-drowsy-driving-143.pdf

Dudin, M. N., Frolova, E. E., Protopopova, O. V., Mamedov, O., & Odintsov, S. V. (2019). Study of innovative technologies in the energy industry: nontraditional and renewable energy sources. Entrepreneurship and Sustainability Issues, 6(4), 1704. http://doi.org/10.9770/jesi.2019.6.4(11)

Echologics. (2023). Private water utilities. https://www.echologics.com/markets/private-water-utilities/

Elendu, C., Amaechi, D. C., Okatta, A. U., Amaechi, E. C., Elendu, T. C., Ezeh, C. P., & Elendu, I. D. (2024). The impact of simulation-based training in medical education: A review. Medicine, 103(27), e38813. http://doi.org/10.1097/MD.0000000000038813

Gamage, S. N., Ekanayake, E. M. S., Abeyrathne, G. A. K. N. J., Prasanna, R. P. I. R., Jayasundara, J. M. S. B., & Rajapakshe, P. S. K. (2020). A review of global challenges and survival strategies of small and medium enterprises (SMEs). Economies, 8(4), 79. https://doi.org/10.3390/economies8040079

Gonczy, S. T. (2015). Federal Aviation Administration (FAA) airworthiness certification for ceramic matrix composite components in civil aircraft systems. In MATEC Web of Conferences (Vol. 29, p. 00002). EDP Sciences. https://doi.org/10.1051/matecconf/20152900002

Gurieiev, V., Kutsan, Y. G., Iatsyshyn, A. V., Iatsyshyn, A. V., Kovach, V. O., Lysenko, E., ... & Popov, O. O. (2020). Simulating systems for advanced training and professional development of energy specialists in power sector. In Proceedings of the 16th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume II: Workshops Kharkiv, Ukraine, October 06-10, 2020 (Vol. 2732, pp. 693-708). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-2732/20200693.pdf

Healthcare IT News. (2020). Universal Health Services faces $67 million loss after cyberattack. https://www.healthcareitnews.com/news/universal-health-services-faces-67-million-loss-after-cyberattack

Heath, C., Sommerfield, A., & von Ungern‐Sternberg, B. S. (2020). Resilience strategies to manage psychological distress among healthcare workers during the COVID‐19 pandemic: a narrative review. Anaesthesia, 75(10), 1364-1371. https://doi.org/10.1111/anae.15180

Jasiūnas, J., Lund, P. D., & Mikkola, J. (2021). Energy system resilience–A review. Renewable and Sustainable Energy Reviews, 150, 111476. https://doi.org/10.1016/j.rser.2021.111476

Los Angeles Department of Water and Power. (2024). Careers. Retrieved from https://www.ladwp.com/who-we-are/careers

Malone, M., Way, D. P., Leung, C. G., Danforth, D., Maicher, K., Vakil, J., ... & San Miguel, C. (2024). Evaluation of high-fidelity and virtual reality simulation platforms for assessing fourth-year

medical students' encounters with patients in need of urgent or emergent care. Annals of Medicine, 56(1), 2382947. https://doi.org/10.1080/07853890.2024.2382947

Mayo Clinic. (2021). Top-ranked Hospital in the Nation. Retrieved from https://www.mayoclinic.org/

Naranjo-Valencia, J. C., Naranjo-Herrera, C. G., Serna-Gómez, H. M., & Calderón-Hernández, G. (2018). The relationship between training and innovation in companies. International journal of innovation management, 22(02), 1850012. https://doi.org/10.1142/S1363919618500123

Okoli, C., & Schabram, K. (2015). A guide to conducting a systematic literature review of information systems research. http://sprouts.aisnet.org/10-26

Olonilua, O. (2022), "Equity and Justice in Hazard Mitigation", Jerolleman, A. and Waugh, W.L. (Ed.) Justice, Equity, and Emergency Management (Community, Environment and Disaster Risk Management, Vol. 25), Emerald Publishing Limited, Leeds, pp. 107-129. https://doi.org/10.1108/S2040-726220220000025006

Olson, P. J. (2020). AWWA Standards for Water Reuse. Journal: American Water Works Association, 112(9). https://doi.org/10.1002/awwa.1575

Patel, V. K., Verma, A., & Verma, P. (2023). Comparative Study of Train Operation Simulators. Journal of Scientific Research, 66(4). DOI: https://doi.org/10.37398/JSR.2023.670411

Pawar, S., & Lal, A. T. (2022). A Study on Branding of Ed-Tech Platforms with focus on Start-Up My Captain. FORE School of Management. https://dspace.fsm.ac.in/jspui/password-login

Perez, A. P., Sauma, E. E., Munoz, F. D., & Hobbs, B. F. (2016). The economic effects of interregional trading of renewable energy certificates in the US WECC. The Energy Journal, 37(4), 267-296. https://doi.org/10.5547/01956574.37.4

Remington, C. L., Witkowski, K., Ganapati, N. E., Headley, A. M., & Contreras, S. L. (2024). First Responders and the COVID-19 Pandemic: How Organizational Strategies Can Promote Workforce Retention. The American Review of Public Administration, 54(1), 33-56. https://doi.org/10.1177/027507402311929

Rondinelli, R. D., Genovese, E., Katz, R. T., Mayer, T. G., Mueller, K. L., Ranavaya, M. I., & Brigham, C. R. (2023). AMA Guides® to the Evaluation of Permanent Impairment, 2023. In AMA Guides® to the Evaluation of Permanent Impairment, Sixth Edition, 2023. American Medical Association. DOI: https://doi.org/10.1001/978-1-64016-282-2

Sahid, A. (2024). Securing Healthcare. Secure Health: A Guide to Cybersecurity for Healthcare Managers, 196. https://doi.org/10.1201/9781003470038

Santana, G. (2022, May 25). What makes small utilities viable? Environmental Finance Center at the University of North Carolina. https://efc.sog.unc.edu/what-makes-small-utilities-viable/

Shashidhar, N. & Varol, C. (2023) Forensic Digital Data Sanitization A Guide for Small and Medium-Sized Businesses A Primer on Data Erasure: An Integral Component of Data Lifecycle Management. (Report No. IHS/CR-2023-1028). The Sam Houston State University Institute for Homeland Security. https://doi.org/10.17605/OSF.IO/MF6HJ

Smart Water Magazine. (2023, October 26). Atlanta will use artificial intelligence tools to detect water main breaks https://smartwatermagazine.com/news/smart-water-magazine/atlanta-will-use-artificial-intelligence-tools-detect-water-main-breaks

UCSF Medical Education. (2024). Kanbar Center for Simulation and Clinical Skills. Retrieved from https://meded.ucsf.edu/kanbar-center-simulation-and-clinical-skills

University of California, Berkeley. (2024). Clean Energy | Sustainability & Carbon Solutions. Retrieved December 17, 2024, from https://sustainability.berkeley.edu/clean-energy

University of Minnesota Rochester. (2022). UMR and Mayo Clinic Collaboration. Retrieved from https://r.umn.edu/academics-research/undergraduate-programs/bachelor-science-health-professions/collaboration

Wahl, K. M. (2019). The Role of Higher Education Programs to the Future of the Wastewater Industry. Baker College (Michigan). https://www.proquest.com/dissertations-theses/

role-higher-education-programs-future-wastewater/docview/2284217243/se-2?accountid=14537

Wei, M. Y., Fang, S. A., & Liu, J. W. (2022). Design and implementation of a new training flight simulator system. Sensors, 22(20), 7933. https://doi.org/10.3390/s22207933

Willett, M. (2023). Lessons of the SolarWinds hack. In Survival April–May 2021: Facing Russia (pp. 7-25). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003422129-1/lessons-solarwinds-hack-marcus-willett

Zohrabian, A., & Sanders, K. T. (2020). The energy trade-offs of transitioning to a locally sourced water supply portfolio in the city of Los Angeles. Energies, 13(21), 5589. https://doi.org/10.3390/en13215589

Authors Biographies

Oluponmile Olonilua, Ph.D. CFM is a professor and coordinator of the Emergency Management and Homeland Security program in the Department of Political Science and Public Administration in the Barbara Jordan-Mickey Leland School of Public Affairs at Texas Southern University. Dr. Olonilua serves as a member of FEMA Region VI Regional Advisory Council and as the Chair of the FEMA Region VI Higher Education Collaborative. She serves on Mary Fran Myers Scholarship Award Committee (MFM), an award at the Natural Hazards annual Workshop in Broomfield, Colorado. Dr. Olonilua has been actively involved with the FEMA Higher Education program in various categories and currently is the Lead for the HBCU Special Interest Group. She has published papers in top journals in the field of Emergency Management and presented her research in professional conferences of Political science, Public Administration, Planning, and Emergency Management. Olonilua is regular reviewer for different peer reviewed journals including Journal of Landscape and Urban Planning, Journal of Public Management and Social Policy, Journal of Emergency Management, Journal of Planning Education and Research, and Disasters Journal. She has attended the International Association of Emergency Managers and has been a certified floodplain emergency manager since 2011. Her research interests include hazard mitigation, emergency management, community engagement, diversity, equity, and inclusion.

John Ogbeleakhu Aliu, PhD, is currently a clinical assistant professor with the Engineering Education Transformations Institute, College of Engineering, University of Georgia, Athens, Georgia. Dr. Aliu's research interests lie in the areas of curriculum development, sustainability, sustainable construction, skills development, employability studies, diversity, equity and inclusion studies. He has authored and co-authored several publications in top journals in the field of construction digitalization, sustainable construction and engineering education. Dr Aliu is currently an Associate Editor of ASCE's Journal of Civil Engineering Education. John is also a regular reviewer for different peer-reviewed journals, including the Journal of Cleaner Production, Engineering, Construction and Architectural Management, Sustainable Development Journal, Frontiers in Built Environment, International Journal of Sustainability in Higher Education, Construction Economics and Building, African Journal of Science, Technology, Innovation and Development, Journal of Construction in Developing Countries, Journal of Engineering, Design and Technology, Journal of Construction Project Management and Innovation, International Journal of Construction Management, Journal of Construction Engineering and Management, Cogent Economics and Finance, Built Environment Project and Asset Management, and others.

Suggested citation: **Olonilua, O., & Aliu, J. O.** (2025). Assessing workforce training strategies in critical infrastructure: Insights and recommendations. *One Step Ahead*, *July 2025*, 29–49. The Sam Houston State University Institute for Homeland Security. OSF | Assessing Workforce Training Strategies in Critical Infrastructure: Insights and Recommendations

GENERATIVE AI FOR ADVANCED SECURITY FRAMEWORKS IN TRANSPORTATION NETWORKS

John Aliu

Abstract

Artificial intelligence (AI) has revolutionized critical infrastructure sectors, enhancing efficiency, safety and decision-making. In transportation, AI has proven valuable in traffic management, autonomous vehicles and logistics optimization. However, as cybersecurity threats become more sophisticated, the integration of AI into transportation security frameworks remains underdeveloped. Generative AI, in particular, has not been fully utilized for threat detection, response and proactive measures. While traditional security measures are well-established, the use of generative AI for enhancing transportation security is still in its early stages and not yet widely adopted. This study aims to bridge this gap by investigating generative AI's role in strengthening transportation security frameworks. Through bibliometric analysis, the research identifies four key clusters where generative AI shows promise: (1) smart routing and traffic control, (2) traffic pattern simulation and prediction, (3) transportation cybersecurity and intelligence and (4) real-time decision support systems. The findings highlight the current state of AI applications in transportation security, revealing both progress and critical gaps. This study also provides actionable insights and practical recommendations for private industry professionals involved in the development, implementation and management of transportation security systems. By identifying the key clusters where generative AI can be most effectively applied, the study offers guidance on how to integrate AI technologies into existing security frameworks. This study is one of the first to conduct a bibliometric analysis of the integration of generative AI into security frameworks within transportation systems. As such, it provides a foundation for future research and development in this emerging area.

Keywords: AI-driven solutions, Autonomous vehicles, Cybersecurity, Generative AI, Threat detection, Traffic management, Transportation networks.

1. Introduction

Artificial Intelligence (AI) is increasingly transforming global businesses, disrupting industries and providing new ways to enhance efficiency, productivity and decision-making across critical infrastructure sectors. AI, through machine learning, deep learning and natural language processing, has opened up vast opportunities to optimize processes, reduce costs and improve safety in industries such as energy, water management, healthcare, manufacturing and several others. For

John Aliu, Clinical Assistant Professor, Engineering Education Transformations Institute, College of Engineering, University of Georgia, Athens, Georgia, USA; Email: john.aliu@uga.edu ORCID: 0000-0001-5651-4009

example, in the energy sector, AI-driven predictive maintenance enables utilities to identify potential equipment failures before they occur, reducing downtime and preventing costly breakdowns (Hamdan *et al.,* 2024). By analyzing real-time data from sensors and historical trends, AI systems can schedule maintenance and suggest repairs, ultimately extending the lifespan of assets and minimizing disruptions. In the healthcare sector, AI-powered diagnostic tools are assisting doctors in detecting diseases early by analyzing medical images, accelerating the diagnostic process and increasing treatment accuracy (Zeb *et al.,* 2024). Similarly, AI in water management uses smart sensors to detect anomalies in water quality and leakage, helping utilities respond faster and more effectively to potential disruptions (Krishnan *et al.,* 2022). Manufacturing industries have also adopted AI for automation and quality control, where AI algorithms continuously monitor and improve production lines, reducing human error and enhancing product quality (Plathottam *et al.,* 2023). With its ability to process and analyze massive amounts of data in real-time, AI is emerging as a critical enabler of efficiency, safety and innovation in these sectors, highlighting its growing importance in enhancing the resilience and sustainability of critical infrastructure worldwide.

In the transportation sector, AI, particularly generative AI, holds tremendous promise in addressing long-standing challenges related to safety, efficiency and infrastructure resilience. Modern transportation systems face numerous hurdles, including traffic congestion, road safety concerns, increasing security risks and aging infrastructure (Lieberthal *et al.,* 2024). For instance, traffic congestion in urban areas not only leads to lost productivity but also exacerbates air pollution and affects public health. Generative AI can offer solutions by using real-time traffic data, weather forecasts and historical patterns to optimize traffic flow and suggest alternate routes, alleviating congestion and reducing travel times (Yan and Li, 2023). Autonomous vehicles, powered by AI, have the potential to drastically reduce traffic accidents caused by human error, thus, ensuring safer roads. However, with the rise of connected and autonomous vehicles, transportation cybersecurity has become a significant concern. AI can address these vulnerabilities by detecting anomalies in the network, identifying potential cyber threats and responding in real-time to prevent disruptions or breaches (Jihong and Xiang, 2024). Another challenge the transportation industry faces is the maintenance of aging infrastructure, which often results in delays, accidents and costly repairs. Predictive maintenance powered by AI models can help transportation agencies monitor the condition of roads, bridges and railways, allowing them to prioritize repairs before they become critical failures (Malathi *et al.,* 2025). Furthermore, the optimization of logistics, from freight management to public transit schedules, can significantly benefit from AI, improving operational efficiency and reducing costs. By incorporating generative AI technologies, transportation networks can become more intelligent, responsive and sustainable, ensuring safer, faster and more efficient systems for the future (Yan and Li, 2023).

2. Gap assessment or problem statement

The use of artificial intelligence (AI) in transportation has significantly advanced in areas such as traffic management, autonomous vehicles and logistics. However, the integration of generative AI specifically for enhancing security frameworks within transportation systems is still in its early stages. Traditional cybersecurity frameworks, like those developed by the National Institute of Standards and Technology (NIST), are being adapted to the transportation sector, but they mainly focus on general cybersecurity measures rather than specifically utilizing generative AI. While generative AI is beginning to show promise in areas like threat detection and response, its application within transportation security frameworks is not yet widespread or fully developed. This gap in application highlights the need for a more focused approach to integrating generative AI into transportation security, which is the central problem addressed by this study. This research aims to explore the potential of generative AI in enhancing security frameworks within transportation systems. Through a bibliometric analysis, the study will assess the current state of generative AI

applications in transportation security and identify existing research gaps. The goal is to provide insights into the direction of future research in this field. Additionally, the study will propose actionable strategies to address the identified gaps, outlining a way forward for the broader integration of generative AI in transportation security. By bridging these gaps, the research aims to contribute to the development of more adaptive, anticipatory security measures within transportation networks, ultimately enhancing their resilience against emerging threats.

3. A BRIEF OVERVIEW OF EMERGING TECHNOLOGIES IN THE TRANSPORTATION SECTOR

The transportation sector has undergone significant transformations in recent years, driven by rapid advancements in emerging technologies. These innovations have not only enhanced the efficiency, safety and sustainability of transportation systems but have also provided new opportunities to address longstanding challenges such as congestion, environmental impact and infrastructure strain.

Artificial Intelligence (AI) and Machine Learning: AI and machine learning are revolutionizing several aspects of the transportation sector. From smart traffic management systems to autonomous vehicles, AI plays a pivotal role in optimizing routes, reducing congestion and improving safety. AI algorithms process vast amounts of real-time data from sensors, cameras and GPS devices to predict traffic patterns, detect anomalies and provide actionable insights for operators. In the autonomous driving space, AI is the backbone of self-driving cars, enabling vehicles to make decisions based on real-time inputs from their environment (Lieberthal *et al.,* 2024). Moreover, AI is increasingly used in logistics to streamline supply chains and enhance fleet management, reducing operational costs and improving delivery times.

Autonomous Vehicles (AVs): Autonomous or self-driving vehicles represent one of the most significant technological innovations in transportation. These vehicles use a combination of AI, sensors and advanced algorithms to navigate roads and make decisions without human intervention. AVs have the potential to significantly reduce traffic accidents, enhance fuel efficiency and provide mobility solutions for people with disabilities (Qayyum *et al.,* 2020). As of now, several companies, including Tesla, Waymo, and Uber, are actively testing and deploying autonomous vehicles, though the widespread adoption of fully autonomous vehicles is still a work in progress.

Electric and Connected Vehicles (EVs and CVs): The rise of electric vehicles (EVs) and connected vehicles (CVs) is transforming the environmental footprint and operational dynamics of transportation. EVs, powered by sustainable energy sources, are becoming more prevalent due to advancements in battery technology and growing consumer demand for greener alternatives. Coupled with connected vehicle technologies, EVs can communicate with infrastructure and other vehicles, enabling smoother, safer and more energy-efficient journeys (Jeihani *et al.,* 2022). Moreover, EVs can integrate with smart grids and renewable energy sources, contributing to the broader goal of reducing greenhouse gas emissions in the transportation sector.

Smart Infrastructure and IoT: The integration of Internet of Things (IoT) devices into transportation infrastructure is enabling more efficient and responsive transportation networks. IoT technology connects vehicles, infrastructure and people, creating a “smart” transportation ecosystem. Sensors embedded in roads, bridges and traffic signals gather data that is used to monitor traffic flow, track vehicle performance and predict maintenance needs. This data can be used for predictive maintenance of infrastructure, helping to avoid costly repairs and downtime. Furthermore, IoT-enabled devices provide real-time updates to travelers, enhancing their overall experience and safety (Bathla *et al.,* 2022).

Blockchain for Transportation: Blockchain technology is gaining traction in the transportation sector, especially for its potential to enhance security, transparency and efficiency. In logistics, blockchain enables secure, immutable tracking of goods, improving the supply chain's transparency and trustworthiness. Additionally, blockchain is being explored for its potential to secure payments, validate vehicle identities and facilitate smart contracts for transportation agreements (Jabbar *et al.,* 2022).

5G and Communication Technologies: The rollout of 5G technology is poised to enable faster, more reliable communication between vehicles, infrastructure and central control systems. This ultra-fast network promises to support the large amounts of data generated by autonomous vehicles and connected infrastructure, reducing latency and improving real-time decision-making. The enhanced communication capabilities of 5G will also support applications such as vehicle-to-everything (V2X) communication, which allows vehicles to communicate with each other and their environment to improve safety and traffic flow (Aliu and Oke, 2023). Table 1 presents a summary of emerging technologies in the transportation sector, detailing their descriptions, applications, and benefits.

Table 1: Summary of emerging technologies in the transportation sector

S/N	Technology	Description	Applications	Benefits
1.	Artificial Intelligence (AI)	Use of algorithms and machine learning to simulate human cognitive functions.	Traffic management, autonomous vehicles, predictive maintenance, route optimization, security systems.	Improved efficiency, reduced human error, better traffic flow, lower operational costs, enhanced security.
2.	Autonomous Vehicles (AVs)	Self-driving vehicles use sensors, cameras and AI to navigate and make decisions without human input.	Passenger transport, freight and delivery services, last-mile logistics, shared mobility.	Reduced accidents, increased mobility for non-drivers, efficient transport, cost savings from reduced labor.
3.	Urban Air Mobility (UAM)	Air transportation systems for passengers and cargo using small, electric aircraft.	Air taxis, urban delivery services, emergency medical transport.	Reduced traffic congestion, faster transportation, and reduced environmental impact.
4.	Electric Vehicles (EVs)	Vehicles powered by electric motors rather than internal combustion engines.	Passenger vehicles, buses, delivery trucks, and even freight transport.	Lower emissions, reduced fuel consumption, cost savings on fuel, and better energy efficiency.
5.	5G Connectivity	High-speed, low-latency mobile network technology enables faster communication.	Real-time vehicle communication, smart traffic lights, vehicle-to-everything (V2X) communication.	Improved safety, real-time data sharing, enhanced automation and efficiency in transport.
6.	Blockchain Technology	A decentralized, secure digital ledger technology used for transparent transactions.	Supply chain management, vehicle ownership tracking, toll systems, and smart contracts.	Enhanced transparency, fraud prevention, reduced administrative costs, and more secure transactions.
7.	Internet of Things (IoT)	Network of interconnected devices that communicate and exchange data.	Smart infrastructure, real-time vehicle diagnostics, tracking systems, traffic management.	Improved operational efficiency, enhanced real-time data collection, and better resource allocation.

S/N	Technology	Description	Applications	Benefits
8.	Drones	Unmanned aerial vehicles used for transport, delivery, and surveillance.	Parcel delivery, traffic monitoring, infrastructure inspection, and surveying.	Faster deliveries, reduced traffic congestion, and improved monitoring of infrastructure.
9.	Smart Infrastructure	Advanced technologies are integrated into roads, bridges, and other infrastructure to optimize performance and safety.	Intelligent traffic systems, dynamic tolling, condition monitoring, and adaptive lighting.	Improved safety, reduced traffic delays, cost-effective maintenance, and better resource management.
10.	Connected Vehicles	Vehicles are equipped with sensors and communication technology that enable them to exchange data with other vehicles and infrastructure.	Vehicle-to-vehicle (V2V) communication, vehicle-to-infrastructure (V2I), smart traffic signals.	Reduced accidents, smoother traffic flow, improved safety, and real-time communication for traffic management.
11.	Mobility-as-a-Service (MaaS)	An integrated system that combines different modes of transport into a single accessible and customer-friendly digital platform.	Multi-modal transport, public transport integration, ride-sharing, and carpooling services.	Seamless travel experiences, reduced reliance on private cars, better urban mobility, and environmental benefits.
12.	Smart Traffic Management	Advanced systems that use real-time data and predictive analytics to manage traffic flow more efficiently.	Adaptive traffic signals, congestion management, incident detection, and predictive route planning.	Reduced congestion, lower emissions, improved travel times, and enhanced driver safety.
13.	Fleet Management Systems	Software solutions that monitor, manage, and optimize the performance of vehicle fleets.	Delivery services, logistics, public transport, and shared vehicle fleets.	Cost savings, fuel efficiency, maintenance optimization, better route planning, and enhanced customer service.
14.	V2X (Vehicle-to-Everything)	Communication systems enable vehicles to interact with each other and with infrastructure elements.	Traffic safety, vehicle coordination, autonomous driving, infrastructure support.	Improved safety, better coordination between vehicles and infrastructure, and reduced accidents.
15.	Quantum Computing	An advanced computing technology based on quantum-mechanical phenomena to solve complex problems.	Traffic flow optimization, logistics optimization, real-time data processing for autonomous systems.	Potential for handling complex calculations much faster than classical computers, improving traffic management and autonomous driving capabilities.
16.	Hyperloop	A new form of high-speed transportation using pressurized pods in near-vacuum tubes.	Long-distance travel, intercity transport.	Significantly faster than traditional rail and air travel, reducing travel times between cities.

S/N	Technology	Description	Applications	Benefits
17.	Augmented Reality (AR)	Technology that overlays digital information on the real world.	Navigation assistance, training for drivers and operators, maintenance support.	Improved user experience, enhanced navigation, better decision-making, and reduced training time.
18.	Advanced Driver Assistance Systems (ADAS)	Safety systems that assist drivers by automating and improving vehicle functions.	Lane-keeping assist, adaptive cruise control, automatic emergency braking, parking assistance.	Increased safety, reduction in accidents, and support for semi-autonomous driving.
19.	Electric Vertical Take-Off and Landing (eVTOL)	Aircraft that can take off and land vertically, powered by electric motors.	Urban air mobility, aerial taxis, cargo transport, and emergency response.	Reduces urban traffic congestion, enables quicker travel, and reduces the carbon footprint of transportation.

4. Research methodology

The main aim of this research is to explore the application of generative AI in enhancing security frameworks within transportation systems. To achieve this, a bibliometric analysis was conducted to assess the current state of generative AI applications in transportation security. Bibliometric analysis, as highlighted by Sajovic and Boh Podgornik (2022), is an effective tool for visualizing knowledge structures and identifying emerging trends in research. This analysis examined key themes and geographical research distribution, providing a holistic view of the state of AI-driven security research in transportation networks. To conduct this analysis, the study used VOSviewer software for data visualization of the bibliometric data. Scopus was selected as the primary database due to its broad coverage and capacity to handle large datasets (Zhao *et al.,* 2018). The bibliometric analysis specifically targeted research published between 2014 and 2024, using a search string that included terms such as “generative AI,” “AI-driven security,” “transportation networks,” “intelligent transportation systems,” “autonomous vehicles,” “machine learning,” “deep learning,” “data privacy,” “security frameworks,” and “critical infrastructure security.” The search was conducted through Scopus to ensure the inclusion of the most relevant and up-to-date studies. By identifying frequently explored themes and collaboration patterns, this quantitative approach complements the qualitative review by offering a broader understanding of the state of research and pinpointing areas where further innovation is needed.

5. Results and discussion

5.1. Publication per year on studies

Figure 1 presents the distribution of published studies per year on the integration of generative AI into transportation security frameworks. The data indicates minimal research activity before 2020, with no recorded publications from 2014 to 2017. A slight emergence of interest appeared in 2018 and 2019, with only one document published each year. There was a notable increase in publications in 2020, with nine studies, suggesting a growing recognition of the potential applications and challenges of generative AI in transportation security. A significant surge is observed in 2023, with 20 published studies, followed by a substantial peak in 2024, where research activity more than doubled, reaching 47 publications. This sharp rise suggests that generative AI’s role in transportation security has gained substantial academic and industry attention, likely due to technological advancements, increased funding and growing concerns over cybersecurity and infrastructure re-

silience. The overall trend highlights a recent acceleration in research efforts, pointing to a rapidly evolving field with increasing scholarly interest.

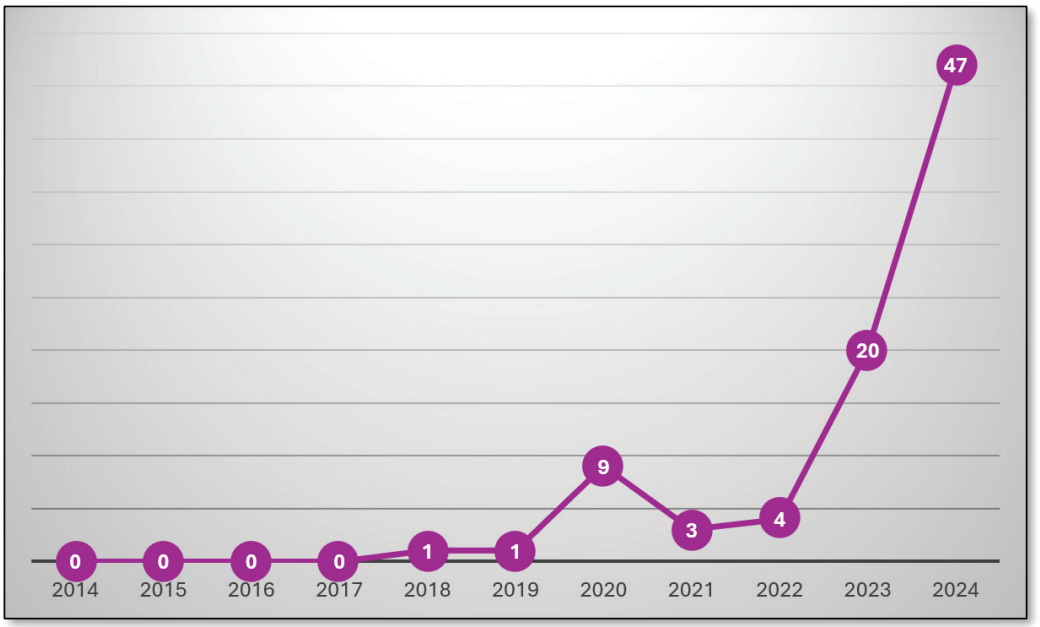


Figure 1: Publication per year on studies around generative AI in transportation networks

(Source: Author's creation)

5.2. Occurrence and cluster analysis

Cluster 1, represented by the red node, contains 21 keywords, with "generative adversarial networks (GANs)" as the focal term. GANs exhibit strong link strength (LS) with "autonomous vehicles" (LS = 35), "traffic control" (LS = 29) and "large language models (LLMs)" (LS = 27), emphasizing the role of generative AI in optimizing transportation security frameworks, particularly in traffic management, predictive analytics, and autonomous mobility. The prominence of "urban transportation" and "real-time systems" suggests researchers are actively exploring AI-powered traffic solutions for smart cities, where AI-driven models enhance mobility, reduce congestion and improve road safety. Other key terms include "Internet of Things (IoT)," "diffusion models," "metaverses," "traffic congestion" and "urban planning," reflecting a research focus on leveraging AI and IoT for real-time traffic monitoring, AI-based simulations for traffic control, and the emerging use of metaverse environments for testing transportation policies. Studies within this cluster highlight how LLMs and GANs process vast traffic datasets and generate synthetic traffic scenarios to optimize congestion management and predict future traffic patterns (Yan and Li, 2023). The connection to "autonomous vehicles" and "motor transportation" suggests AI applications are extending into self-driving vehicle decision-making, where real-time AI models enable dynamic route optimization and enhanced road safety (Jihong and Xiang, 2024). Strong links to "traffic congestion" and "traffic control" align with AI-powered adaptive traffic management systems, where predictive models preemptively adjust signal timing and reroute vehicles to alleviate congestion (Malathi *et al.,* 2025). The inclusion of "IoT" and "highway administration" indicates researchers are examining how AI can integrate with sensor-based traffic monitoring and highway management for efficient transport planning. By leveraging AI-driven real-time control mechanisms, traffic agencies can mitigate bottlenecks, reduce accidents and enhance road efficiency. Based on these interconnections, this cluster is named ***Smart Routing and Traffic Control***.

Cluster 2, represented by the green node, contains 19 keywords, with "deep learning" as the focal term. It exhibits strong link strength (LS) with "reinforcement learning" (LS = 33), "predictive models" (LS = 30) and "intelligent transportation" (LS = 28), emphasizing the role of AI-driven predictive models in transportation security frameworks. These technologies support vehicle-to-vehicle communication, forecasting and autonomous decision-making, making transportation systems more adaptive and efficient. The connection to "reinforcement learning" and "deep reinforcement learning" highlights AI's ability to optimize real-time traffic flow, autonomous navigation, and adaptive control mechanisms in self-driving vehicles (Malathi *et al.,* 2025). "Adversarial machine learning" is also prominent, indicating its importance in detecting vulnerabilities in AI-powered models and enhancing cybersecurity within transportation networks (Qayyum *et al.,* 2020). These learning models contribute to improving decision-making capabilities, allowing intelligent transportation systems to respond effectively to dynamic traffic conditions. Other key terms include "contrastive learning," "autoencoders" and "neural networks," which point toward the development of self-learning AI models for anomaly detection, predictive traffic modeling and intelligent vehicle systems. These AI techniques help simulate traffic patterns, forecast congestion and optimize real-time route planning, thus, enhancing overall transportation efficiency. Additionally, the presence of "job analysis" and "task analysis" suggests research into AI's role in workforce transformation, particularly in human-AI interactions within transportation security operations (Loske and Klumpp, 2021). As AI-driven systems become more sophisticated, integrating AI with human decision-making will be critical for operational efficiency. Given the strong focus on predictive modeling, traffic forecasting, and intelligent adaptation, this cluster is named ***Traffic Pattern Simulation and Prediction***.

Cluster 3, represented by the blue node, contains 15 keywords, with "artificial intelligence" as the focal term. It has strong link strength (LS) with "machine learning" (LS = 32), "generative adversarial networks (GANs)" (LS = 28), and "computer vision" (LS = 27), emphasizing AI's role in transforming transportation systems through enhanced security, operational efficiency and automation. The connection to "network security" and "adversarial networks" highlights growing concerns about securing AI-driven transportation networks. As AI models become essential for traffic management and autonomous vehicle operations, their vulnerability to adversarial attacks must be addressed (Malathi *et al.,* 2025). GANs play a crucial role in cybersecurity by simulating cyberattacks, and helping to develop more resilient defense mechanisms for transportation infrastructures (Yan and Li, 2023). These networks also generate synthetic data for training AI systems, improving their ability to detect and respond to real-time threats. The presence of "big data," "data set" and "predictive models" signals a shift toward utilizing large-scale datasets and AI-driven predictive analytics to enhance transportation security. AI is increasingly applied in processing real-time traffic data, optimizing traffic flow, predicting maintenance needs, and improving system resilience (Malathi *et al.,* 2025). Furthermore, the term "learning systems" underscores AI's ability to continuously adapt to evolving traffic conditions, environmental factors, and infrastructure performance, ensuring more accurate and efficient real-time decision-making. The inclusion of "intelligent transportation" and "intelligent vehicle highways" highlights AI's growing application in autonomous vehicles and smart infrastructure. AI-powered systems enable real-time navigation, vehicle-to-infrastructure communication and adaptive traffic management, enhancing safety and reducing congestion (Bathla *et al.,* 2022). Given the cluster's focus on AI-driven security and predictive analytics, it is named ***Transportation Cybersecurity and Intelligence***.

Cluster 4, represented by the yellow node, consists of 11 keywords, with "artificial intelligence (AI)" as the focal term. It has strong link strength (LS) with "decision making" (LS = 34), "machine learning" (LS = 30) and "deep neural networks" (LS = 28), emphasizing AI's role in enhancing decision-making processes within transportation security frameworks. The connection to "decision making" highlights AI's ability to automate complex processes, such as traffic management, route optimization, and security risk assessment, by analyzing vast amounts of real-time data (Malathi

et al., 2025). The presence of "machine learning" and "deep neural networks" suggests AI-driven models are being used for predictive analysis, optimizing vehicle performance, and strengthening transportation infrastructure. The term "emerging technologies" indicates the adoption of advanced innovations, such as the integration of AI with the Internet of Things (IoT), to create intelligent transportation systems capable of anticipating and mitigating potential security threats (Loske and Klumpp, 2021). "Federated learning" points to decentralized AI models that enable secure data-sharing across transportation networks without compromising privacy, making it a crucial component in large-scale, interconnected systems. Additionally, the terms "interpretability" and "learning algorithms" highlight ongoing research into making AI-driven decision-making systems more transparent and explainable. Ensuring that AI models can be interpreted by human operators is essential for trust, accountability, and regulatory compliance in transportation security applications. Given the cluster's emphasis on AI-driven automation, predictive analytics and secure decision-making frameworks, it is named ***Real-Time Decision Support Systems***.

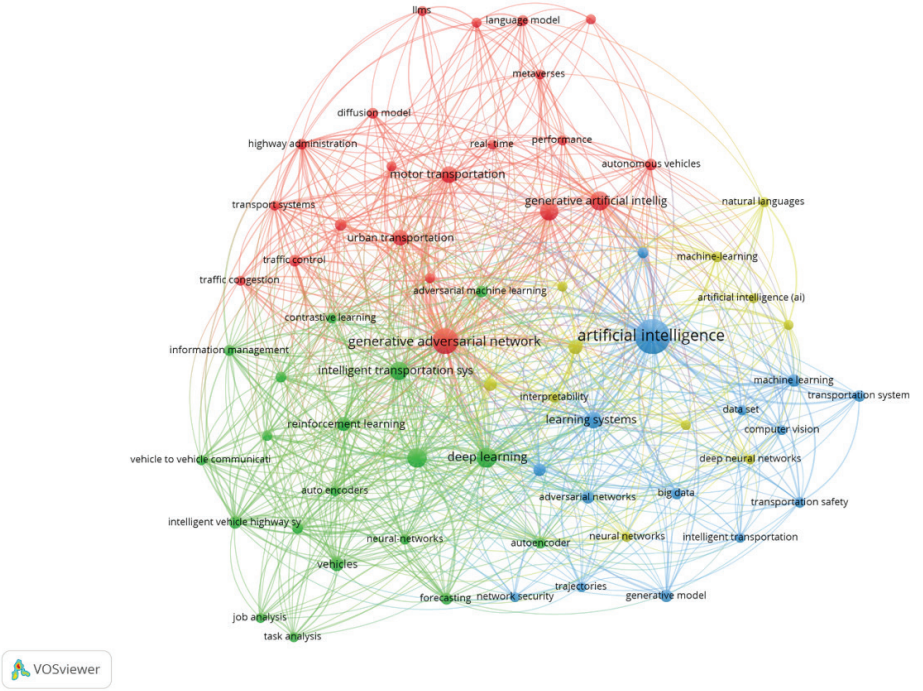


Figure 2: Network visualization of co-occurring keywords in generative AI studies on transportation security

5.3. Directions and Gaps

Further assessment of the overlay visualization map generated by VOSviewer and presented in Figure 3. The visualization, structured as a network graph, showcases the relationships between different keywords over the timeline from 2022 to 2024. The nodes in the graph represent keywords, with their sizes indicating relative importance or frequency of occurrence. Additionally, the color gradient, transitioning from blue (2022) to yellow (2024), provides insight into the temporal progression of research focus areas. Connections between nodes represent co-occurrences, highlighting interdependencies among concepts. The early research phase, characterized by blue nodes, predominantly focused on foundational concepts. The emphasis during this period was on understanding transportation challenges, task structuring and fundamental AI applications. However, security-related terms such as "network security" and "adversarial machine learning"

remained peripheral, suggesting that while security concerns were acknowledged, they were not yet a central theme in generative AI applications for transportation.

The subsequent period, represented by green nodes, marked a shift towards the integration of advanced AI techniques. This transition signifies a growing interest in leveraging sophisticated AI methodologies for transportation challenges. Concurrently, security considerations became more pronounced, with “adversarial machine learning” and “network security” emerging as more interconnected with AI and transportation concepts. In the most recent phase, illustrated by yellow nodes, “real-time performance” and “autonomous vehicles” have gained traction, highlighting the growing need for AI solutions capable of dynamic and automated decision-making in transportation systems.

Despite these advancements, several research gaps remain. One notable gap is the lack of explicit security frameworks tailored specifically for generative AI in transportation. While “adversarial machine learning” and “network security” are present in the visualization, they do not indicate the development of dedicated security architectures addressing generative AI-related vulnerabilities. Furthermore, there is an absence of explicit mentions of “data privacy” and “trustworthy AI,” which are critical given the data-intensive nature of generative AI models in transportation networks. Another key gap is the limited focus on explainability and interpretability. The visualization does not prominently feature “explainable AI” (XAI), a crucial aspect in ensuring transparency and accountability in AI-driven transportation systems. Additionally, while “real-time performance” is acknowledged, considerations regarding scalability and the real-world deployment of generative AI-based security solutions in complex transportation networks remain underexplored. Also, the visualization does not explicitly reflect interdisciplinary collaboration, which is essential for effectively addressing security challenges in AI-driven transportation systems. The integration of expertise from AI researchers, transportation engineers, cybersecurity specialists and policymakers is necessary to develop comprehensive and robust security solutions. Finally, as discussed in the previous section, existing studies have predominantly focused on four key clusters which include: (1) smart routing and traffic control, (2) traffic pattern simulation and prediction, (3) transportation cybersecurity and intelligence and (4) real-time decision support systems. While these areas have garnered significant attention, other potential applications, such as urban planning and smart city integration or behavioral analysis and fraud detection, remain underexplored and present opportunities for further investigation.

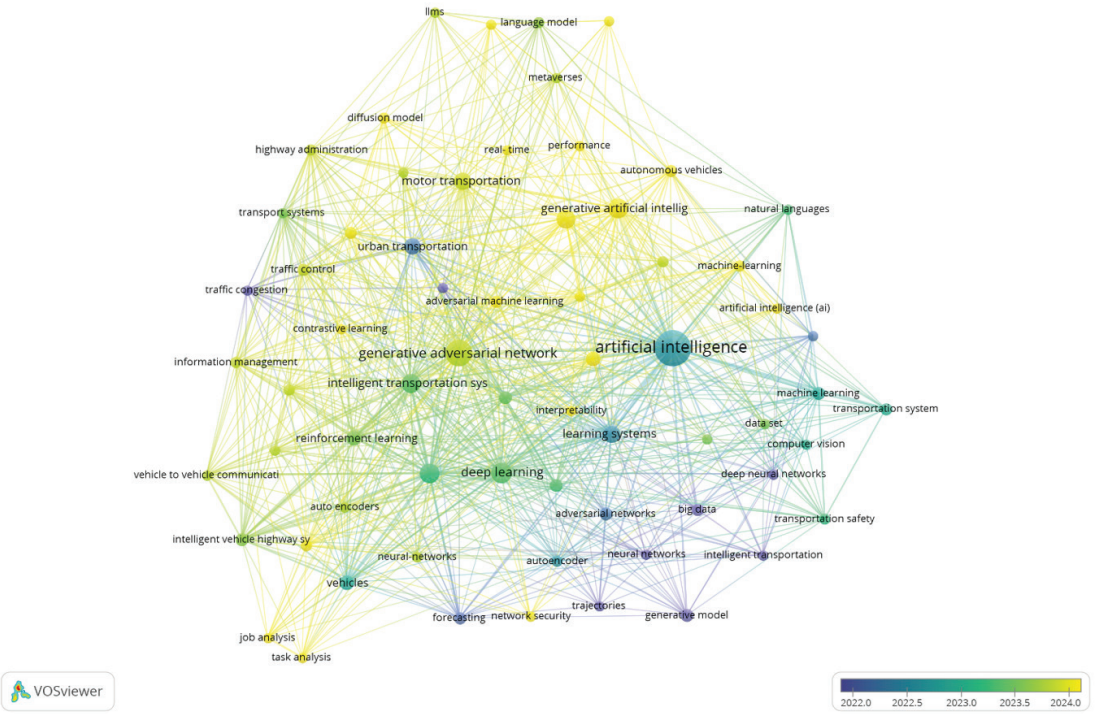


Figure 3: Overlay visualization of co-occurring keywords showing trends and possible gaps

5.4. The way forward to address these gaps

To address the gaps identified in the previous section of the report, several strategic actions must be taken.

Development of tailored security frameworks

A major gap in current research is the lack of explicit security frameworks designed specifically for generative AI in transportation. Given the unique vulnerabilities introduced by AI, particularly in adversarial attacks and data manipulation, it is essential to develop robust and adaptive security architectures. For instance, generative adversarial networks (GANs) could be used to simulate potential attack scenarios, helping to identify weaknesses in AI-driven systems before they are deployed. Companies like Tesla, which utilize AI in autonomous vehicles, are beginning to explore the need for more rigorous security measures to prevent attacks such as data poisoning, which could manipulate the vehicle's decision-making processes (Fu *et al.,* 2024). Therefore, future research should focus on creating security protocols that anticipate and counteract AI-specific vulnerabilities in transportation systems.

Strengthening data privacy and building trust

As generative AI models rely on vast amounts of data, the protection of this data is paramount. The absence of explicit mentions of "data privacy" and "trustworthy AI" in current research indicates a significant gap. To address this, future work should focus on strengthening data privacy measures to comply with regulations like the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the U.S. For example, using federated learning, where data remains decentralized, can help mitigate privacy risks by enabling AI models to learn from data without directly accessing it. This approach is already being tested by companies like Google, which applies federated learning in mobile devices to enhance privacy while improving machine

learning models. Implementing such privacy-preserving techniques will not only ensure legal compliance but also build public trust in AI applications in transportation.

Fostering explainability and interpretability in AI

The lack of explainability and interpretability is another critical gap in the application of generative AI in transportation. AI systems often operate as "black boxes" (Felder, 2021), making it difficult for operators to understand how decisions are made, which is problematic for safety-critical applications like autonomous driving. To enhance transparency, future research must focus on integrating Explainable AI (XAI) techniques that provide clear insights into the decision-making processes of AI models. For instance, in autonomous vehicles, operators and passengers must understand why a vehicle chose one route over another or how it responded to an obstacle. Companies like Waymo are exploring the integration of interpretable AI to ensure that autonomous vehicles' decision-making processes can be understood and audited. Developing these systems will increase accountability and help ensure the safety of AI-driven transportation networks.

Focusing on scalability and real-world deployment

While generative AI has demonstrated significant potential in controlled environments, scaling these solutions to work in real-world transportation networks remains a challenge. The scalability of AI-based security solutions must be tested in complex, large-scale transportation systems. For example, AI-driven traffic management systems, which optimize traffic flow in real-time, need to be capable of handling the vast number of variables present in urban settings, such as unpredictable traffic conditions, accidents, or weather. Cities like Singapore have successfully implemented AI-based traffic control systems that analyze traffic patterns in real-time and adjust signals to reduce congestion. Future research should aim to develop similar solutions that are not only effective in simulation but also capable of handling the complexity of real-world environments. This includes ensuring that AI systems are adaptable and reliable across different transportation infrastructures.

Encouraging interdisciplinary collaboration

The complexity of securing AI-driven transportation systems highlights the importance of interdisciplinary collaboration. Current research does not explicitly reflect the collaboration between AI researchers, transportation engineers, cybersecurity experts and policymakers, which is critical for creating widespread and practical security solutions. For example, the collaboration between AI experts and transportation authorities in the development of autonomous vehicle regulations is essential to address both technical and ethical concerns. A real-world example of such collaboration can be seen in the work of the U.S. Department of Transportation, which partners with various research institutions and private companies to shape policies that ensure the safety and security of autonomous vehicles. Encouraging collaboration across disciplines will help address the multifaceted challenges of securing AI-driven transportation systems.

6. Practical applicability of findings

The findings of this study provide key insights for private industry professionals engaged in the development, deployment and management of generative AI technologies in transportation networks. By focusing on the four key clusters obtained in this study, industry stakeholders can apply AI-driven solutions to enhance operational efficiency, improve safety and address emerging security challenges. Generative AI's potential in optimizing smart routing systems is particularly relevant for private companies working in traffic management and urban mobility solutions. AI-driven routing systems, powered by reinforcement learning and deep learning models, can dynamically adapt to changing traffic conditions, improving flow and reducing congestion. For example, companies like Waymo and Tesla are already integrating real-time traffic data into their autonomous

vehicle systems to optimize routing decisions. Private industry professionals can adopt similar AI-driven solutions to manage large-scale transportation systems, integrating generative AI into traffic signal systems or smart traffic lights to reduce wait times and increase traffic throughput. Also, AI can be used to predict traffic disruptions and suggest alternative routes for drivers, improving efficiency across urban transportation networks. This would be especially beneficial for large logistics and transportation companies such as FedEx and UPS, who rely heavily on efficient route optimization to manage their fleet operations.

The ability to simulate and predict traffic patterns is crucial for both urban planning and day-to-day traffic management. Industry professionals in transportation and logistics can leverage generative AI models to simulate traffic scenarios and predict congestion patterns, enabling proactive decision-making. For instance, AI models can predict peak traffic hours and advise cities or companies on how to manage traffic flows during those times. Companies like Google with their Google Maps application already utilize AI to forecast traffic conditions, but the potential for deeper integration with generative AI models remains largely untapped. Private industry professionals can use these insights to develop more accurate simulations of traffic flows in cities, allowing for better planning of infrastructure projects such as new roads or overpasses. These predictions could also be integrated into fleet management systems, helping companies like DHL or Amazon optimize delivery routes based on traffic predictions, saving time and reducing fuel costs.

With the increasing reliance on AI for transportation systems, ensuring cybersecurity is paramount. This study highlights the need for tailored security frameworks that address vulnerabilities specific to generative AI applications in transportation. For instance, Generative Adversarial Networks (GANs) could be used to simulate cyberattacks, helping companies identify vulnerabilities before they are exploited. Transportation management companies and smart city developers can leverage these techniques to create proactive, self-healing systems that automatically detect and mitigate potential cyber threats. A concrete example is Tesla's use of AI for autonomous driving, where constant software updates and vulnerability testing are crucial for maintaining system integrity. Professionals in the transportation sector can collaborate with cybersecurity experts to develop generative AI-driven security systems that predict and defend against potential attacks, protecting both the data and physical infrastructure of transportation networks. These models can also help detect malicious activities in real-time, allowing quick responses to cyber threats that could otherwise disrupt transportation operations.

The ability to make decisions quickly and accurately in real-time is vital for the efficient operation of transportation networks. Generative AI can enhance real-time decision support systems by analyzing massive amounts of data instantly and providing actionable insights. For example, in the context of autonomous vehicles, AI can be used to analyze traffic, weather and road conditions, and make real-time decisions that ensure safe and efficient operation. Uber and Lyft, for instance, rely heavily on AI to optimize ride-sharing routes in real-time. However, with the integration of generative AI, these companies can take this a step further by allowing their systems to adapt autonomously to unforeseen circumstances, such as accidents or road closures, in real-time. Public transportation providers can also use AI to adjust schedules, routes, and vehicle assignments based on real-time passenger demand, ensuring a seamless commuting experience for users. For large-scale operations, AI can assist in optimizing the deployment of resources during peak hours or emergencies, improving service delivery and customer satisfaction.

To fully harness the potential of generative AI in transportation networks, industry professionals must address several critical gaps highlighted in this study. Firstly, there is an urgent need for the development of security frameworks specifically designed to address generative AI-related vulnerabilities in transportation systems. This includes creating proactive and self-healing systems that can detect and mitigate potential cyber threats. Also, the industry must integrate consider-

ations around data privacy and trustworthy AI to ensure that the data-intensive nature of generative AI models does not compromise user privacy and the integrity of transportation systems. Additionally, explainable AI (XAI) needs to be a key focus. The lack of transparency in how AI systems make decisions is a significant challenge, especially in safety-critical applications like autonomous driving. Industry stakeholders must invest in making AI models more interpretable and transparent, ensuring that operators and regulators can understand the decision-making process. This will also help address public concerns around the accountability of AI-driven systems. Finally, there needs to be a stronger emphasis on real-world deployment and scalability. While AI models show great promise in simulations, real-world applications, especially at the scale required for large transportation networks, remain underexplored. Collaboration between AI researchers, transportation engineers, cybersecurity professionals and policymakers is essential to design robust and scalable solutions that can be effectively deployed in complex environments.

7. Conclusion

The main aim of this research is to explore the application of generative AI in enhancing security frameworks within transportation systems. Using a bibliometric analysis approach, the study reviewed existing literature and revealed key themes and research clusters, including smart routing and traffic control, traffic pattern simulation and prediction, transportation cybersecurity and intelligence and real-time decision support systems. Despite the growing interest in these areas, several critical gaps were identified, particularly around security frameworks, explainability, scalability and interdisciplinary collaboration.

Practically, the findings from this study can guide policymakers, technology developers and transportation network operators in making informed decisions about how to harness the potential of generative AI. For instance, addressing the security gaps related to generative AI's vulnerabilities, such as developing tailored security frameworks and enhancing real-time decision-making capabilities, can help reduce risks and improve system resilience. Additionally, advancing explainable AI (XAI) will be essential for building trust and ensuring that these technologies are not only effective but also transparent and accountable. The insights from this study can also inform future investments in AI-driven security solutions, including the development of more scalable and real-world deployable systems. Another key contribution of this study is the identification of the research gaps and the categorization of generative AI applications into specific clusters. This approach provides a more structured pathway to understanding the opportunities and possibilities in integrating AI technologies into transportation security. Industry professionals can benefit from this taxonomy by focusing on specific clusters that are most relevant to their operations. For example, a transportation company focusing on autonomous vehicles could prioritize cybersecurity and intelligence, while a smart city developer might focus on smart routing and traffic control. Researchers can also use this clusterization to design future studies that investigate the impact of generative AI on specific areas of transportation security and infrastructure resilience.

Looking ahead, future research efforts should address several key areas. First, empirical data collection will be crucial to validate the theoretical insights from this study and provide a real-world understanding of the challenges and benefits of implementing generative AI in transportation security. A mixed-methods approach combining surveys and case studies of organizations that have adopted AI-driven solutions could offer deeper insights into the practical implications of these technologies. Furthermore, exploring region-specific challenges and opportunities will allow for more targeted research. For example, the security needs of urban transportation networks may differ from those of rural or remote areas and understanding these distinctions will help in tailoring AI applications for different contexts. Additionally, future studies should explore the potential of generative AI in other under-explored areas, such as urban planning, smart city integration and

behavioral analysis. These areas have significant implications for enhancing overall transportation system efficiency and security, but they remain largely unexplored in the current body of literature. Addressing these gaps could open up new avenues for research and innovation that drive the next generation of intelligent transportation systems.

References

Aliu, J., & Oke, A. E. (2023). Construction in the digital age: exploring the benefits of digital technologies. Built Environment Project and Asset Management, 13(3), 412-429. https://doi.org/10.1108/BEPAM-11-2022-0186

Bathla, G., Bhadane, K., Singh, R. K., Kumar, R., Aluvalu, R., Krishnamurthi, R., ... & Basheer, S. (2022). Autonomous vehicles and intelligent automation: Applications, challenges, and opportunities. *Mobile Information Systems*, *2022*(1), 7632892. https://doi.org/10.1155/2022/7632892

Felder, R. M. (2021). Coming to terms with the black box problem: how to justify AI systems in health care. *Hastings Center Report*, *51*(4), 38-45. https://doi.org/10.1002/hast.1248

Fu, T., Sharma, M., Torr, P., Cohen, S. B., Krueger, D., & Barez, F. (2024). PoisonBench: Assessing Large Language Model Vulnerability to Data Poisoning. *arXiv preprint arXiv:2410.08811*. https://doi.org/10.48550/arXiv.2410.08811

Hamdan, A., Ibekwe, K. I., Ilojianya, V. I., Sonko, S., & Etukudoh, E. A. (2024). AI in renewable energy: A review of predictive maintenance and energy optimization. *International Journal of Science and Research Archive*, *11*(1), 718-729. https://doi.org/10.30574/ijsra.2024.11.1.0112

Jabbar, R., Dhib, E., Said, A. B., Krichen, M., Fetais, N., Zaidan, E., & Barkaoui, K. (2022). Blockchain technology for intelligent transportation systems: A systematic literature review. *IEEE Access*, *10*, 20995-21031. https://10.1109/ACCESS.2022.3149958

Jeihani, M., Ansariyar, A., Sadeghvaziri, E., Ardeshiri, A., Kabir, M. M., Haghani, A., & Jones, A. (2022). Investigating the effect of connected vehicles (CV) route guidance on mobility and equity. URL : https://rosap.ntl.bts.gov/view/dot/60931

Jihong, X. I. E., & Xiang, Z. H. O. U. (2024). Edge Computing for Real-Time Decision Making in Autonomous Driving: Review of Challenges, Solutions, and Future Trends. *International Journal of Advanced Computer Science & Applications*, *15*(7). 10.14569/IJACSA.2024.0150759

Krishnan, S. R., Nallakaruppan, M. K., Chengoden, R., Koppu, S., Iyapparaja, M., Sadhasivam, J., & Sethuraman, S. (2022). Smart water resource management using Artificial Intelligence—A review. *Sustainability*, *14*(20), 13384. https://doi.org/10.3390/su142013384

Lieberthal, E. B., Serok, N., Duan, J., Zeng, G., & Havlin, S. (2024). Addressing the urban congestion challenge based on traffic bottlenecks. *Philosophical Transactions A*, *382*(2285), 20240095. https://doi.org/10.1098/rsta.2024.0095

Loske, D., & Klumpp, M. (2021). Intelligent and efficient? An empirical analysis of human–AI collaboration for truck drivers in retail logistics. *The International Journal of Logistics Management*, *32*(4), 1356-1383. https://doi.org/10.1108/IJLM-03-2020-0149

Malathi, D., Alaswad, F., Aljaddouh, B., Ranganayagi, L., & Sangeetha, R. (2025, January). AI-Powered Traffic Management: Improving Congestion Detection and Signal Regulation. In *2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)* (pp. 899-904). IEEE. http://doi.org/10.1109/ICMSCI62561.2025.10894186

Plathottam, S. J., Rzonca, A., Lakhnori, R., & Iloeje, C. O. (2023). A review of artificial intelligence applications in manufacturing operations. *Journal of Advanced Manufacturing and Processing*, *5*(3), e10159. https://doi.org/10.1002/amp2.10159

Qayyum, A., Usama, M., Qadir, J., & Al-Fuqaha, A. (2020). Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward.

IEEE Communications Surveys & Tutorials, *22*(2), 998-1026. https://doi.org/10.1109/COMST.2020.2975048

Sajovic, I., & Boh Podgornik, B. (2022). Bibliometric analysis of visualizations in computer graphics: a study. *Sage Open*, *12*(1), 21582440211071105. https://doi.org/10.1177/2158244021107110

Yan, H., & Li, Y. (2023). A survey of generative ai for intelligent transportation systems. *arXiv preprint arXiv:2312.08248*. https://doi.org/10.48550/arXiv.2312.08248

Zeb, S., Nizamullah, F. N. U., Abbasi, N., & Fahad, M. (2024). AI in healthcare: revolutionizing diagnosis and therapy. *International Journal of Multidisciplinary Sciences and Arts*, *3*(3), 118-128. https://doi.org/10.47709/ijmdsa.v3i3.4546

Zhao, F., Fashola, O. I., Olarewaju, T. I., & Onwumere, I. (2021). Smart city research: A holistic and state-of-the-art literature review. *Cities*, *119*, 103406. https://doi.org/10.1016/j.cities.2021.103406

Author Biography

John Aliu, PhD, is currently a Clinical Assistant Professor with the Engineering Education Transformations Institute, College of Engineering, University of Georgia, Athens, Georgia. He has authored and co-authored several publications in top journals in the field of construction digitalization, sustainable construction and engineering education. John is a regular reviewer for different peer-reviewed journals, including the *Journal of Cleaner Production, Engineering, Construction and Architectural Management, Sustainable Development Journal, Frontiers in Built Environment, International Journal of Sustainability in Higher Education, Construction Economics and Building, African Journal of Science, Technology, Innovation and Development, Journal of Construction in Developing Countries, Journal of Engineering, Design and Technology, Journal of Construction Project Management and Innovation, International Journal of Construction Management, Journal of Construction Engineering and Management, Cogent Economics and Finance, Built Environment Project and Asset Management*, and others. He is currently an Associate Editor of ASCE'S *Journal of Civil Engineering Education*.

Suggested citation: **Aliu, J.** (2025). Generative AI for advanced security frameworks in transportation networks. *One Step Ahead*, *July 2025*, 50–65. The Sam Houston State University Institute for Homeland Security. OSF | Generative AI for Advanced Security Frameworks in Transportation Networks

AI ASSISTANT COMPARATIVE RISK ASSESSMENT FOR HOMELAND SECURITY THREATS

Russell Lundberg

Abstract

Comparative risk rankings are essential for homeland security planning, helping allocate resources, shape policy, and improve preparedness. Traditional methods like the Deliberative Method for Ranking Risk (DMRR) provide structured comparisons but are time-intensive and require expert coordination. This study evaluates whether artificial intelligence (AI), particularly large language models (LLMs), can approximate structured risk ranking methods and produce results comparable to established benchmarks.

AI-generated rankings were tested against DMRR, public perception surveys, and quantitative analytical models to assess their reliability. When provided with structured inputs and appropriate oversight, AI's rankings aligned closely with human-driven methodologies, demonstrating its potential to streamline risk assessment. However, AI's sensitivity to input structure and occasional inconsistencies highlight the need for careful implementation.

AI is not a replacement for human judgment but can serve as a scalable decision-support tool to enhance homeland security risk assessment. By integrating AI into structured frameworks, practitioners can accelerate risk ranking processes while maintaining analytical rigor.

1. Introduction and Overview

Comparative risk rankings are essential for effective homeland security planning. Agencies allocate resources, develop policies, and prepare response strategies based on perceived risk. If risk rankings are inconsistent or based on intuition rather than analysis, they may lead to poor decisions. A structured process is necessary to ensure that rankings reflect informed judgment rather than instinct.

Comparing homeland security risks is difficult because threats vary widely in nature, likelihood, and consequence. Some, like pandemics, primarily affect public health. Others, like cyberattacks, target infrastructure. Some, like terrorist nuclear detonations, could cause catastrophic physical, economic, and psychological harm, but they have never happened, making their likelihood uncertain. These differences make direct comparison hard. Decision-makers must weigh trade-offs—how much economic damage is equal to loss of life or environmental destruction? Since these involve subjective value judgments, human input is necessary.

A structured process is needed to make risk rankings more consistent and useful. The Deliberative Method for Ranking Risk (DMRR) was designed to improve risk assessments by structuring human judgment. (Lundberg & Willis, 2016) This method requires individuals to rank risks, justify their rea-

soning, and refine their assessments through structured discussion. It reduces bias and produces more defensible rankings. However, DMRR is slow. A full session can take hours, and scheduling a group of experts may take weeks. This makes it resource intensive to use in decision-making.

Artificial intelligence (AI) could speed up this process. The Department of Homeland Security (DHS) already uses AI for cybersecurity, threat detection, and emergency response. Most of these systems rely on structured data and predefined algorithms. But risk ranking is different. It requires processing complex, unstructured information and making reasoned comparisons across very different types of threats. Large language models (LLMs), such as ChatGPT-4, may be well-suited for this task. Unlike traditional AI, LLMs analyze qualitative and quantitative data, generate logical responses, and adjust their reasoning based on structured prompts. If LLMs can replicate structured human judgment, they could provide a scalable tool for comparative risk assessment.

This study examines the use of artificial intelligence in comparative risk ranking in multiple ways. It tests whether an LLM can approximate or improve upon the deliberative method for ranking risks by evaluating AI-generated rankings under different conditions. It also explores how AI rankings shift as more structured information is added and whether AI produces consistent, reliable results. The goal is to determine whether AI can serve as a decision-support tool for homeland security professionals—not replacing human judgment but providing a structured, scalable way to supplement traditional risk assessments.

2. Problem Statement

2.1 The Need for Comparative Risk Ranking in Homeland Security

Homeland security professionals must make critical decisions about how to allocate resources, develop policies, and prioritize response strategies in the face of diverse threats. These decisions rely on comparative risk rankings, which allow planners to determine which threats require the most immediate attention and investment. Without structured risk comparisons, agencies may misallocate resources, underestimating high-impact threats or over-preparing for lower-priority risks. Effective planning depends on ensuring that risk rankings are consistent, justifiable, and based on structured reasoning rather than instinct or political pressure.

If risk rankings are inconsistent, intuition-driven, or based on limited data, decision-making can become fragmented and ineffective. Different stakeholders may prioritize risks based on individual experience, media influence, or recent high-profile events, rather than long-term strategic concerns. This can lead to reactive rather than proactive planning, where resources are directed toward recent or emotionally salient threats rather than those with the greatest potential impact. To ensure that risk rankings support sound policy and operational decision-making, a structured and repeatable approach is necessary.

Homeland security risks vary widely in nature, likelihood, and consequence. A pandemic and a cyberattack may both be high-risk events, but their impacts and mitigation strategies are vastly different. A nuclear terrorist attack, while unlikely, could cause catastrophic harm, while an oil spill may have a significant but localized environmental and economic impact. Because these risks differ so greatly, comparing them requires a method that accounts for their unique characteristics while still enabling decision-makers to prioritize effectively.

Human decision-making in risk ranking is influenced by two cognitive processes—System 1 and System 2 thinking. (Kahneman, 2011) System 1 thinking is fast, intuitive, and based on heuristics, while System 2 thinking is deliberate, analytical, and structured. Public perception surveys, such as those conducted through the American Life Panel (ALP) and Amazon Mechanical Turk (MTurk), capture instinctual, System 1-driven risk perceptions. These methods reflect how people feel about

risks rather than an analytical evaluation of their actual impact or likelihood. In contrast, structured deliberation methods like the Deliberative Method for Ranking Risk (DMRR) aim to engage System 2 thinking, forcing participants to reflect on and justify their rankings based on structured criteria. (Florig et al., 2001) The challenge lies in ensuring that homeland security risk rankings are based on structured analysis rather than intuitive or emotionally driven responses.

Existing risk ranking methods each have limitations that impact their usefulness for homeland security decision-making. DMRR is effective but slow, requiring expert coordination, extensive deliberation, and multiple rounds of analysis to refine rankings. (Lundberg & Willis, 2016) While this produces high-quality, structured results, it is time-intensive and difficult to scale.

Public perception methods, such as ALP and MTurk surveys, provide a faster way to gauge how the general population perceives risk. (Lundberg & Willis, 2019) However, these methods often reflect emotional responses, recent news cycles, or biases rather than an objective evaluation of likelihood and consequence. They lack the depth needed for strategic decision-making and can lead to rankings that do not align with actual security priorities.

Purely quantitative approaches, such as Principal Component Analysis (PCA), provide consistency by ranking risks based on numerical attributes rather than human judgment. (Lundberg, 2025) While this ensures repeatability and objectivity, it does not incorporate qualitative insights or the nuanced trade-offs that experts consider in real-world decision-making. As a result, purely quantitative methods alone may not fully capture the complexities of homeland security risks.

Artificial intelligence (AI) presents an opportunity to speed up and enhance structured risk ranking processes while maintaining analytical rigor. By processing large amounts of structured and unstructured data, AI has the potential to replicate structured human decision-making, reduce bias, and improve the efficiency of risk assessments. AI-assisted approaches may help bridge the gap between time-consuming expert deliberation and overly simplistic public perception rankings, offering a scalable solution for homeland security planning. However, ensuring that AI is used effectively and with proper oversight is essential to maintaining accuracy, transparency, and reliability in risk ranking processes.

2.2 AI's Potential for Comparative Risk Ranking

Artificial intelligence is widely used in homeland security across threat detection, cybersecurity, emergency response, and intelligence analysis. AI-powered surveillance systems analyze video feeds to detect anomalous behavior, unattended objects, or unauthorized access in secured areas. (DHS, 2024) In cybersecurity, AI monitors networks for malware, phishing attempts, and insider threats, allowing for rapid response to cyberattacks. AI-driven predictive models help emergency management agencies anticipate natural disasters, optimize resource distribution, and improve evacuation planning. In intelligence operations, AI assists in processing vast amounts of data from communications, social media, and other sources to identify emerging threats. As AI technology evolves, its role in proactive security measures and crisis management continues to grow.

More recently, AI has been used in risk assessment of individual hazards, helping analysts estimate potential impacts, assess vulnerabilities, and model threat scenarios. (Afzal et al., 2019; Chan, 2023; Faheem, 2021) AI-driven tools have been applied to areas such as disaster preparedness, infrastructure resilience, and cybersecurity risk modeling, where they process large datasets to detect patterns and forecast emerging threats. Machine learning algorithms assist in identifying weaknesses in critical systems, simulating potential attacks, and improving emergency response planning.

While AI has proven useful in assessing risks in isolation, its application in comparative risk ranking has been limited. Comparing homeland security risks is particularly difficult due to the wide variation in risk types and the inherent subjectivity involved in weighing different kinds of harm. Because risk ranking often requires value judgments about economic, environmental, and human costs, AI's role in structured, multi-risk assessment remains an area of ongoing exploration. Artificial intelligence may offer an alternative to human-driven comparative risk assessment. Large language models (LLMs), such as ChatGPT-4, can process complex, unstructured information, recognize patterns across multiple domains, and generate structured reasoning. Because LLMs are trained on vast amounts of public information—including news articles, academic papers, and online discussions—they may reflect public perceptions to some extent when assessing risks. If properly guided, LLMs could follow structured processes like DMRR, making them a potential tool to assist in comparative risk assessment. While AI cannot remove the need for value judgments.

3. Topic Discussion: AI's Strengths and Weaknesses in Risk Ranking

3.1 How We Examine the AI at Ranking Risks

The ability of an AI to conduct a comparative risk ranking will be considered in several parts. Florig et al. describe a five-step process for the DMRR, although it would also hold for other risk rankings. The first two steps involve conceptualizing the risk, deciding what to describe and how to describe it. The third step involves applying those concepts to describe the selected risks. The fourth step involves determining the comparative ranking. The fifth step involves reporting the ranking results. This research will consider two different parts of this process: can the AI describe the risks individually and can the AI compare the individual risks?

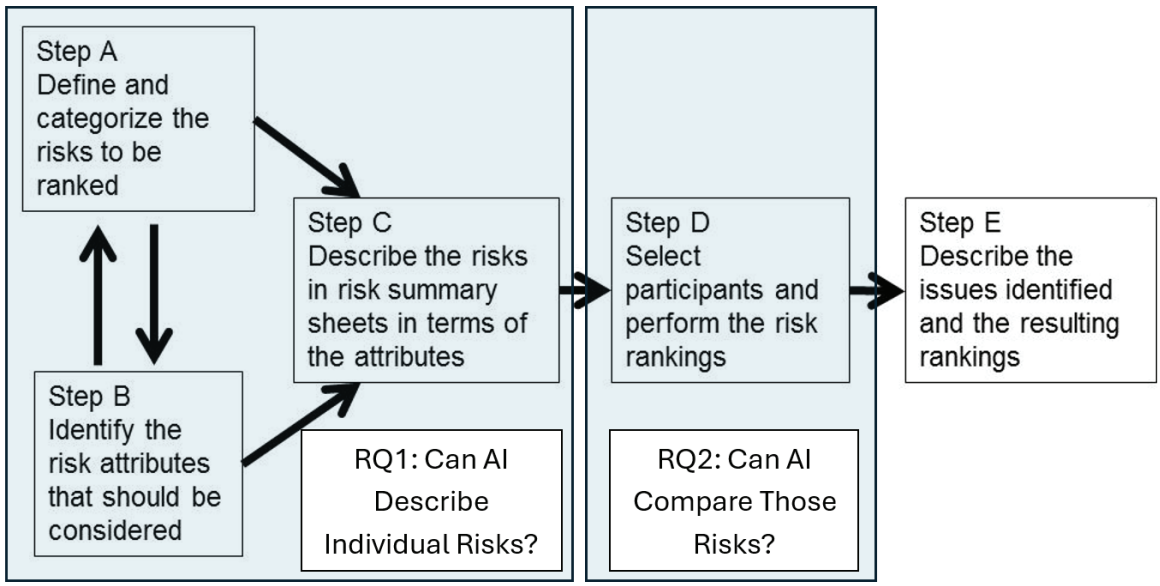


Figure 1- Analytical Steps Drawn from the Deliberative Method for Ranking Risks (Adapted from Florig et al, 2001)

The decision was made to categorize the risks at the hazard level. This is the equivalent of step A, and it was done by people rather than AI. Comparative risk rankings often serve a purpose and the items to be ranked naturally follow that purpose. Comparing risks at the hazard level is not the only choice but it is a common approach for strategic decision-making (such as in the Quadrennial Homeland Security Review).

The rest of the process steps B through D were tested using ChatGPT 4o. This model was chosen as it was at the time the baseline model from OpenAI, a foremost AI company. All analyses were done in early February 2025.

3.2 AI Did Not Create a Comparable Set of Attributes

The AI was asked to identify a set of attributes to be considered in two ways. First, it was asked to do so directly with a prompt that provided minimal guidance. The prompt told the AI that these attributes would be used to describe a set of homeland security hazards that vary in kind and consequence, including risk from intentional adversaries, accidentally caused human risks, and natural disasters. The AI was further asked to draw on the literature on risk perception to provide a list of attributes that can be used to describe the hazards in a way that is both comprehensive and parsimonious.

This prompt resulted in a list of attributes on the following subjects: likelihood, consequence, risk perception, intentionality, systematic impact and recovery, and data. This list has several strengths: it recognizes both consequence and non-consequence aspects of concern, accounts for both likelihood and consequence, and acknowledges uncertainty as a key factor in risk assessment. However, there are some issues as well. Jenni suggests that a good risk attribute should be justifiable, clearly defined, and measurable. (Florig et al., 2001; Jenni, 1997) Many of the attributes here do not fully meet these criteria, as some are vague, difficult to quantify, or missing aspects that people care about. This limits their usefulness for systematic human risk ranking.

A second way that the AI was given an opportunity to identify attributes of concern was in an unstructured prompt for assessing an individual risk. As noted in the next section, the AI was prompted to assess the risk of hurricanes and given only minimal guidance that it be for a homeland security hazard, that it reflect the concerns of the U.S. as a whole, and that it reflect the risks over the next year. This led the AI to create a list of attributes of concern, but it was an even more limited list of attributes than the previous set. As it was not explicitly guided to consider the risk perception literature, it did not, and its attention was more on the risk at hand than on the attributes to describe that risk.

These results suggest that AI requires strong guidance when identifying attributes of concern, as the range of possible attributes is vast. As Keeney and von Winterfeldt have described, there are many possible attributes to describe homeland security risks and structuring decision problems involves carefully selecting attributes that capture what matters most. (Keeney & von Winterfeldt, 2011) Without explicit direction, the AI struggles to balance comprehensiveness with parsimony and may overlook key aspects of concern. This highlights the need for well-crafted prompts that not only specify the scope of analysis but also guide the AI toward attributes that are justifiable, clearly defined, and measurable.

3.3 AI Can Create Useful Risk Assessments of Individual Hazards

AI can generate structured risk assessments when properly guided. To test this, the AI was first asked to assess the risk of hurricanes, a hazard for which a detailed manual assessment already existed. When given an unstructured prompt, the AI produced a reasonable but incomplete assessment, focusing on broad impacts but lacking the specific attributes necessary for homeland security decision-making.

However, the AI was then provided with a structured prompt that reflected 17 key attributes that were identified in previous studies to describe homeland security risks. These attributes were used for two reasons. First, this list was developed to be justified, specifically defined, and measurable, meeting the criteria for a good set of attributes. Second, the use of this list of attributes in previous

studies would make the resulting rankings more comparable to human-based rankings developed earlier. This comparison will be an important part of analyzing the results of the rankings.

When the AI was prompted to not only be concerned about the risk to the nation as a whole and use the annualized expected value of risk over the next year but also to use the 17 selected attributes with consideration of low, best and high values when possible, the results closely matched the human-produced analysis (see Table 1). While the numerical estimates were not identical, they overlapped within error bounds, demonstrating that AI could approximate structured human evaluations.

Table 1: Human and AI Assessments of Hurricane Risk Provide Similar Results

Hurricanes	**Lundberg 2013**			**AI**		
Average Deaths	10	40	60	10	75	300
Greatest Deaths	2,000-4,000			Up to 8,000		
Average More Severe Injuries	200	600	1,000	100	500	5000
Average Less Severe Injuries	400	1,000	2,000	200	2000	15000
Psychological Damage	High			Moderate		
Average Economic Damage	$2B	$10B	$20B	$10B	$30B	$100B
Greatest Economic Damage	$60-200B			Up to $300B		
Duration of Economic Damage	Months to years			Months to years		
Size of Area Affected by Economic Damage	Counties to states			City-to multi-state region		
Average Environmental Damage	High			Moderate		
Average Individuals Displaced	10,000-100,000			20,000-300,000		
Disruption of Government Operations	Moderate to High			Moderate to High		
Natural/Human-Induced	Natural			Natural		
Ability to Control Exposure	High			Moderate		
Time between Exposure and Health	Immediate up to years			Hours to days		
Quality of Scientific Understanding	Moderate to high			High		
Combined Uncertainty	Low			Moderate		

One possibility considered is that the AI results were similar to the human results because perhaps the AI had been trained on the human estimate, as it was published at the time of the training. To examine this possibility, the AI was prompted to repeat the process for two additional hazards that were not a part of the original hazard sheets: a sarin gas release (intentional) and a wildfire (natural). In both cases, the AI-generated assessments appeared plausible and followed logical risk characterization patterns.

This suggests that while AI needs guidance in structuring its risk assessments, it can effectively support risk assessment for a variety of homeland security threats. This ability to quickly generate structured risk assessments could significantly aid planning and preparedness efforts, though human oversight remains essential.

3.4 AI Can Conduct Complex Comparative Risk Rankings

In this section, the AI was asked to rank a set of 10 homeland security risks. This set of risks was selected to be consistent with previous studies of human risk ranking for purposes of comparison.

(Lundberg & Willis, 2015) The risks were initially selected to cover the range of homeland security concerns: risks that are natural, intentional, and accidental; risks that are common, rare, and completely novel; risks with small, medium, and large consequences and consequences along several different dimensions. (See Table 3.)

Table 2- Ten Selected Homeland Security Hazards

Natural	Terrorist	Accidental
Earthquakes	Nuclear detonation	Toxic industrial chemicals
Hurricanes	Explosive bombings	Oil spills
Tornadoes	Anthrax attacks	
Pandemic influenza	Cyber-attacks on critical infrastructure	

ChatGPT was prompted to provide a ranking of the ten hazards from the hazard of most concern to the hazard of least concern. This ranking was done under several scenarios using increasing levels of information. The least informed case asked the AI to rank the risks based only on the name of the risk while the DMRR-AI was the most informed case. An additional test was done to see if the name itself would alter the rankings—both condition 3 and 4 were done with information from the attribute table with the only difference whether the name of the hazard was included. These ranking conditions included:

1. Risk name only.
2. Risk name with a short paragraph summary.
3. Risk name with an attribute table of 17 structured factors.
4. Attribute table without risk name.
5. Risk name with a four-page summary of the hazard.
6. Deliberative Method for Ranking Risk (DMRR-AI).

The Deliberative Method for Ranking Risk adapted for AI (DMRR-AI) represents the most guided of the conditions. All the rest involve only a single prompt but the DMRR has several steps which were adapted for the DMRR-AI. These steps involve:

1. An initial ranking
2. A ranking of the attributes used to describe the hazards, which is used to create a calculated ranking of the risks.
3. A consideration of the difference between the initial ranking and calculated ranking to inform a revised ranking
4. A group discussion, which in the DMRR-AI will be simulated with “participants” with different “perspectives”, resulting in a group ranking
5. A final ranking informed by all the steps that have come before it.

The script for this adapted DMRR-AI is provided in the appendix.

Each ranking condition was run 10 times to evaluate the AI’s consistency and variability. The primary outcome examined was a ranking of the hazards. The standard deviation of the rankings for each hazard under each condition was also examined as a secondary outcome measure.

Due to the inherent subjectivity of the risk assessments, it is hard to say that one ranking is better than another. However, we can assess the AI’s performance in comparison to established

risk ranking methods that have been used in previous homeland security studies. These methods include:

- Deliberative Method for Ranking Risk (DMRR): A structured human-driven approach where experts iteratively refine rankings through deliberation and trade-off analysis. (Lundberg & Willis, 2016)
- Two Public Perception Surveys—the American Life Panel (ALP) and a survey done in Amazon Mechanical Turk (MTurk): Surveys capturing instinctual, System 2 thinking from the general public. (Lundberg & Willis, 2019)
- Principal Component Analysis (PCA): A quantitative approach ranking risks based solely on numerical attributes, without human judgment. (Lundberg, 2025)

AI's rankings will be compared across results from these methods to determine how closely its outputs align with structured human decision-making versus public perception or analytical models. Comparisons will focus on ranking correlations across different input conditions and will evaluate whether AI can replicate structured risk assessment approaches when properly guided.

The study also qualitatively examined how consistently AI follows the structured ranking process and whether it responds to prompts as intended. This is particularly relevant in the DMRR-AI process, where intermediate steps allow for closer evaluation of how AI processes new information and justifies its ranking decisions. By analyzing both AI's outputs and its explanations, this research assessed whether AI's decision-making is stable, logical, and aligned with the given structure—or if inconsistencies or unexpected shifts emerge.

These rankings took place in early February 2025 using OpenAI's ChatGPT 4o, a standard non-reasoning model available at the time.

3.4.1 AI's Efficiently Created Comparable Risk Rankings

AI was able to generate comparative risk rankings across multiple approaches, demonstrating its ability to process complex assessments regardless of the input structure.

We cannot determine whether AI's rankings were "correct"—as risk assessment inherently involves value judgments—but rankings of the AI were consistent with those made by humans using their own judgment frameworks. This suggests that AI can engage in comparative decision-making in a structured way, aligning with human reasoning when provided with the appropriate inputs. Table 3 shows the rankings under each condition, and as we will discuss, these rankings correlate with human rankings to a sizable extent.

Table 3- Rank of Hazards across Multiple Approaches of Increasing Information

	Name Only	Name and Summary	Name and Table	Full Description	DMRR-AI
1	Pandemic flu	Terrorist nuke	Pandemic flu	Pandemic flu	Terrorist nuke
2	Cyber on CI	Pandemic flu	Terrorist nuke	Hurricane	Pandemic flu
3	Terrorist nuke	Cyber on CI	Hurricane	Terrorist nuke	Earthquake
4	Hurricane	Hurricane	Earthquake	Cyber on CI	Hurricane
5	Earthquake	TIC	Cyber on CI	Earthquake	Anthrax attack
6	TIC	Earthquake	TIC	Anthrax (tie)	Cyber on CI
7	Bomb (tie)	Anthrax attack	Anthrax attack	Bomb (tie)	Tornado
8	Anthrax attack	Bomb (tie)	Bomb (tie)	TIC	Bomb (tie)
9	Tornado	Tornado	Tornado	Oil spill	TIC
10	Oil spill	Oil spill	Oil spill	Tornado	Oil spill

The rankings of the AI varied from session to session. Human rankings also vary, and the variance of the AI rankings was actually smaller than the human variance in previous studies. However, variability in ranking is not inherently good or bad—some homeland security risks, such as the likelihood of a terrorist nuclear detonation in the next decade, involve extreme uncertainty. In such cases, consistency does not necessarily mean accuracy. While AI may provide a more stable baseline than individual human rankings, we cannot say whether this smaller variance is "better".

However, there is no denying that the AI completed risk rankings far faster than traditional human deliberation methods while producing results that aligned well with structured human assessments such as DMRR and PCA. The human rankings took weeks to prepare and execute while the AI results took minutes (in the simplest ranking conditions such as name only) to hours (in the full execution of the DMRR-AI.) This suggests that AI can function as a scalable decision-support tool, though careful oversight is required to ensure its outputs remain both valid and unbiased.

3.4.2 AI's Rankings Depend on Input Structure

AI's risk rankings are not fixed but shift depending on how information is presented. When given minimal information—such as just the name of a risk or a brief summary—AI's rankings closely resembled public perception surveys like those conducted through the American Life Panel (ALP) and Amazon Mechanical Turk (MTurk). These methods capture instinctual, System 2 thinking, where individuals rely on general impressions rather than detailed analysis. This suggests that, in the absence of structured data, AI defaults to a ranking style similar to broad public sentiment rather than expert-driven risk assessments.

However, when AI was provided with detailed structured inputs, such as attribute tables or prompts modeled after the Deliberative Method for Ranking Risk (DMRR), its rankings aligned more closely with analytical methods such as DMRR and Principal Component Analysis (PCA). This shift indicates that AI does not inherently rank risks analytically but can be guided toward structured reasoning through well-designed prompts.

One of the most significant findings was that removing risk names from the input made AI rankings significantly more analytical. When risk names were included alongside structured attributes, AI's correlation with DMRR was 0.56, and with PCA, 0.75. However, when risk names were removed, these correlations jumped to 0.81 and 0.94, respectively. This suggests that AI, like humans, is anchored by intuitive associations with risk names, leading to rankings that reflect general expectations rather than structured analysis. By removing risk names, AI was forced to rely only on numerical attributes and structured information, producing rankings that more closely aligned with expert-driven methods.

This finding highlights the importance of carefully structuring AI inputs for risk ranking. If AI is used without structured guidance, its outputs may reflect public intuition rather than analytical decision-making. However, when properly prompted—and when risk names are excluded—AI can approximate expert-driven assessments, making it a valuable tool for structured risk evaluation.

3.4.3 AI Can Exhibit Unexpected Instability

AI's approach to structured risk ranking was not entirely stable over time, demonstrating unexpected shifts in reasoning and methodology. During initial tests of the Deliberative Method for Ranking Risk (DMRR) with AI (DMRR-AI), the AI's rankings remained unchanged throughout the process. When questioned, the AI explicitly stated that it had rejected new information from subsequent stages, believing its initial ranking to be superior. However, in tests conducted a week later, this behavior changed—AI now adjusted its rankings based on new inputs and acknowledged

doing so. This shift serves as a reminder that AI models are constantly evolving, and assessments made at one point in time should be tested for consistency if used in decision-making.

Beyond these process changes, AI also displayed unexplained shifts in specific rankings. In later DMRR-AI sessions, a single risk jumped three spaces in the final ranking without any new information. Notably, both the AI's most recent individual ranking and the simulated group ranking had placed this risk lower, yet it still moved up in the final ranking. This suggests that AI may sometimes introduce opaque, unexplainable reasoning into its decision-making.

These findings highlight the need for expert oversight when using AI for risk ranking. While AI rankings may appear structured, they can be unstable and influenced by unknown internal mechanisms. If AI is used for real-world decision-making, practitioners should verify consistency across multiple runs and ensure that unexplained shifts do not distort risk assessments.

4. Way Forward

The findings from this study suggest that AI can be a valuable decision-support tool in homeland security risk ranking, but its use must be carefully structured, validated, and integrated into broader risk assessment frameworks. While AI demonstrates the ability to approximate structured human rankings and process risk attributes efficiently, it also exhibits instabilities, biases, and sensitivity to input structure. This section outlines practical recommendations for practitioners to effectively incorporate AI into homeland security risk assessment while ensuring that its limitations are accounted for.

4.1 Current AI Should Be a Decision-Support Tool, Not a Replacement for Human Judgment

Practitioners should treat AI as an enhancement to risk assessment, not as a standalone solution. While AI can accelerate comparative risk ranking, it lacks human judgment, contextual understanding, and the ability to navigate deep uncertainties. Practitioners should use AI as an initial ranking tool, then refine results with human deliberation.

Recommendations for Use of AI in Risk Ranking:

- AI should be used to supplement human deliberation, identifying patterns and structuring information, but final decisions should rest with trained experts.

4.2 AI Can Provide Individual Risk Assessments as Inputs to Risk Ranking When They Are Structured

Before engaging in comparative risk ranking, AI can be used to generate structured assessments for individual risks, ensuring that rankings are based on clear, consistent, and analytically rigorous inputs. AI can process available data to describe specific threats using a standardized set of attributes, allowing for direct comparison across different hazards. These structured assessments serve as the foundation for comparative risk ranking.

Recommendations for AI-generated individual risk assessments:

1. Use a structured attribute-based approach. AI assessments should be based on a predefined set of attributes to ensure consistency across hazards. A 17-attribute framework provides a comprehensive yet manageable way to structure risk descriptions.
2. Ensure attributes capture both consequence attributes (e.g., loss of life, economic damage, environmental impact) and non-consequence attributes (e.g., voluntariness, intentionality). Additionally, the deep uncertainties of homeland security risks should be

included using low/high estimates as well as best estimates, qualitative levels instead of quantitative estimates, and estimates of overall uncertainty.

3. Be clear on qualitative scale guidelines. Many attributes require qualitative scales (e.g., "low," "moderate," "high" for severity or likelihood). It is critical to define clear guidelines for these categories to avoid inconsistencies or AI misinterpretation. If possible, anchor scales to real-world examples to ensure clarity and reliability.
4. Validate AI-generated assessments against expert-developed risk descriptions. AI should be used as a first draft generator, but its outputs should be reviewed and adjusted by experts to ensure accuracy and relevance before being used in comparative risk ranking.

Once structured individual risk assessments are established, they can serve as inputs to a comparative ranking process, ensuring that AI ranks risks based on consistent and analytically sound descriptions.

4.3 Structuring AI Inputs Give More Analytical Comparative Risk Rankings

AI's rankings are highly dependent on input structure. Practitioners must be mindful of how information is provided to AI systems to ensure valid and meaningful outputs.

Recommendations for structuring AI inputs in comparative risk ranking:

1. Use a structured approach to framing risks. AI produces more reliable rankings when it receives detailed, multi-attribute descriptions of risks rather than broad, unstructured prompts.
2. Avoid relying solely on risk names. Removing risk names and focusing on structured attribute data leads to more analytical AI rankings, reducing bias from name-based associations.
3. Ensure AI incorporates a range of consequence and non-consequence attributes. A 17-attribute framework provides a balanced and parsimonious way to describe homeland security risks while ensuring consistency across assessments.
4. Use established frameworks for AI input. Two effective approaches include:
    - The DMRR-AI script (detailed in the appendix), which simulates a structured deliberative process.
    - A table of attributes without the risk name attached, which allows AI to rank risks based purely on numerical and descriptive factors rather than preconceived associations.

By following these structured input approaches, practitioners can ensure that AI-generated rankings align more closely with analytical risk assessments rather than instinctual or biased judgments.

4.4 Multiple Sessions are Needed to Reduce AI's Instability and Variability

One challenge in using AI for risk ranking is its variability between sessions and occasional unexplained ranking shifts. While AI was found to be more stable than individual human rankings, unexplained movements in ranking without new information indicate that AI's decision-making process is sometimes opaque.

Recommendations for practitioners:

- Run multiple AI sessions and average rankings to identify stable patterns and reduce the risk of one-off anomalies.

- Use AI as a preliminary tool to structure discussions but involve human analysts to review and adjust rankings when inconsistencies arise.

4.5 AI's Role in Risk Communication and Policy Development

AI-generated risk rankings could have applications beyond internal assessments, including risk communication and policy discussions. However, using AI for external decision-making comes with additional challenges, as AI-generated insights could mislead policymakers if taken at face value.

Recommendations for policy applications:

- AI-generated rankings should be clearly labeled as decision-support tools, not authoritative conclusions.
- Transparency is key. If AI contributes to a risk assessment, the methodology and limitations must be clearly communicated to avoid over-reliance on AI-generated results.
- Practitioners should remain aware of AI's influence on public perception. If AI rankings align with public intuition rather than structured analysis, they may reinforce perceptions that do not align with actual security priorities.

4.6 Future Research Directions

AI's ability to replicate structured decision-making in risk assessment is promising but requires further refinement to improve consistency, transparency, and reliability. While AI-generated rankings can approximate structured human methods, unexplained ranking shifts and sensitivity to input structure highlight areas that need additional study. One key area for future research is understanding why AI rankings shift unpredictably. Investigating the internal mechanisms behind these changes could help refine AI's stability and reduce erratic ranking behavior. Additionally, comparing multiple AI models could provide insights into how different systems handle deliberation and structured decision-making, identifying which are best suited for comparative risk ranking.

Another important direction is testing AI's performance in real-world homeland security applications. While AI has been evaluated in controlled settings, its effectiveness in operational decision-making remains uncertain. Future research should explore how AI-generated rankings influence policy, resource allocation, and emergency planning when used by homeland security professionals. Ensuring AI integrates seamlessly into existing risk assessment frameworks will be critical for its adoption. By addressing these challenges, AI can become a more reliable and transparent tool for comparative risk assessment, enhancing decision-making without replacing human judgment.

4.7 Summary of Findings

AI risk ranking tools offer significant potential but should be integrated into multi-method assessment strategies rather than used in isolation. While AI can efficiently process large amounts of data and generate structured rankings, its outputs should always be evaluated alongside human deliberation, expert judgment, and traditional risk assessment methodologies. Decision-makers should ensure that AI-generated rankings are contextualized within broader security frameworks to avoid overreliance on automated assessments.

To maximize AI's utility, structured AI methodologies should be developed for consistent risk ranking applications. Standardized approaches, such as predefined risk attributes and deliberative AI frameworks, will help ensure AI produces transparent and repeatable results. Additionally, future policy efforts should focus on integrating AI into decision-making while maintaining human oversight. AI should function as a decision-support tool, with clear protocols for expert validation and accountability. Establishing best practices for AI risk ranking in homeland security will allow

agencies to leverage AI's efficiency while ensuring that critical security decisions remain guided by human expertise.

5. References

Afzal, F., Yunfei, S., Nazir, M., & Bhatti, S. M. (2019). A review of artificial intelligence based risk assessment methods for capturing complexity-risk interdependencies: Cost overrun in construction projects. International Journal of Managing Projects in Business, 14(2), 300–328. https://doi.org/10.1108/IJMPB-02-2019-0047

Chan, A. (2023, April 28). Industry News 2023 Can AI Be Used for Risk Assessments. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2023/can-ai-be-used-for-risk-assessments

DHS. (2024). AI Use Case Inventory Library | Homeland Security. https://www.dhs.gov/publication/ai-use-case-inventory-library

Faheem, M. A. (2021). AI-Driven Risk Assessment Models: Revolutionizing Credit Scoring and Default Prediction. Iconic Research And Engineering Journals, 5(3), 177–186.

Florig, H. K., Morgan, M. G., Morgan, K. M., Jenni, K. E., Fischhoff, B., Fischbeck, P. S., & DeKay, M. L. (2001). A deliberative method for ranking risks (I): Overview and test bed development. Risk Analysis, 21(5), 913–913.

Jenni, K. E. (1997). Attributes for Risk Evaluation [Unpublished doctoral dissertation]. Carnegie Mellon University.

Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.

Keeney, R. L., & von Winterfeldt, D. (2011). A value model for evaluating homeland security decisions. Risk Analysis, 31(9), 1470–1487.

Lundberg, R. (2018). A Multiattribute Approach to Describe Homeland Security Risks. Journal of Risk Research, 21(3), 340–360.

Lundberg, R. (2025). Characterizing Homeland Security Risk: A Principal Component Analysis of 10 Hazards. Journal of Homeland Security and Emergency Management. https://doi.org/10.1515/jhsem-2023-0040

Lundberg, R., & Willis, H. H. (2015). Assessing Homeland Security Risks: A Comparative Risk Assessment of 10 Hazards. Homeland Security Affairs, 11, 1–24.

Lundberg, R., & Willis, H. H. (2016). Deliberative Risk Ranking to Inform Homeland Security Strategic Planning. Journal of Homeland Security and Emergency Management, 13(1), 3–34.

Lundberg, R., & Willis, H. H. (2019). Examining the Effectiveness of Risk Elicitations: Comparing a Deliberative Risk Ranking to a Nationally Representative Survey on Homeland Security Risk. Journal of Risk Research, 22(12), 1546–1560. https://doi.org/10.1080/13669877.2018.150159

Slovic, P. (1992). Perceptions of risk: Reflections on the psychometric paradigm. In S. Krimsky & D. Golding (Eds.), Social Theories of Risk (pp. 117–152). Praeger.

Starr, C. (1969). Social benefit versus technological risk. Science, 165, 1232–1238.

Suggested citation: **Lundberg, R.** (2025). AI assistant comparative risk assessment for homeland security threats. *One Step Ahead, July 2025,* 66–78. The Sam Houston State University Institute for Homeland Security. OSF | AI Assistant Comparative Risk Assessment for Homeland Security Threats

The Institute for Homeland Security

Future Topics in Research

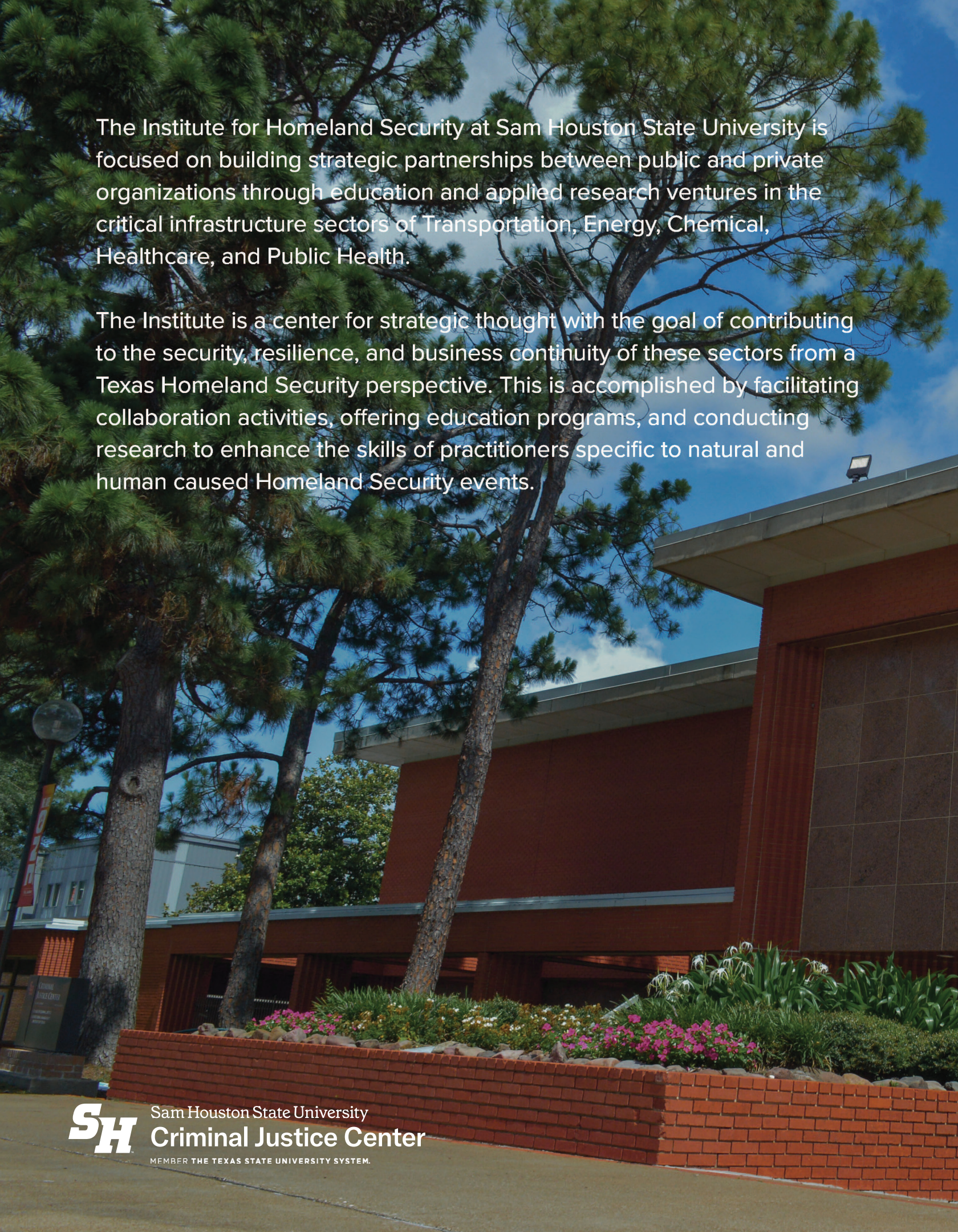
Critical Infrastructure Innovation Sandboxes: Enhancing Technology Testing through Digital Twins

The Convergence of Safety and Security related to the implementation of Small Modular Nuclear Reactors in Texas: Threats, Vulnerabilities, and Disruptive Pathways

Clinical Diagnoses and Their Role in Hospital Workplace Violence A Comprehensive Literature Review

The Transformation of Security in the Texas Energy Sector

For More Information on Events, Training or Research Opportunities find us at ihsonline.org



The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Sam Houston State University
Criminal Justice Center
MEMBER THE TEXAS STATE UNIVERSITY SYSTEM.