



7. DELIBERATE HAZARDS

7.1 HAZARD PROFILE

7.1.1 HAZARD DESCRIPTION

This section provides a description of the hazard, including causes, hazard or incident characteristics, and potential impacts.

Deliberate hazards, for the purposes of this chapter, are defined as hazards resulting from intentional human actions taken to harm people, infrastructure, or the environment with the goal of inflicting harm, damage, or disruption. These hazards are typically planned and executed with specific objectives in mind, such as creating fear, undermining security, sabotaging systems, or causing economic or social instability.

While a wide variety of malicious acts falls under the category of deliberate hazards, this chapter focuses on two subcategories of primary concern for the City – acts of mass violence and cyber attacks.

Mass Violence Incidents

A mass violence hazard refers to a deliberate, human-caused act of violence intended to cause widespread physical harm, death, or psychological trauma to multiple individuals or to disrupt public safety and security.

The following are key characteristics of violence incidents.

- Intentional harm - deliberate and premeditated violence
- Multiple victims - typically more than 3 or 4 people injured or killed
- Sudden onset - occurs quickly, often without warning
- Disruptive impact - taxes or overwhelms local response capacity and affects the wider community

MASS VIOLENCE INCIDENT TYPES

Mass violence incidents can take a number of different forms, including mass shootings, terrorist attacks, bombings, or large-scale assaults. Below are definitions of mass violence incidents of most concern to the City.

Terrorist Attacks

Terrorism is defined by the FBI as “the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives” (OIG 2005).



The FBI categorizes terrorism into two categories, domestic terrorism from international terrorism (FBI 2025):

- Domestic terrorism: Violent, criminal acts committed by individuals and/or groups to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature.
- International terrorism: Violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations (state-sponsored).

There are various types of terrorist attacks, or tactics, which include but are not limited to assassinations, kidnappings, hijackings, bomb scares and bombings, cyber attacks (computer-based attacks), and use of chemical, biological, nuclear, and radiological weapons (FEMA 2004)

Bombings

A bomb hazard in the context of mass violence involves the deliberate placement, detonation, or threat of an explosive device for the purpose of causing mass casualties, destruction, disruption of public order, and widespread fear. Bombings may occur as part of an act of terrorism or large-scale criminal violence.

Active Shooters and Mass Shootings

Active shooter incidents are defined by the FBI as “one or more individuals actively engaged in killing or attempting to kill people in a populated element.” Active shooter events can result in mass shooting incidents. The definition of mass shooting can vary across organizations and there is not a universally accepted definition. For the purpose of this plan, the Gun Violence Archive definition is used, which is four or more people killed or wounded by gunshots, excluding the shooter.

Civil Disturbances or Riots

Large-scale violent protests or riots can escalate to mass violence, where there is widespread damage, injury, or death.

POTENTIAL IMPACTS OF MASS VIOLENCE

Mass violence events often result in fatalities and serious injuries, with lasting psychological trauma for survivors, responders, and affected communities. Emergency medical services, law enforcement, and public health systems may be overwhelmed during or after such events, affecting the overall capacity to respond to other concurrent emergencies. These incidents can erode public confidence, fuel fear or social unrest, and challenge the cohesion and resilience of communities.

Cyber Attack

A cyber attack is the intentional exploitation of computer systems, networks, and technologies through unauthorized access, code injection, data manipulation, or service disruption, often aimed at achieving espionage, financial gain, sabotage, or destruction.



CYBER ATTACK TYPES

Table 7-1 shows prevalent types of cyber attacks.

Table 7-1. Cyber Attack Causes and Types

Incident	Description
Denial of Service	Denial of service attacks inundate computers and networks with traffic that can overwhelm systems and hinder legitimate requests. This traffic typically originates from multiple locations, complicating efforts to mitigate the attack. These incidents are known as distributed denial of service (DDoS) attacks. By restricting access to websites that are critical for business operations, malicious actors can pose cause financial losses and harm to the organization’s reputation. DDoS attacks have been employed to disrupt access to government websites.
Malware	Malware is any type of software designed to harm or exploit a programmable device, service, or network by performing any of a wide variety of malicious actions.
Ransomware	Ransomware uses encryption to deny access to information. Ransomware actors demand ransom to decrypt the information and may also threaten to publish the information unless the ransom is paid.
Spyware	Spyware infects computers and collects information about user activity, such as usernames and passwords, payment information, information in emails, and other sensitive information that may enable threat actors to perform other malicious activity.
Trojan	A trojan provides a backdoor gateway for malicious programs or threat actors to enter a system and steal valuable data without the user’s knowledge or permission.
Worm	A worm replicates and spreads across devices within a network. As it spreads, it consumes bandwidth, overloading infected systems, and making them unreliable or unavailable.
Phishing	Phishing consists of email or text messages (smishing) sent to trick people into clicking a link, downloading malicious software (malware) or revealing login credentials. If successful, phishing may infect the email recipient’s computer.
Spear Phishing	Spear phishing is a tactic that targets specific organizations or individuals with personalized messages that deceive the receiver into trusting the message.
Third-Party Compromises	Malicious actors attack third-party vendors of software and services because other organizations rely upon and trust vendors and install their software to manage complex systems. Adversaries gain access to third-party vendor software to exploit the modified software once installed by the vendor’s customers.

Source: FEMA 2023



POTENTIAL IMPACTS OF CYBER ATTACKS

The potential impacts of a cyber attack are diverse and often interconnected, affecting multiple sectors simultaneously:

- **Operational Disruptions and Public Safety Risk**—Attacks can render critical systems and services inoperable, delaying emergency response, halting public operations, or disrupting essential infrastructure such as power grids, healthcare facilities, and transportation networks. Disruptions to hospitals, water treatment plants, emergency communication systems, and transportation infrastructure pose serious threats to public health and safety.
- **Data Compromise**—Breaches may lead to the exposure, theft, or destruction of sensitive data, including personal, financial, medical, and classified information. Intellectual property loss can also damage innovation and competitiveness.
- **Financial Loss**—Cyber incidents often result in direct financial damage through ransom payments, incident response costs, regulatory penalties, and business interruption. For some entities, the financial consequences can be catastrophic. According to the Federal Bureau of Investigation’s (FBI) 2024 Internet Crime Report, the Internet Crime Complaint Center (IC3) received more than 880,418 cyber attack complaints, with potential losses exceeding \$12.5 billion (FBI 2024).
- **Reputational Damage**—Loss of public trust and stakeholder confidence is a common fallout, especially for government institutions, healthcare providers, and businesses entrusted with sensitive information. Cyber crimes can damage a company’s brand and reputation, destroy competitive advantage, lead to reduced credit rating, and increase cyber insurance premiums (Huang, et al. 2023).
- **Legal and Regulatory Exposure**—Organizations may face lawsuits, investigations, and compliance penalties following data breaches or service failures, particularly when critical or protected data is involved.
- **National Security Concerns**—State-sponsored or politically motivated cyber attacks may target defense networks, critical infrastructure, or election systems, resulting in intelligence compromise or geopolitical instability.
- **Societal and Psychological Impacts**—Public fear, misinformation, and decreased trust in institutions can arise from high-profile attacks, especially those affecting communications or essential services.

7.1.2 LOCATION

This section identifies areas of greater vulnerability based on their physical location. Deliberate hazards can occur anywhere within the City.

Mass Violence Incidents

Mass violence events can occur anywhere in the City. Certain types of locations are often targets of mass violence attacks, including those with high concentrations of people, symbolic significance, or vulnerable populations. Specific locations depend on an individual’s or organization’s agenda. High-risk targets are primarily soft targets, or locations which are open to the public and easily accessible, leaving them vulnerable to attacks.



Areas most at risk for mass violence incidents include the following:

- Schools and Universities due to the presence of youth and open access.
- Workplaces, especially those with high stress, poor security, or conflict history.
- Public Events and Gatherings, such as concerts, parades, and rallies, are frequent targets.
- Transportation Hubs such as airports
- Houses of Worship are often targeted for ideological or religious motives.
- Government Facilities, including courthouses and administrative buildings.
- Healthcare Facilities, particularly hospitals and emergency departments.
- Retail and Entertainment Venues such as malls, cinemas, nightclubs.
- Critical Infrastructure including energy, water, and communications systems.
- Sites with Historical, Cultural or other Significance

Cyber Attacks

O'ahu's unique concentration of government, military, economic, and infrastructure assets makes it particularly vulnerable to cyber attacks. Any processes that are networked and controlled by a computer are vulnerable to a cyber attack. The following locations and sectors are at elevated risk:

- Critical infrastructure systems that support the delivery of drinking water, power, or wastewater services are targets for operational disruption or ransomware.
- Government agencies such as City and County of Honolulu IT systems, public safety communications, permit and payment systems, public transit operational systems, and emergency management operations could be targeted for denial of service attacks, ransomware or data theft.
- Military installations on O'ahu may be high-priority target for espionage or nation-state actors.
- Healthcare facilities such as hospitals that handle large volumes of personal health information and rely on digital records and connected devices.
- Financial sector, including banks and credit unions headquartered or operating on O'ahu
- Tourism and hospitality, including hotels and resorts in Waikīkī and Ko Olina may be targeted for guest data, payment systems, or as part of broader economic disruption efforts.
- Airport systems at Daniel K. Inouye International Airport (HNL) are potential targets, including aviation control, flight scheduling, and baggage handling systems.

7.1.3 EXTENT

Hazard extent refers to the potential severity or magnitude of hazard events in a given area. This section describes measurements used to indicate the extent of this hazard and the systems in place for monitoring severity and providing warnings as necessary.



Mass Violence Incidents

The extent of a mass violence event depends on the type and scale of the attack, population involved, equipment and other key assets affected, and duration of the incident or exposure to the agent used. There is not a standardized system to categorize the severity of mass violence events. The City's emergency management agency uses the following categories to indicate the scale, severity and response required to an event.

- **Small Scale**—Localized event (such as a single active shooter with limited casualties). Minimal strain on local resources.
- **Moderate Scale**—Multiple shooters or complex attack (for example, a car ramming or shopping mall attack with multiple injuries)
- **Large Scale**—Coordinated or mass casualty attack (such as large bombings or multiple active shooters) that overwhelms on-island capabilities.
- **Catastrophic/Complex Coordinated Attack**—Terrorists attacks involving multiple methods, possibly in multiple cities, causing severe disruption and a robust federal response.

The effect of a mass violence event can vary depending on the type of attack and the magnitude of the event. Terrorism events can cause public fear regarding the use of mass transportation or leaving their homes in the event of a biological or nuclear attack. Communication systems, both public and private, can fail because of an overwhelming amount of usage or damage to its infrastructure. Healthcare facilities can become quickly inundated and must be prepared to triage injured patients, handle mass casualties, and conduct decontamination operations. The secondary hazards resulting from a mass violence incident depend on the size and scope of the incident. Some possible secondary hazards include widespread utility failure, health effects such as epidemics or pandemics, flooding (if a dam was destroyed), and environmental contamination.

Cyber Attacks

Cyber attacks can vary in severity based on the systems affected, warning time, and ability to preempt an attack (Cybersecurity & Infrastructure Security Agency n.d.). Impacts can be limited to the organization that was targeted or may be felt community-wide if systems that provide essential services are targeted directly or disrupted as a result of cascading impacts.

The Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security, classifies cyber incidents using a severity scale called the National Cyber Incident Scoring System. This system helps assess the potential impact of an incident and prioritize response.

- **Emergency (Black)**—An Emergency priority incident poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.
- **Severe (Red)**—A Severe priority incident is likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.



- **High (Orange)**—A High priority incident is likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
- **Medium (Yellow)**—A Medium priority incident may affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
- **Low (Green)**—A Low priority incident is unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
- **Baseline**—A baseline priority incident is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The bulk of incidents will likely fall into the baseline priority level with many of them being routine data losses or incidents that may be immediately resolved. However, some incidents may require closer scrutiny as they may have the potential to escalate after additional research is completed. In order to differentiate between these two types of baseline incidents, the National Cyber Incident Scoring System separates baseline incidents into two categories:
 - **Baseline – Minor (Blue)**—A Baseline–Minor priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.
 - **Baseline – Negligible (White)**—A Baseline–Negligible priority incident is an incident that is highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.

7.1.4 PREVIOUS OCCURRENCES

Recent Events

This section provides an overview of hazard occurrences since the publication of the previous LHMP, which covers the period between January 2020 and February 2025. It identifies significant events that resulted in federal disaster declarations and/or state or local emergency proclamations. Table 7-2 shows recent mass violence events for O’ahu and Table 7-4 shows recent cyber attacks.



Table 7-2. Mass Violence Threat Events in the City (2020 to 2024)

Event Date	Disaster Declaration/ Proclamation			Description
	Federal	State	Mayoral	
2020	—	—	—	Hibiscus Drive Shooting and Arson, January 19, 2020—A man being evicted from a property opened fire on officers responding to reports of a stabbing. Two officers were fatally wounded. The man then set fire to the property, which spread to neighboring homes. The bodies of the suspect and his landlady were later recovered.
2024	—	—	—	Waianae Valley Mass Shooting, August 31, 2024—A shooting at a home on Waianae Valley Road resulted in three deaths and two injuries. The shooter was fatally shot by a neighbor who intervened.

Table 7-3. Cyber Attack Events in the City (2020 to 2024)

Event Date	Disaster Declaration/ Proclamation			Description
	Federal	State	Mayoral	
2021	—	—	—	Vulnerability exploitation; information technology (IT) disruption, resource diversion (to mediation), reputational
2021	—	—	—	Ransomware; IT disruption, resource diversion (to mediation), reputational
2022	—	—	—	Targeted phishing
2022	—	—	—	Denial of service; outward-facing website availability
2024	—	—	—	In June 2024, O’ahu Transit Services (OTS), the operator of the City’s public transportation systems – theBus and TheHandi-Van – was impacted by a significant ransomware attack and led to the shutdown of critical digital services, including transit websites, GPS tracking systems and payment processes. No ransom was paid, but the attack resulted in about \$300,000 in damages

Source: HI-EMA 2022

Federal Disaster Declarations

Under the Stafford Act, the President of the United States may issue an Emergency Declaration (EM) or Major Disaster Declaration (DR) for health related events and activate certain federal assistance programs based on factors related to the magnitude of the hazard threat or impacts. No Stafford Act declarations for this hazard type that included the City occurred during this period.



State and Local Emergency Proclamations

State law authorizes the Governor to issue emergency proclamations if an emergency or disaster has occurred, or there is imminent danger or threat of an emergency or disaster in any portion of the state. County Mayors have the authority to issue local emergency proclamations when such conditions exist within any part of their respective jurisdictions. No state or local emergency proclamations related to this hazard were issued for the City during this period.

7.1.5 PROBABILITY OF FUTURE OCCURRENCES

Information on previous deliberate hazard occurrences in the City was used to calculate the probability of future occurrence of such events. Table 7-4Table 17-4 lists the number of events from various sources over the five-year period from 2020 to 2024 which is the most complete period of record for all sources reviewed. Based on these records, the probability of occurrence in the City is considered “frequent.”

Table 7-4. Probability of Future Deliberate Hazard Incidents in Honolulu

Hazard Type	Number of Occurrences from 2020 to 2024	Percent Chance of Occurring in Any Given Year
Mass Violence	2	40%
Cyber Attacks	4	100%

Source: HI-EMA 2022

Note: A 100 percent probability indicates statistical likelihood for an event to occur every year. It does not indicate that occurrence of an event is a certainty in any given year.

The 2025 Homeland Security Threat Assessment from the Department of Homeland Security indicates that looking forward, the threat of violence from United States-based violent extremists will remain high, aligning with the Steering Committee’s input. The threat will continue to be characterized primarily by lone offenders or small cells motivated to violence by a combination of racial, religious, gender, or anti-government grievances; conspiracy theories; and personalized factors. Concern primarily surrounds the likelihood of violence motivated by developing domestic and global events, including the ongoing Israel-HAMAS conflict. Foreign Terrorist Organizations (FTO), like ISIS and al-Qaida, are thought to continue maintaining the intent to conduct or inspire attacks in the United States and have leveraged the conflict in the Middle East to reaffirm this intent. FTO media outlets promote rhetoric intended to inspire persons in the United States to mobilize to violence, while foreign terrorists continue engaging online supporters to solicit funds; create and share media; and encourage followers to attack the United States, its interests, and what the FTOs perceive as the West (Department of Homeland Security 2024).

Furthermore, the U.S. Government Accountability Office’s (GAO) February 2023 Domestic Terrorism Report revealed that incidents of domestic terrorism increased by 357 percent between 2013 and 2021, from 1,981 cases to 9,049 cases. The extreme increase in cases indicates the heightened likelihood of domestic terrorism within the United States (GAO 2023).



7.2 VULNERABILITY AND IMPACT ASSESSMENT

Overall, it is difficult to quantify potential losses due to deliberate hazards because of the many variables that must be considered. Potential impacts may be local, statewide, or national depending on the magnitude and location of the event. A qualitative assessment is discussed below.

7.2.1 LIFE, HEALTH, AND SAFETY

Overall Population

The entire population of the City is exposed to mass violence and cyber attacks.

MASS VIOLENCE INCIDENTS

Mass violence events can occur in all communities, often with little warning, and typically occur in public places.

CYBER ATTACKS

While cyber attacks do not directly physically harm the population, indirect impacts are possible that threaten the welfare of the population if critical services or utilities are disrupted that affect safety or public health.

Cyber attacks, for example, can affect the health care system (e.g., networked medical equipment may be vulnerable to hacking). Individuals' personal information also is at risk. Commonly stolen personal information includes name, Social Security number, and drivers' license information. Because it is difficult to predict the particular target of cyber attack, assessing vulnerability to the hazard is also difficult. Generally, all members of the population who directly use a computer or those receiving services from automated systems are vulnerable to cyber attack.

Socially Vulnerable Population

Socially vulnerable populations include groups that face greater obstacles due to factors like poverty, disability, language barriers, or age.

MASS VIOLENCE INCIDENTS

Language barriers can prevent understanding of emergency instructions. People with disabilities, elderly individuals, or those without reliable transportation may find it harder to escape or respond during a mass violence incident. After an event, mental health resources may not be equitably distributed, making these groups more likely to suffer long-term effects.



CYBER ATTACKS

While some members of socially vulnerable communities may not have access to devices that are susceptible to cyber attacks, they likely rely heavily on agencies and programs that do use such devices, which could worsen the effects of cyber attack on these communities.

If a cyber attack targeted Honolulu's power or utility grid, vulnerable populations could face the greatest effects. For example, individuals with medical needs are vulnerable because many of the life-saving systems on which they rely require power. The vulnerable populations most susceptible to cyber attacks are adults over 75 (Gaskell 2021).

Cyber attacks that expose personal information can result in individuals facing economic hardship from fraud. For those already experiencing impoverishment, a cyber attack can compound the situation.

7.2.2 ECONOMY AND GENERAL BUILDING STOCK

Mass Violence Incidents

The entire general building stock inventory in the City is exposed and vulnerable to mass violence events, particularly terrorism. This includes a wide range of structures, from residential buildings to commercial properties, all of which can suffer significant damage in the event of a terrorist attack. Structural impacts typically include damage to roofs, building frames, windows, and the contents within these buildings. Unfortunately, current modeling tools are not sophisticated enough to estimate specific losses from such hazards accurately.

Given these vulnerabilities, it is imperative that the City continues to implement and enhance mitigation and protection measures to safeguard these public locations. This includes physical security measures such as surveillance systems, security personnel, and controlled access points. Additionally, emergency preparedness plans should be regularly updated and tested to ensure a swift and effective response in the event of an attack.

Public awareness and community engagement are also crucial. Educating residents about the importance of vigilance and encouraging them to report suspicious activities can help prevent potential threats. Collaboration with federal and state agencies can provide additional resources and expertise to bolster local efforts.

Cyber Attacks

The general building stock is not at risk from cyber attacks, but the information systems and data storage within those buildings are vulnerable, as are the business and/or operation functions that they support.



7.2.3 COMMUNITY LIFELINES AND OTHER CRITICAL FACILITIES

Community lifelines are particularly vulnerable to deliberate acts due to the importance of lifeline facilities. In addition, the interdependencies among lifelines means that widespread impacts are possible by intentional acts against a single target.

Mass Violence Incidents

Critical facilities and culturally significant locations are particularly vulnerable to terrorism. These include schools, community centers, libraries, and other public spaces that are essential to the fabric of the community. These areas are not only important for their functional roles but also as places where people gather, socialize, and spend time. As previously discussed, the core aim of terrorism is to instill fear and terror among large groups of people by targeting community events and public spaces.

Schools, for instance, are vital as they educate and nurture the city's youth. An attack on a school could have devastating psychological and emotional impacts on students, staff, and families, disrupting education and creating a climate of fear. Community centers and libraries serve as hubs for social interaction, learning, and cultural activities. An attack on these facilities could disrupt community cohesion and access to essential services.

The full functionality of critical facilities, such as police stations, fire departments, and medical facilities, is essential for both the immediate response to and the aftermath of a mass violence event. These facilities are the backbone of a community's safety and security, providing the necessary services to protect and assist residents during emergencies.

Cyber attacks

All community lifelines and other critical facilities are vulnerable to cyber attacks. Interruption of services may affect facilities that must be in operation in response to a cyber attack. An attack that causes loss of power to businesses could cost millions of dollars in revenue.

7.2.4 NATURAL, HISTORIC, AND CULTURAL RESOURCES

Terrorist events involving biological or chemical agents can severely impact the environment by contaminating water sources, degrading soil, and polluting the air. Historical structures and significant landmarks, especially those over 50 years old, hold immense cultural value and are potential terrorist targets. Protecting these sites preserves heritage and strengthens community resilience. Cultural spaces and major hubs, such as event venues and parks, are vulnerable to attacks due to large gatherings. Potential targets include the USS Arizona Memorial, Hawaii Convention Center, Aloha Stadium, Honolulu Marathon, UH Manoa, and Waikiki.



Cyber attacks

A cyber attack does not directly affect environmental resources; however, secondary effects on the environment can occur. If a water or wastewater treatment facility is targeted and operations are interrupted, overflows may result that could pollute land and water environments.

7.2.5 FUTURE CHANGES THAT MAY AFFECT RISK

Potential or Planned Development

Potential and planned development are not projected to change the location, intensity, frequency, or duration of deliberate hazard incidents. However, additional developments can increase the number of potential targets for terrorism.

Projected Changes in Population

Changes in population are not expected to change the location, intensity, frequency, or duration of deliberate hazard incidents. Increases in population increase vulnerability due to the potential for an increase in public gatherings, such as sporting events, public spaces, concerns, and more.

Climate Change

Climate change effects are not projected to change location, intensity, frequency, or duration of deliberate hazard incidents. However, with increases in intensity, frequency, and duration of natural hazard events, disaster survivors may be at risk of becoming victimized by cyber attackers posing as survivor resources. An indirect effect of climate change on cyber attacks could be politically based. Eco-terrorist hackers might target companies or agencies with policies or practices that they oppose.

Evolving Technology

Cyber attacks exploit existing operating system and network vulnerabilities. As technology evolves, cyber attackers will find new ways to exploit vulnerabilities.

The Internet of Things is a network of physical devices, vehicles, appliances, and other physical objects embedded with sensors, software, and network connectivity, allowing them to collect and share data. These include wearable devices (e.g., smart watches), smart homes and assistants (e.g., Alexa, Google Home, etc.), networked doorbells (e.g., Ring), etc. The Internet of Things will increase vulnerability to cyber attacks and provide new targets for malicious actors (IBM 2024).

Likewise, as autonomous vehicle technology progresses and autonomous vehicles become more common on the City's roadways, they are vulnerable to cyber attacks that could cause transportation accidents.