The 19th International Conference on
“Technical and Physical Problems of Engineering”
ICTPE-2023
31 October 2023
International Organization of IOTPE

CYBER SECURITY CHALLENGES OF CRITICAL INFRASTRUCTURES IN A SMART CITY ENVIRONMENT

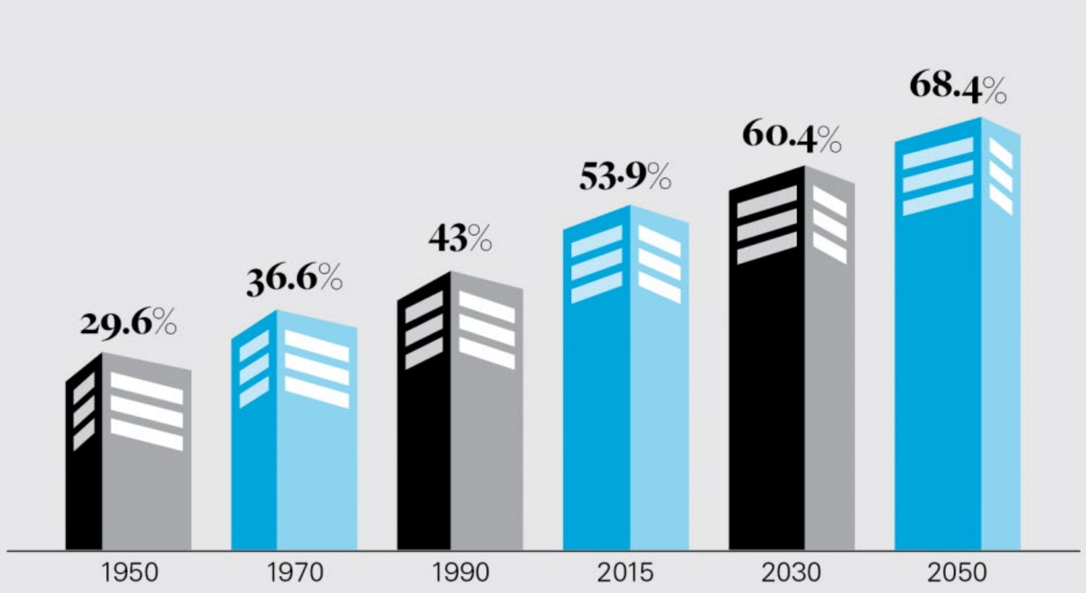
M.A. Hashimov

Institute of Information Technology, Ministry of Science and Education, Baku, Azerbaijan

Introduction

The report of the Department of Economic and Social Affairs of the United Nations (DESAP) for 2018 estimated about 30% of the world’s population to live in urban in the 1950s. In 2014, this figure rose to 55%. These studies estimate 60% of the world’s population to live in modern cities by 2030 and 70% by 2050.

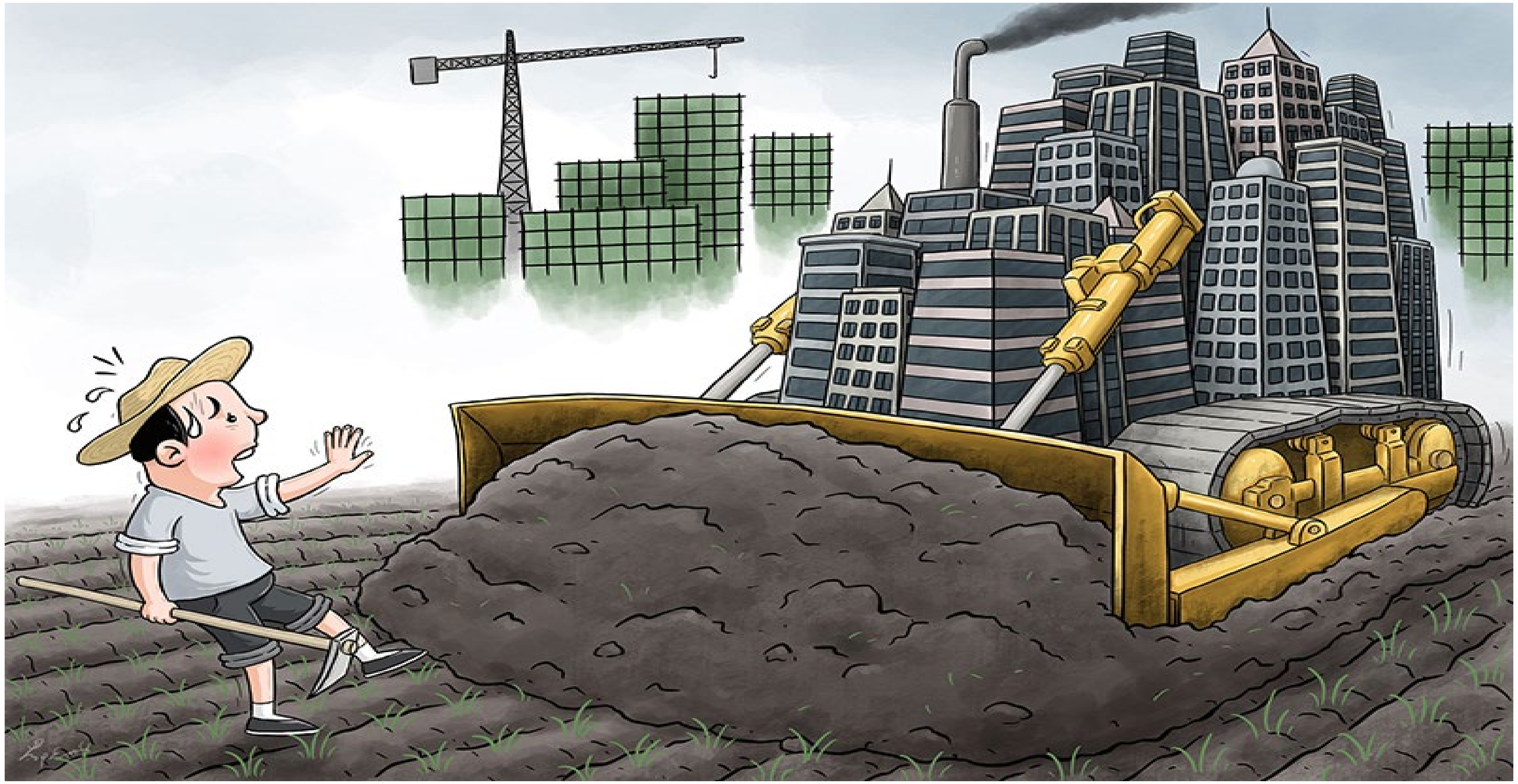
Global urbanization rate, 1950 – 2050, percentage



Source: United Nations Department of Economic and Social Affairs

The rapid growth of cities exacerbates many problems associated with living in an urban environment (public safety, transport management, waste disposal, noise, air and water pollution, etc.).

Experts think that ***“It will not be possible to prevent urbanization. The influx of people into the city will continue as usual.*** Therefore, we need to make life easier. “The only way out of this situation may be” ***smart cities***.”



Smart city concept

The infrastructure of the “Smart City” is built based on high technology.

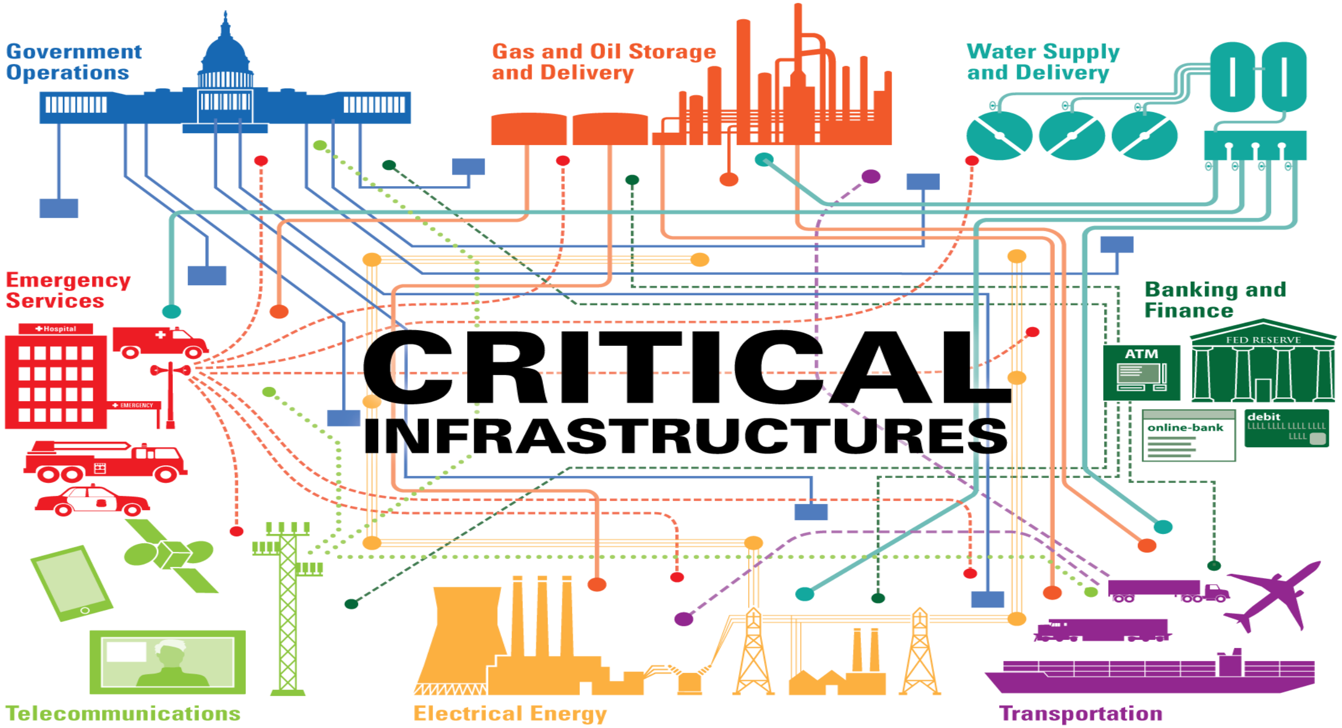
A “smart city” uses ICT to solve the urban problems. The main goal of creating a smart city is to improve social and economic indicators, make life easier and safer for citizens

The main idea of the “Smart City” system is to integrate and manage all services and facilities of the city in a single computerized system.

The 19th International Conference on "Technical and Physical Problems of Engineering" (ICTPE-2023)

Smart city and critical infrastructures

As the smart cities have developed recently, critical infrastructures have become primary components of the national security issues as they are interconnected through the Internet and corporate networks. Security of cities has been an imperative issue for centuries, however with the emergence of smart cities, the development of Internet and communication technologies, and the interconnection of critical infrastructures in smart cities, a new security dimension, that is the cyber security problems, has become even more real.



Critical infrastructures

- Transport systems: highways, bridges, airports, seaports, railway systems and public transport.
- Energy systems: power grids, oil and gas pipelines, oil refineries.
- Water and wastewater systems: water treatment plants, reservoirs, dams and distribution networks.
- Communication systems: telephone and Internet networks, satellite systems and broadcasting infrastructure.
- Emergency services: police and fire departments, emergency management agencies and disaster response systems.

Healthcare facilities: hospitals, clinics, emergency services and medical research facilities.

- Financial institutions: banks, stock exchanges and other financial services.
- Food and agriculture: farms, plants and distribution networks, etc.

The 19th International Conference on “Technical and Physical Problems of Engineering” (ICTPE-2023)

Critical infrastructures are the most important strategic infrastructures of exceptional significance that are considered especially central for the society and ensure the viability of the state.

Critical infrastructures facing serious risks in their operations due to natural or man-made impacts can be a source of great threat to the stability, governance and defense capacity of society.

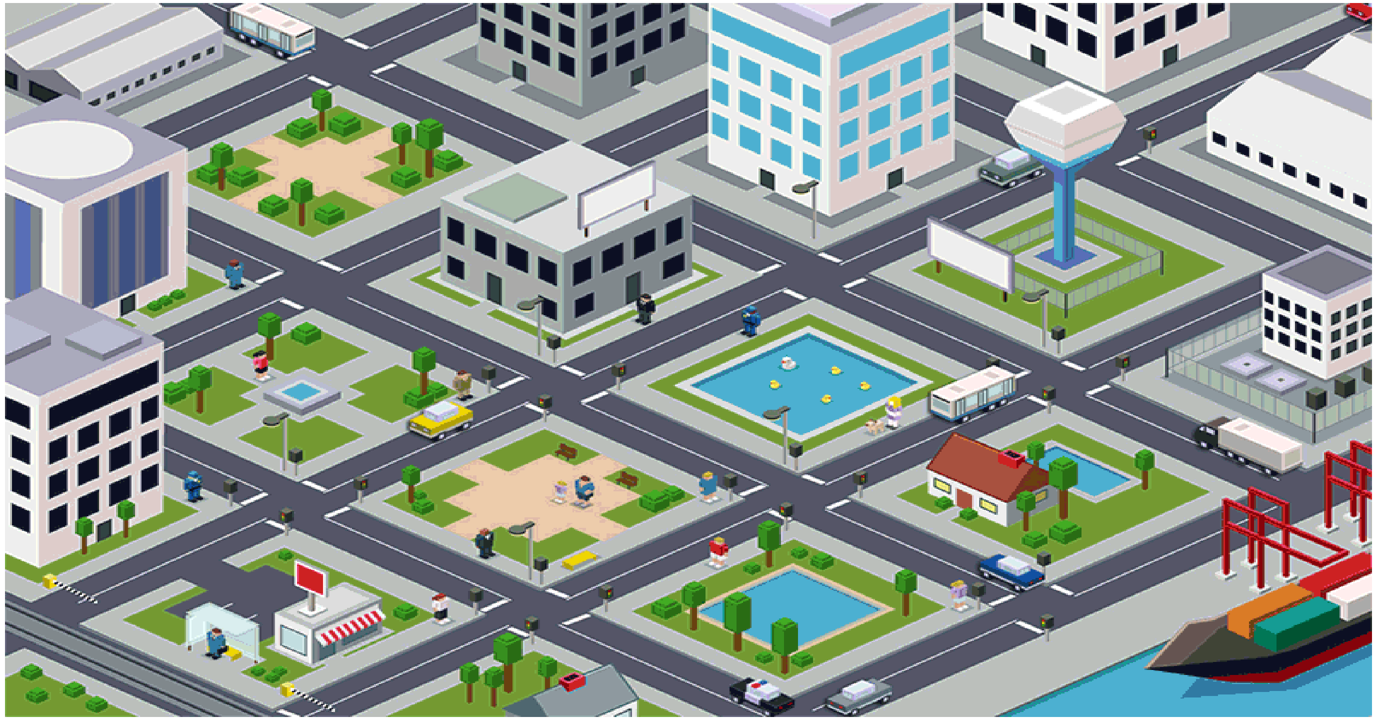
These infrastructures are critical because their failure or destruction significantly affect the healthcare of population, their safety, economic security, or national security.

Some of the critical infrastructures surrounding the smart city environment and their cybersecurity challenges

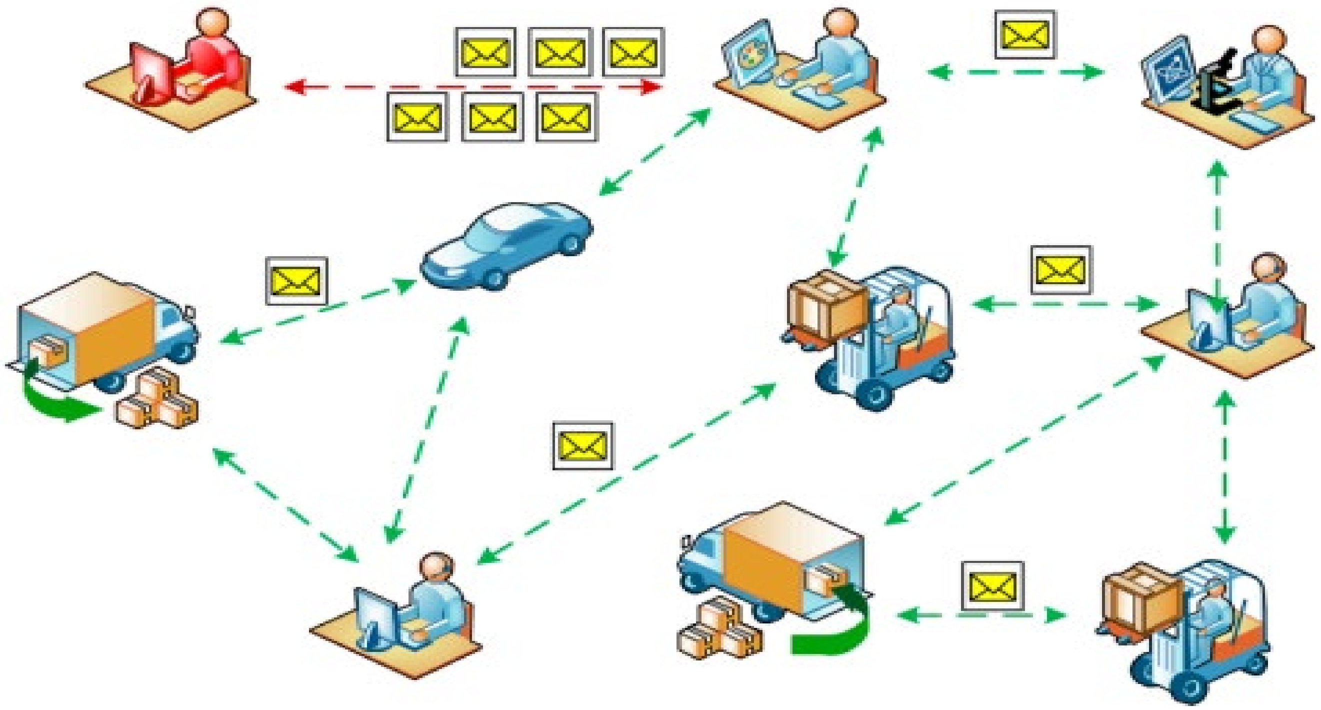
Intelligent transport management systems refer to the monitoring and management of traffic, all types of transport (private, public, cargo).

Smart management of public transport

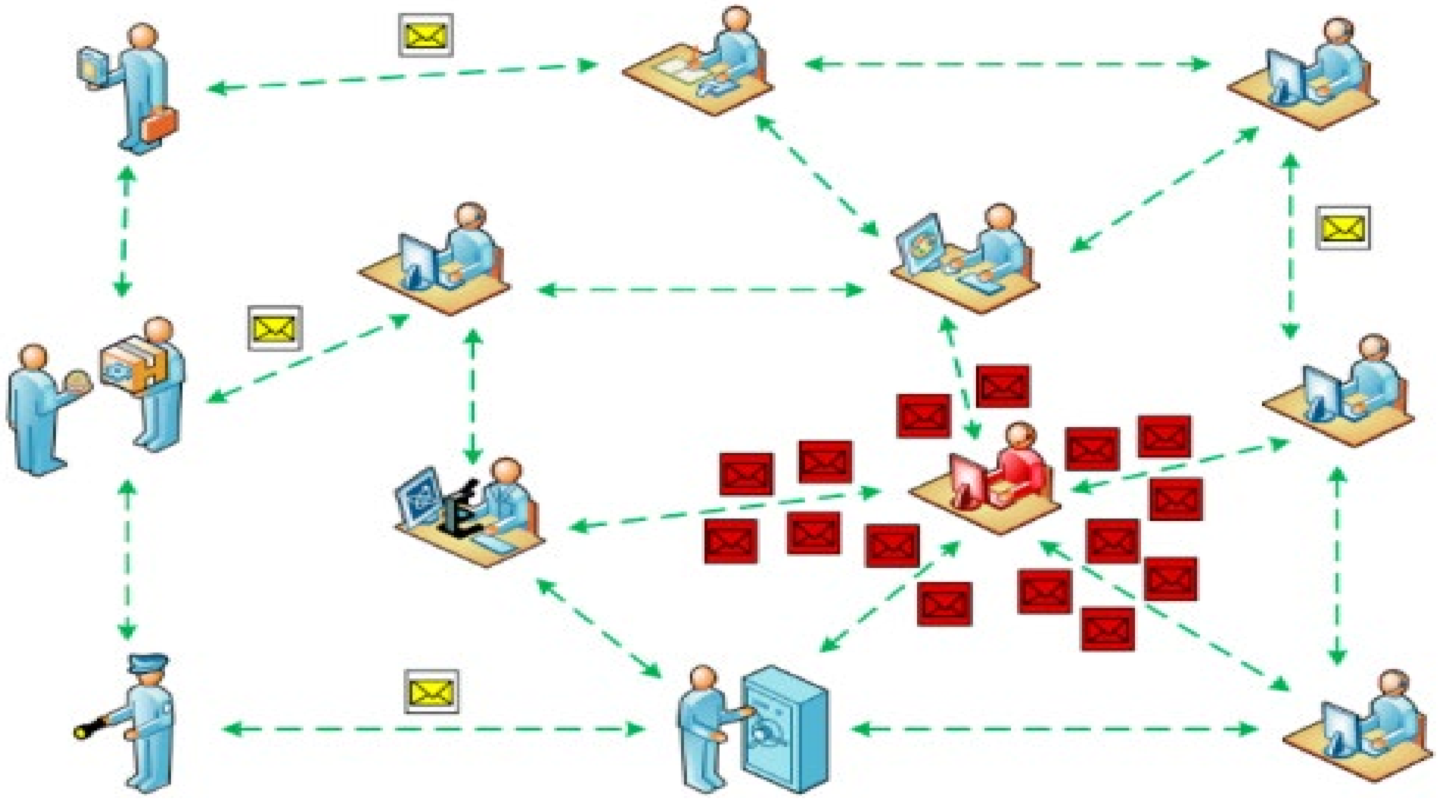
Smart parking systems use sensors and mobile apps to help drivers find available parking spaces more efficiently, reducing time spent for searching for parking and minimizing traffic jam in urban areas



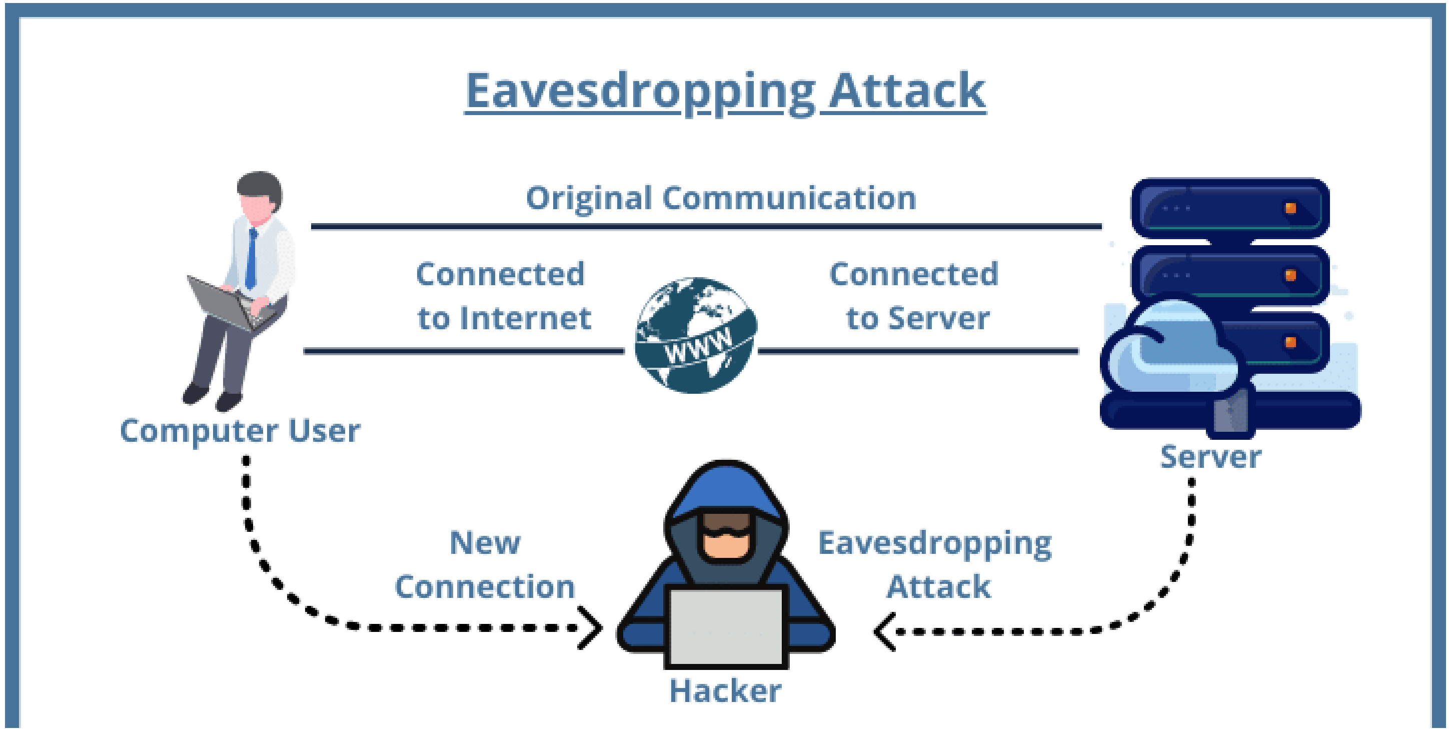
Denial-of-service attacks (DoS). Smart transport infrastructure is the most common target of DoS attacks. DoS attacks are a serious concern for smart cities due to their potential to disrupt critical services and infrastructure. DoS attack uses multiple compromised devices to flood a targeted system or network with an excessive amount of traffic. An attacker can practice malicious devices to disrupt the vehicular network, jam signals and even cause collisions. DoS attacks on a vehicular network can hamper emergency response times or compromise security measures.



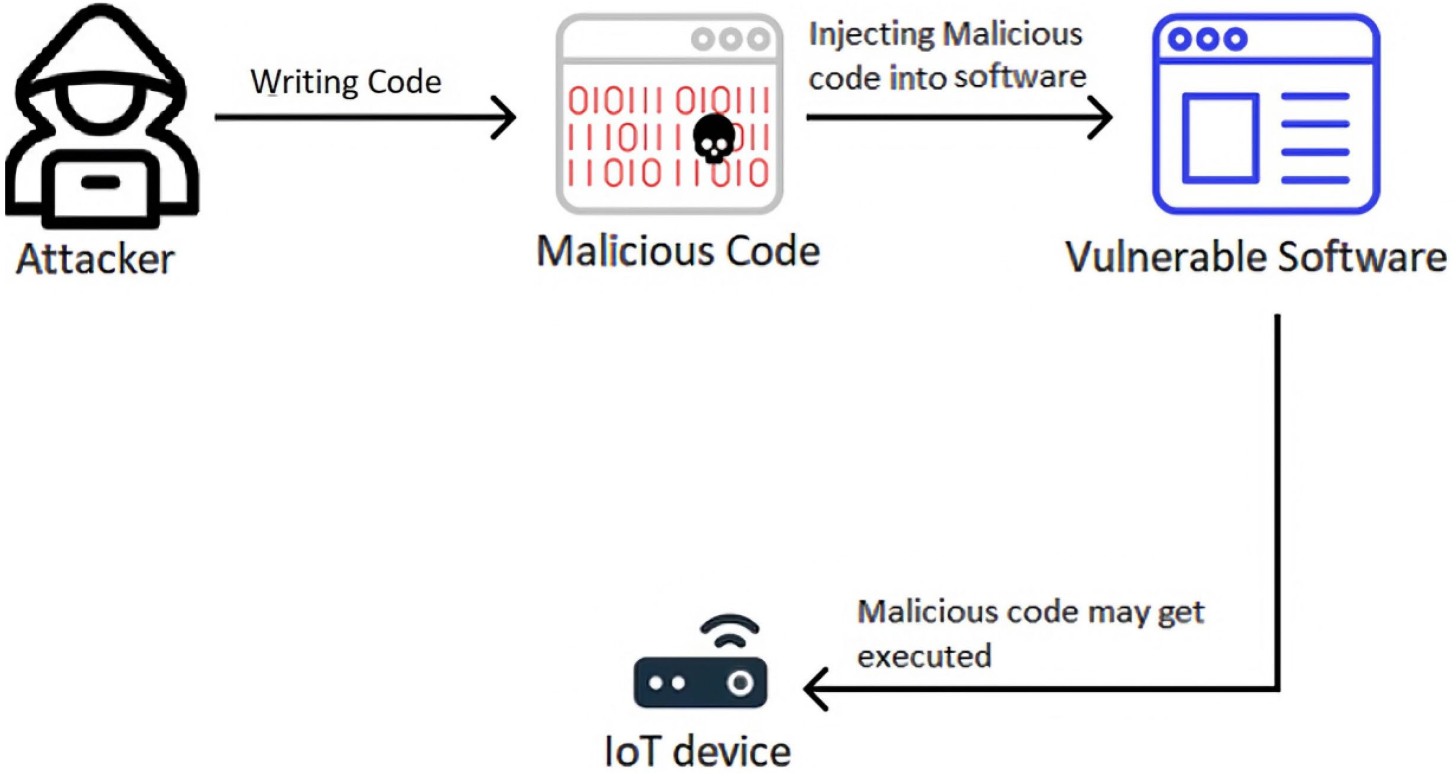
Black hole attack. It is a type of cyber-attack that can target communication systems in a smart city. A malicious node in the network manipulates all incoming data packages, rendering the communication link or network segment impractical. A malicious node does not forward packets to their intended address, resulting in a loss of network connectivity and preventing other vehicles from receiving critical traffic information.



Passive eavesdrop attack is a type of cyber-attack where vehicle tracking or an unauthorized party eavesdrops on the communication between two or more parties. In this attack, the attacker does not actively modify or disrupt the connection, but passively monitors and collects the information shared between the communicating parties. If communications between emergency services or traffic management systems are intercepted, this can prevent real-time responses to incidents.



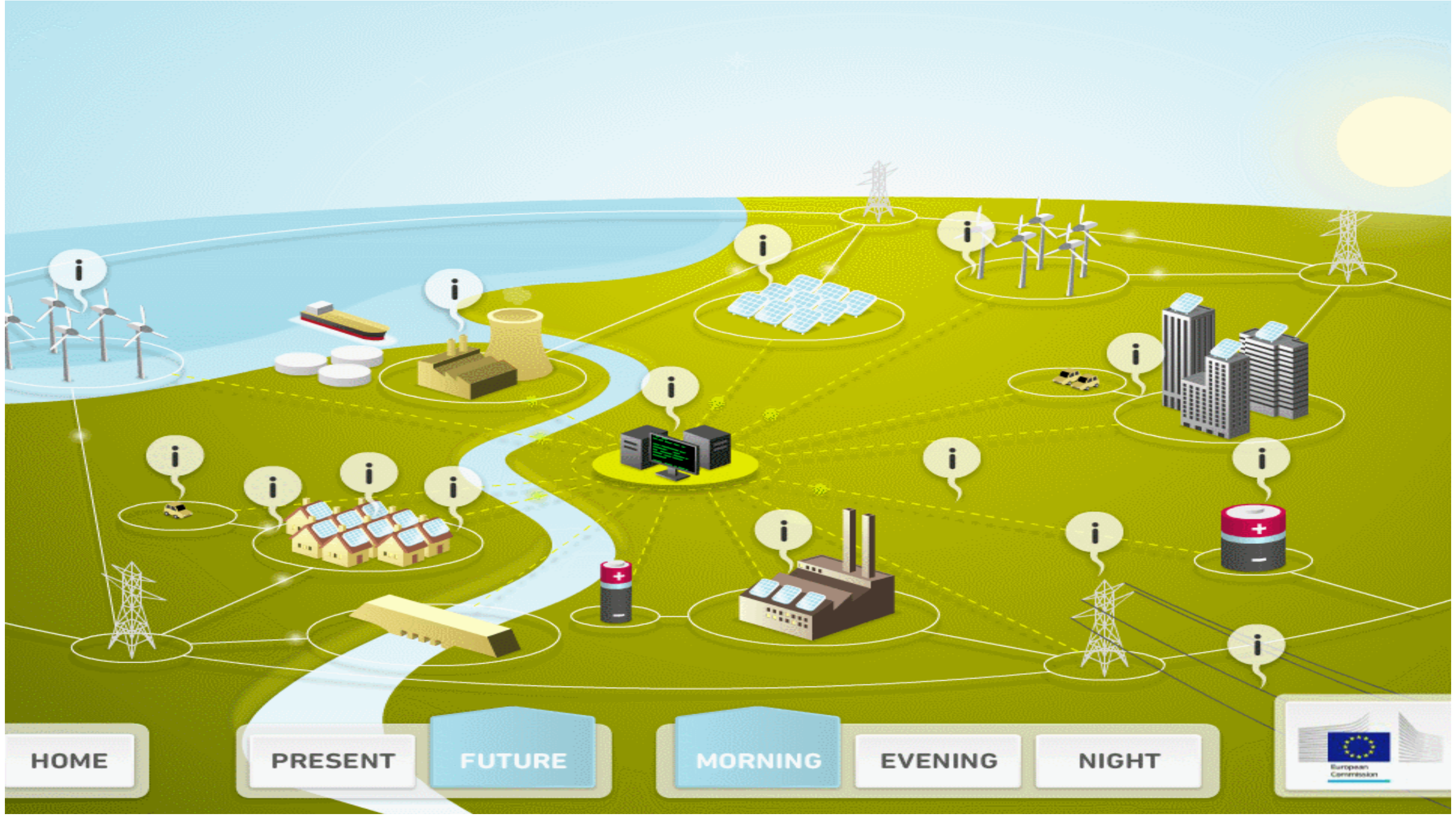
Malicious code injection. It is a type of cyber-attack in which an attacker injects malicious code into a legitimate application or system intending to perform unauthorized actions or harm the target. Injected code can exploit vulnerabilities in an application or system to gain unauthorized access, steal data, modify it, or perform other malicious activities. Injecting malicious code into traffic management systems can lead to erroneous traffic information and manipulation of traffic signals, which can lead to traffic jams or accidents.



The 19th International Conference on "Technical and Physical Problems of Engineering" (ICTPE-2023)

Smart utilities enable smart cities to reduce excessive consumption of resources such as water, gas and electricity, improve economic development and contribute to environmental protection.

A smart grid is a data transmission network that provides an intelligent approach to traditional energy generation, storage, transmission, distribution and demand management to improve reliability and achieve better power quality.



DoS. Since a smart grid is IP-based, it is vulnerable to DoS attacks. These attacks can prevent message packets from being sent over the network or block access to meter readings. DoS or DDoS attacks attempt to suspend, block, or damage the data transmission and sharing between nodes in a smart grid.

Through malware, an attacker can disable smart meters or other critical resources. Malware can also modify or delete sensitive data on smart grid systems.

in 2015, a power outage caused by a denial of service **(DoS) attack on a smart grid (SG)** in Ukraine affected **230,000** people

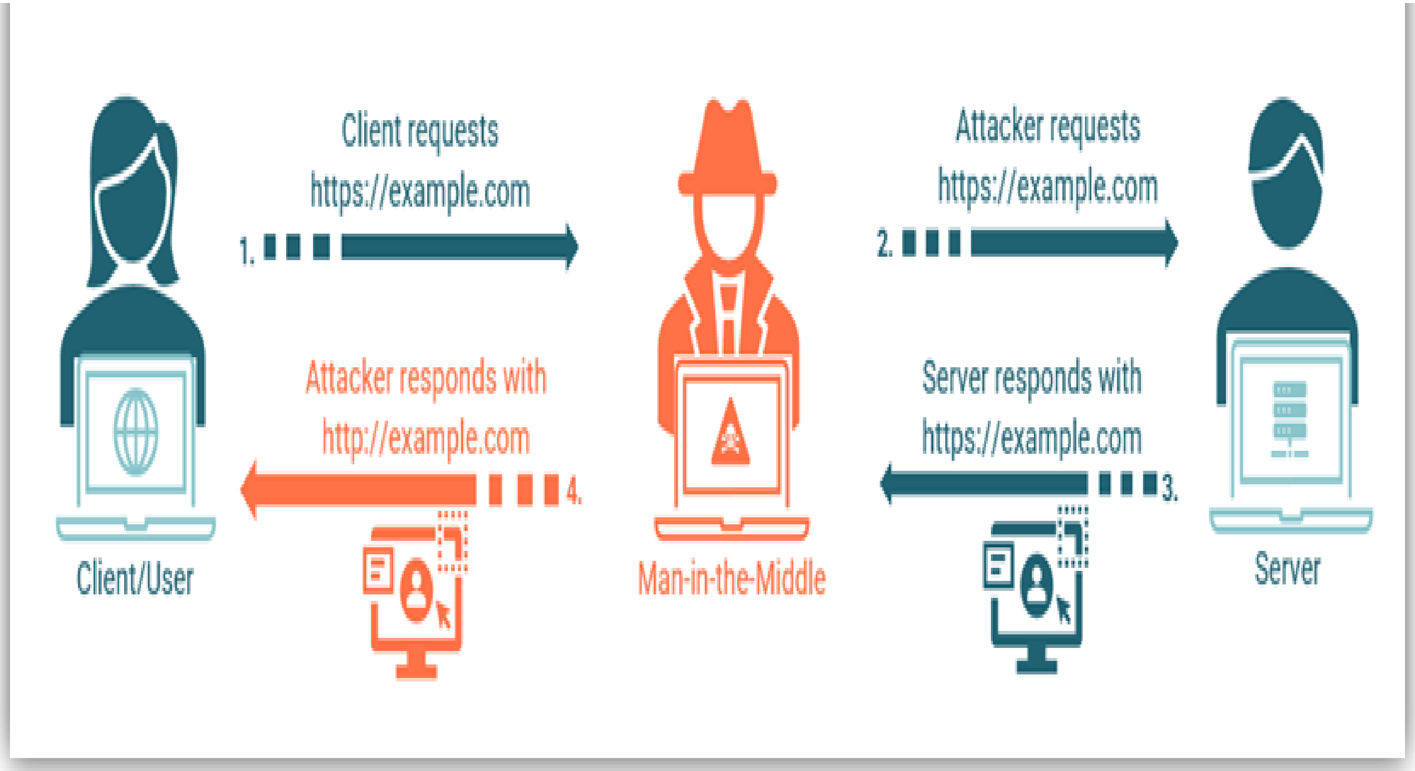
2017 Cyber attack on power infrastructure that distributes electricity in the UK and Ireland. The goal was to penetrate the power management system, which led to the shutdown of a part of the power system.

Cyber Victim: Kyivoblenergo
Time of Attack: Dec 2015
Type of Attack: Spear-phishing, malware
GlobalSign®
GMO INTERNET GROUP

Replay. An attacker may send forged messages or resend the same message several times. These erroneous messages cause the receiver to overload and cause the entire system to fail or slow down. Any intrusion or software attack can result in massive power outages and network disruptions.

2010	The control system of the Iranian nuclear power plant facility was attacked by Stuxnet worm, causing a 20% number of the centrifuges to be forced to shut down [3, 5].	Cyber attack
2013	Several industrial and energy-related companies in the United States were hit by a malware attack from dragonfly attackers, resulting in a massive energy data breach [6].	Cyber attack
2015	The BlackEnergy virus was implanted in the Ukrainian power grid information system, causing continuous tripping of transmission lines and preventing the system from restarting properly, causing 22,500 customers and half of the country outages for several hours [4, 7].	Cyber attack
2016	Electricity sector suffered an unknown cyberattack that paralysed the computer systems in the electric power department for several weeks [8].	Cyber attack
2019	Venezuela's power grid suffered five consecutive rounds of attacks, including cyber, electromagnetic, and physical attacks, within 20 days, causing two consecutive widespread power outages [9, 10].	Coordinated cyber-physical attack
2020	Light S.A, a Brazilian electricity company, was attacked by the Sodinokibi malware and hacked for a ransom of $14 million, while a large amount of electricity data was locked [11, 12].	Cyber attack

A man-in-the-middle attack is an insider attack. Here, the data from the source node passes through the attacker before reaching the destination node, both the source and the receiver think that the data is shared directly. Attackers can identify operator’s behaviors and patterns by recording and analyzing the network traffic over a time period. Monitoring the electricity flow can reveal the privacy of users (lifestyle, working hours, whether the building is vacant or occupied, the time a resident spends at home or on the street). Thus, based on the obtained information, criminals can easily determine the most suitable time for burglary.



The 19th International Conference on "Technical and Physical Problems of Engineering" (ICTPE-2023)

Today, **smart water technology** controls the entire water supply chain, from freshwater storage to wastewater collection and handling. Smart water resource management widely uses various sensors. Using the data generated by sensors at various points in the water supply chain, smart meters and monitoring centers measure water consumption in real time, identify overuse and waste points, adjust usage patterns, and predict future consumption.

Malicious Node Injection: an attacker can inject a virtual node into the network, which in turn enables him to access the network and control the data flow in the smart water system.

DoS. This attack can disable the system by preventing the sending of data from the sensors, the receiving of data and the issuing of commands by the controllers, as well as preventing the actuators from receiving commands and executing actions.

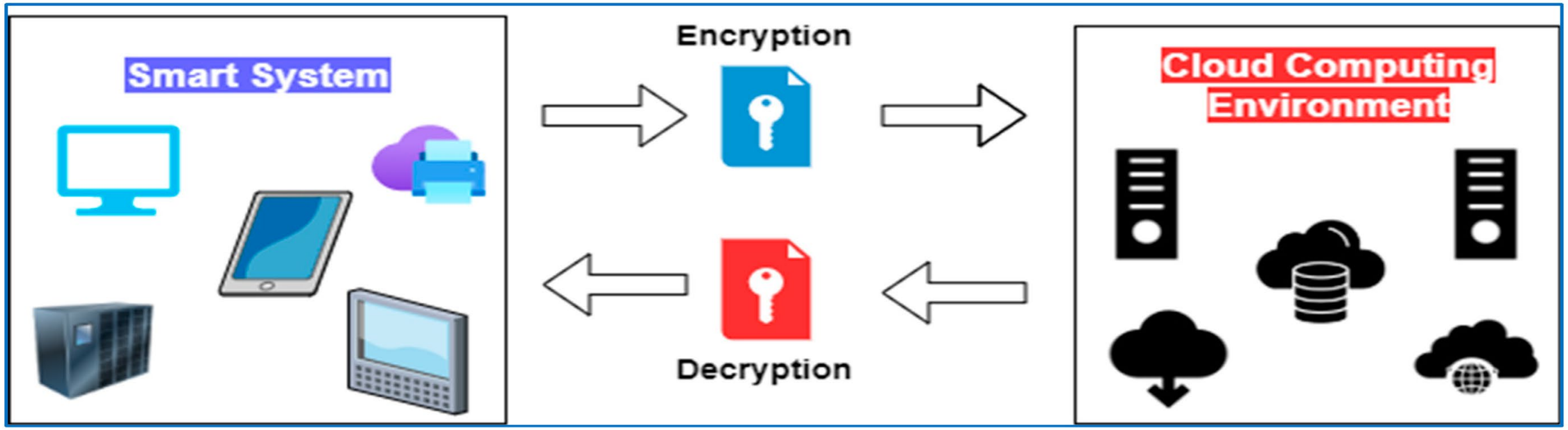
According to the US Department of Homeland Security, **25 cyber-attacks** on various water systems were detected in 2015.

Between 2019 and 2020, there were three attacks on water systems. **The first attack caused a change in the chlorine level** in the water and a consequent deterioration of the water quality in the system, while the other attacks in 2020 changed the operating points of the pumping stations, **which caused an increase in the system pressure and a corresponding increase in leaks**

some recommendations to address the cybersecurity challenges facing smart city services

1. **Implement cybersecurity standards:** standard security protocols such as encryption, access control and authentication must be implemented to protect smart city systems from cyber-attacks.

2. **Update devices regularly**: smart city devices should be updated regularly to address identified vulnerabilities and prevent cyber-attacks.



3. **Develop a comprehensive cybersecurity strategy:** smart cities should develop a strategy that comprises the risk assessments, incident response plans, and employee training programs.

4. **Collaborate with cybersecurity experts**: smart cities should collaborate with cybersecurity experts to identify vulnerabilities and develop effective solutions to address them.

5. **Monitoring and auditing systems:** smart cities have to monitor and audit their systems regularly to detect and respond promptly to any cyber security incidents.

Conclusion

In the concept of smart city, all services are of great significance, consequently certain demands are set forth on their security and reliability. Vulnerabilities in smart city include a lack of centralized infrastructure, which creates problems in the fight against cyber-attacks. And it becomes very problematic to detect attackers. Hence, for each smart city service, by studying the attack scenarios and their effects, various solutions have to be employed to avoid these attacks. These solutions include applying cybersecurity standards, regularly updating devices, developing a comprehensive cybersecurity strategy, collaborating with cybersecurity experts, monitoring and auditing systems, etc.

Further research should focus on the development of new approaches and technologies to improve the cyber security of critical infrastructures in smart cities. Consequently, smart cities can provide their residents with a safe urban environment benefitting from the power of technology.