Cybersecurity governance in large-scale infrastructures

Răzvan STOLERIU[1], Ionuț PETRE[2], Florin POP[1,2,3]

[1] National University of Science and Technology Politehnica Bucharest, Romania

[2] National Institute for Research & Development in Informatics – ICI Bucharest, Romania

[3] Academy of Romanian Scientists, Romania

raz.stoleriu@gmail.com, ionut.petre@ici.ro, florin.pop@ici.ro, florin.pop@upb.ro

Abstract: The fast technological development in smart cities is meant to increase humans' conditions of life, but at the same time, it comes with various challenges and risks. People are already connected via gadgets and smartphones, while intelligent systems and appliances are utilized in many cities. Home devices, cars, and public venues are interconnected and communicate by sending data to each other, forming the Internet of Things. However, this opens new opportunities for malicious actors to launch different attacks that may have a destructive impact on the important infrastructures in a city. This paper proposes a framework for cybersecurity risk assessment in large-scale infrastructures alongside mitigation techniques and countermeasures. The methodology employed in the study is a qualitative one. It is based on 66 projects from the CORDIS database of the European Commission that are related to cybersecurity governance in smart cities. They are focused on research and innovation and held between 2022 and 2027. The work brings a significant contribution to the scientific community as it identifies the security risks in large-scale infrastructure and proposes mitigation techniques and countermeasures for these challenges.

Keywords: Cybersecurity, Governance, Large-Scale Infrastructures, Smart City, Cyber-Attacks.

Guvernanța securității cibernetice în infrastructurile la scară largă

Rezumat: Dezvoltarea rapidă a sistemului tehnologic în orașele inteligente este menită să crească condițiile de viață ale oamenilor, dar, în același timp, vine cu diverse provocări și riscuri. Oamenii sunt deja conectați prin diverse dispozitive mobile, în timp ce sistemele și echipamentele cu capacități avansate de procesare sunt deja utilizate în multe orașe. Dispozitivele de acasă, mașinile și locurile publice sunt interconectate și comunică prin trimiterea de date între ele, formând Internetul lucrurilor. Totuși, aceste aspecte deschid noi oportunități pentru utilizatorii rău intenționați, care pot lansa diferite atacuri cibernetice cu un impact distructiv asupra infrastructurilor importante și critice dintr-un oraș. Acest articol propune un cadru pentru evaluarea riscului de securitate cibernetică în infrastructurile distribuite la scară largă, propunând tehnici și contramăsuri de atenuare. Metodologia folosită în studiu este una calitativă. Aceasta se bazează pe 66 de proiecte din baza de date CORDIS a Comisiei Europene, care au legătură cu guvernanța securității cibernetice în orașele inteligente. Proiectele analizate sunt axate pe cercetare și inovare, desfășurate pe perioada anilor 2022 și 2027. Lucrarea aduce o contribuție semnificativă comunității științifice, deoarece identifică riscurile de securitate în infrastructuri distribuite la scară largă și propune măsuri de gestiune pentru acestea.

Cuvinte cheie: securitate cibernetică, guvernanță, infrastructuri distribuite la scară largă, orașe inteligente, atacuri cibernetice.

1. Introduction

Many cities around the world risk facing problems concerning life conditions since they have important issues regarding the security, scalability, and the environment of their infrastructures. This is due to the population growth that will reach 9.8 billion in 2050 (United Nations, 2017). As a result, the urban environment will encounter both challenges and benefits. Some of the difficulties that it would face are represented by the fact that the education and the health sectors will need new approaches, the economy will have issues, the energy consumption will increase, public safety will face new risks, and the possibility of cyberattacks against cities is high. The key solution for these problems is innovative, scalable, and cost-effective infrastructures (Khatoun & Zeadally, 2017). With the growing number of the world population, the tasks the people are requiring become more

https://doi.org/10.33436/v35i1y202504

demanding. All of the devices that are inter-connected inside a network and perform the actions asked by end-users to fulfill their needs also come with various security challenges. As the global tendency is to migrate to large-scale infrastructures that represent a big project involving anything from installing power grids, establishing dams, and expanding a hospital wing to constructing a new school. All of these facilities ensure improving people's quality of life (Vickerman, 2007).

Nowadays, Internet of Things (IoT) devices become more adopted in various buildings and infrastructures since they bring many advantages such as energy save, efficient space storage, automation, and fast response time (European Commission, 2022). This way, many constructions get spaces with connected devices that communicate through various protocols. As data are sent to the servers in the cloud for auditing and storage, the attackers can leverage the vulnerabilities in there (e.g., open ports, weak credentials, out-of-date software) to exploit and conduct more sophisticated cyber-attacks (Yu et al., 2020; Jayaraman et al., 2023).

IoT devices also play a crucial role and are at the base of smart city infrastructure. They gather different information from the environment, process and analyze it, and then pass it to other interconnected devices. Finally, the data can be accessed by the people who are interested. According to a recent study, the number of IoT devices will exceed 75 billion by 2025. This is also facilitated by the 5G technology as it allows an increased number of simultaneous connections. The IoT devices also play a vital role in the prevention of natural disasters. For instance, certain sensors can monitor the wind speed or water level and determine the population that may be vulnerable to such disasters. IoT, blockchain, and artificial intelligence-driven technologies are complementary and help provide high-quality services, improving life conditions and the user's experience (Radu, 2020).

The services in a smart city can belong to various domains, such as transportation, healthcare, environment, security, and energy. The most widely adopted smart city model is the one proposed by NIST. A cyber-attack that exploits a vulnerability in one of the components of a smart city can put the entire city at risk. Given the fact that the amount of data that is generated in an infrastructure is huge, the digital forensic operation represents a challenge. The same concern hits the smart grid. A viable option for storing the huge amount of data that comes from there is the cloud. Security solutions based on anomaly detection are useful in this case since they can operate on traffic patterns to identify compromised devices. Smart grid threats may have an impact on the privacy and integrity of data, and network availability. Some adversaries may launch attacks that allow them to discover the number of users in a house or the types of appliances that are in use (Baig et al., 2017).

Smart cities also comprise smart buildings. They are inherited with different services, such as heating, ventilation, and air conditioning (HVAC) equipment, closed-circuit television (CCTV), elevators, and water and energy systems. Users can remotely control and interact with them via the sensors connected to the Internet. Some security threats that target the systems in smart buildings are physical damage and denial-of-service (DoS) attacks. A big concern is represented by the fact that usually, there is no authentication in the protocols used by the systems in the smart buildings as the devices trust each other for the actions they perform (Baig et al., 2017).

Smart cities are becoming more and more populated with both civilian and commercial unmanned aerial vehicles (UAVs) and drones. Nowadays, a drone is price accessible and usually comes inherited with an onboarding camera, leaving the possibility open to add extra customizable features. It has been observed that drones are used these days for package delivery, coast patrol, and distribution of insecticide for agricultural surfaces. Some security threats could emerge from the civilian drones as they utilize unsecured Wi-Fi connections, and the onboard system that is Linux-based uses an account with privileged rights and open FTP and Telnet ports. One of the mitigation techniques proposed over time was the use of encryption over the communication channels to make them secure. Adversaries may launch sophisticated attacks that could lead to video interception, communication/ connection disruption, and total system control (Baig et al., 2017).

Smart healthcare proposes to offer patients better diagnosis and treatment procedures supported by good technology at costs as low as possible. The medical systems in smart healthcare allow patients to have an easier way to communicate with doctors and be carefully monitored. IoT devices, such as sensors, wearables, and home-monitoring solutions are meant to offer more in-depth investigations. Cyber threats that target medical devices and systems are DoS, sensor, and eavesdropping attacks. Blockchain technology could be used to increase the data privacy and security. Moreover, encryption algorithms should be considered when storing medical records in the cloud (Demertzi, Demertzis, & Demertzis, 2023).

Although there are many papers in the literature that identified security flaws in IoT devices, there are only a few solutions that have been proposed to patch and mitigate the potential attacks. There are not many vendors that support patches after the sale of their products. Beyond the security protections provided by the supplier, a potential direction would be to monitor and lock down the malicious traffic that comes from or goes to the IoT devices (Sivaraman et al., 2015). But, this requires the knowledge of the expected traffic of that system when it is deployed in an enterprise or commercial environment.

The corporate world experienced both physical and cyber security threats during the pandemic times when employees were sent home to work. Then malicious actors stole the IT assets from the vacated buildings to exploit and obtain information. To combat the nowadays sophisticated attacks, organizations need to combine both the physical (e.g., security cameras, strong gates, guardians) and software (e.g., Anti-Virus solutions, Firewall, Intrusion Detection / Prevention Systems) security approaches so that they can automatically respond to incoming threats (Hamza et al., 2022).

This paper proposes a model for cybersecurity risk assessment in large-scale infrastructures alongside mitigation techniques and countermeasures. The methodology employed in the study is a qualitative one. It is based on 66 projects from the CORDIS database of the European Commission that are related to cybersecurity governance in smart cities. They are focused on research and innovation and belong to the date range between 2022 and 2027. The work brings a significant contribution to the scientific community by identifying the security risks in large-scale infrastructure and proposing mitigation techniques and countermeasures for these challenges.

The rest of the paper is structured as follows: Section 2 presents an analysis of similar papers that deal with the cybersecurity risk assessment in large-scale infrastructures, Section 3 presents the proposed methodology, and Section 4 highlights the obtained results. Finally, Section 5 draws the conclusions and identifies future research opportunities.

2. Literature review

This section provides some limited research in the field that addresses the cybersecurity challenges and solutions for large-scale infrastructures. Although many scientific contributions have been made by scientists, this section only tries to expose the most important ones for the subject. In smart cities, for example, the authors are concerned about the security and privacy of data. Cybersecurity depends there on three important factors: governance, the socio-economic sector, and the technological one. Some of the key areas related to governance are infrastructure, health, transport, and education. The concerns associated with the socio-economic sector are people's safety and communications, while as regards the technological ones there are smartphones, Radio-Frequency Identification (RFID), and Machine-to-Machine (M2M) communications (Hamid et al., 2019). Some of the potential works for cybersecurity risk assessment are listed in Table 1.

Table 1. Potential works for cybersecurity risk assessment in large-scale infrastructures

References	**All areas of a large-scale infrastructure**	**Proposed security solutions**	**Methodology**	**Observations**
Elmaghraby & Losavio (2014)	× Transportation	×	IBM IN3	Focus on the transportation sector.
Belgaum et al. (2018)	✓	×	Fuzzy Analytic Hierarchy Process	Study areas in Smart Cities impacted by cyber security attacks and try to assign a rank to each of them.
Kalinin, Krundyshev & Zegzhda (2021)	✓	×	Artificial neural network (ANN)	Artificial Neural Networks (ANNs) for cyber-security risk assessment.
Elsaeidy et al. (2017)	✓	×	Deep neural network	New model to identify DoS attackers for smart city applications.

Hamza et al. (2022)	✓	×	Machine Learning	Machine learning technique to detect cyberattacks in an IoT infrastructure.
Ten, Manimaran & Liu (2010)	× SCADA systems	✓	Framework	SCADA systems – framework with the following components: real-time monitoring, anomaly detection, impact analysis, and mitigation strategies.
Alam & Ibrahim (2019)	✓	×	Actor-Network Theory framework	Cybersecurity strategies in the development of smart cities.
Alamer & Almaiah (2021)	× SCADA systems, IoT	✓	Systematic mapping study	Scientific articles review, the papers' screening, the keywords generation from the abstracts, and the mapping to production.
Jiang et al. (2023)	× Power grid	✓	Design science research	Security taxonomy of the information and operational technology entities along with a vulnerability assessment program to identify security breaches.
Mohamed, Al-Jaroodi & Jawhar (2020)	× Applications	✓	Data-driven-based approach	Data-driven based methodology for securing applications in a Smart City.
Almeida (2023)	× IoT systems	✓	Qualitative methodology	Cybersecurity risks in smart cities and mitigation actions.
Yusif & Hafeez-Baig (2021)	× Applications	×	Research and literature survey	Cyber-risks across organizations and highlights the most targeted industries.
Melaku (2023)	×	×	Design science research method	The framework's processes and strategies are presented in general and not showcased to industries.
Maleh, Sahid & Belaissaoui (2021)	×	×	Qualitative description and design science	Framework focusing on organization's security posture evaluation and digital information protection.
De Bruin & von Solms (2015)	×	✓	Literature review	Framework consisting of five maturity models and different security practices.
Vinnakota (2016)	×	×	Cybernetic control systems	Cybersecurity governance model that comprises strategies, resources, security initiatives, and threat scanning.
Proposed model	✓	✓	Qualitative methodology	Emphasizes the cybersecurity threats in large-scale infrastructures and proposes mitigation actions.

Many research papers propose the integration of Artificial Intelligence for the security of large-scale infrastructures. For instance, some authors employ Artificial Neural Networks (ANN) in their solutions for cyber-security risk assessment. The perceptron model with the backpropagation algorithm is used for training. An accuracy of 97% has been achieved (Kalinin, Krundyshev & Zegzhda, 2021). Other researchers use a Deep Learning-based model to identify attack patterns in the network traffic. Each layer in the model uses the restricted Boltzmann machine. On the HTTP Flood attack dataset, they obtained an F1 score of 80% (Elsaeidy et al., 2017). Some solutions use Machine Learning to analyze the traffic generated by the IoT infrastructure and detect attacks. In their study, they consider device information and network configuration, and they achieve a detection rate of 92.5% (Hamza et al., 2022).

Other research papers are oriented to cybersecurity integration in the development of smart cities. For instance, Alamer & Almaiah (2021) propose a methodology that addresses the security challenges in smart cities. They study several research papers, outline the main keywords and use them to generate content in the designed solution. Based on their findings, they identify security challenges, detection techniques, and countermeasures. Alam & Ibrahim (2019) study cybersecurity strategies in the development of smart cities. As a first step, they determine the factors involved in cybercrime handling based on the technological, human, and institutional perspectives. Technology is the main component since it makes the functionalities of Smart cities available and properly work. Humans are the beneficiaries of Smart applications and use them in daily activities. Institutions represent the places where citizens utilize technological services. Mohamed et al. propose a data-driven based methodology for securing applications in a Smart City. Their study brings fast identification and inspection of security breaches and improvement of the defense mechanisms and security management processes (e.g., auditing, upgrading, recovery). At the end of their paper, they include a table with challenges and possible solutions for various categories of applications. Almeida uses in his study a qualitative methodology to highlight the main cybersecurity challenges in smart cities and proposes countermeasures. He took 62 projects related to security risks from the CORDIS database, imported them into the NVivo program for analysis, and obtained the areas that are the most vulnerable to attacks in a smart city. Finally, he came up with mitigation techniques for each of the latter.

Elmaghraby & Losavio (2014) analyze the two most important challenges of smart cities: security and privacy. Moreover, they also present a model that describes the interactions between persons, servers, and things. The researchers use in their analysis the IN3 principle from the IBM methodology. IN3 comes from intelligent, instrumented, and interconnected and establishes the relationships between humans, the smart city, and its components. Instrumented refers to the fact that the humans' devices and the city's components are guided and instructed by a sensor from the network. These are interconnected as the information is passed through the network. Finally, that information is available for analysis and decision-making causing the smart city to be intelligent. They focus more on the transportation sector, where they emphasize different sources of data and data types and address some security and privacy issues. They present in detail what components are vulnerable and what kind of attacks could be conducted. However, they do not propose any solutions or mitigation techniques for the security threats they identified.

Belgaum et al. (2018) study in their research the main areas in Smart Cities that are impacted by cyber security attacks. They reviewed numerous scientific papers and materials from experts in the field, and as a result, they divided the areas into nine groups (e.g., Smart Healthcare, Smart Technology). Each group is split into three or four sub-groups (e.g., Intelligent Healthcare, Intelligent Mobility). The authors used the Fuzzy Analytic Hierarchy Process (FAHP) to calculate the weights of the groups and sub-groups. Finally, the obtained results highlight the area most impacted by cyber-security attacks is "Smart Security," while the one that is the least affected is "Smart Building." On the other hand, the most impacted sub-area is "Surveillance and Biometrics," while the least affected is "Advanced Heating Ventilation and Air Conditioning Systems."

Ten, Manimaran & Liu (2010) propose a security framework for SCADA systems that consists of multiple phases. The first one is called real-time monitoring and deals with the interception of network packets. A case study would be the detection of DoS attacks. The next phase is called anomaly detection, and it is based on event correlation from various sources. The impact analysis phase finds the vulnerabilities of the components and computes the potential loss they can bring in the case of an attack. The last phase, the mitigation strategies, begins with the most vulnerable component and proposes mitigation strategies. Furthermore, the authors propose a methodology based on an attack tree for cybersecurity evaluation. It considers the auditing of ports and policies implemented for passwords.

Jiang et al. (2023) propose a taxonomy for the security of the information technology (IT) and operational technology (OT) entities. They focus on the cyber and cyber-physical domains of critical infrastructures (CIs). They reviewed several research papers concerning the architecture and fundamental components of the power grid networks. Further, they leveraged a vulnerability assessment tool and standards from NIST to identify potential security breaches. The proposed taxonomy has been implemented in a program called ConceptBase.

Yusif & Hafeez-Baig (2021) propose a model for cybersecurity governance that considers multiple key points, such as processes, goals, strategies, and resources. In their paper, they present the most popular cybersecurity risks, the industries that face them (e.g., healthcare, education, finance), and the infrastructures targeted by attackers. The researchers outline how Internet exposure brings flexibility and user satisfaction at the price of vulnerabilities, data leaks, and other security concerns. They state that the human factor can be responsible for multiple security breaches.

Melaku (2023) proposes a cybersecurity governance framework based on the design science research method and assures, among others, the management of risks and the organization’s resources. The proposed framework considers strategies for incident management, business continuity, and disaster recovery, and its efficiency is measured via evaluation techniques and performance metrics. The author does not present how the framework behaves in specific industries, but he describes its capabilities in general.

Maleh, Sahid & Belaissaoui (2021) propose CYBERGOV, a cybersecurity governance framework that can be used to evaluate and bring improvements to the security posture of an organization. This paper represents a qualitative descriptive study, and for the data collection part, the researchers reviewed multiple scientific articles and case studies. CYBERGOV protects digital information by monitoring for data disclosure, operations disruption, and unauthorized access. The framework also assures the confidentiality, integrity, and availability of data.

De Bruin & von Solms (2015) propose a cybersecurity governance framework that helps organizations assess their maturity level. The framework comprises five maturity models and outputs a dashboard where organizations can check their security posture. Every model was selected by literature review and is divided into technology, processes, and people. Each of those three components contains four levels of practice, the last one corresponding to the highest maturity level. At the end of the article, researchers present a formula that is based on the results of the five maturity models. It assesses an organization's cybersecurity governance maturity.

Vinnakota (2016) designs a cybersecurity governance model for enterprises. It comprises security initiatives, strategies, resources, performance assessment, and threat identification via external and internal environment scanning. The author presented a case study where the proposed model was adopted by a telecom organization. There, it brought a plus of value by providing increased security, efficiency, and production improvements.

In comparison with the above-described models, the present one is mapped to all areas of large-scale infrastructure and is based on modern research projects that leverage cutting-edge technologies. Moreover, this model strengthens the security posture for each area of a large-scale infrastructure by identifying the main security threats and proposing effective countermeasures.

3. Methodology

To identify the ongoing development trends for the smart era we live in, our study began by evaluating research projects of the European Commission. They are stored in the CORDIS database and belong to different fields of activity, such as medicine, transport, buildings, education, and technology. They are proposed and implemented by universities, research centers, and corporates. By filtering the projects by the two most important themes of the paper, ″cybersecurity″ and ″infrastructure″, 66 results were obtained. Then, each project was taken and imported into NVivo 14, a tool for qualitative data analysis. A theme was assigned to each of the projects and the ones belonging to the same type were grouped together so that the most prevalent sectors of activity or areas of a large-scale infrastructure could be identified. Based on them, the security risks were spotted, and the potential mitigation techniques and countermeasures were decided. Table 2 briefly presents the steps adopted in this methodology.

Table 2. The proposed methodology

Phase	Description
1.Data gathering	Searching for research projects of the European Commission in the CORDIS database.
2.Data filtering	Filtering the projects by the ″cybersecurity″ and ″infrastructure″ keywords.

3.Project import	Taking each obtained project and importing it into NVivo 14, a tool for qualitative data analysis.
4.Theme assigning	Analyzing each project and assigning a theme to it.
5.Theme grouping	Grouping the themes of the same type together and identifying the main areas they belong to.
6.Security risks	Analyzing each identified area from a large-scale infrastructure and assigning security risks.
7.Mitigation	Proposing mitigation techniques and countermeasures for the identified security risks.

Tables 3 to 12 contain the research projects from the CORDIS database, mapped to the main areas of a large-scale infrastructure. Based on them, the main security risks and the potential countermeasures are highlighted.

Table 3. Research projects for the technology area

Project	Start Date	Duration	Objective
COBALT	1 November 2023	3 years	Certification scheme for cybersecurity using decentralized digital twinning.
DA23	1 January 2023	9 months	Opportunities offered by Europe's digital transformation.
DISCOVER-US	1 January 2024	2.5 years	Research on computing continuum, distributed computing and swarm intelligence.
ELSA	1 September 2022	3 years	Proposes a virtual center of excellence on safe and secure AI.
EMERALD	1 November 2023	3 years	Develops a certification-as-a-service solution.
EXTRACT	1 January 2023	3 years	Software platform that will utilize computing technologies.
FAST-STREAM	1 May 2022	2 years	Maximizes the quality for adaptive video streaming and video conferencing.
HORSE	1 January 2023	3 years	Services for future 6G wireless and computing ecosystems.
NEMO	1 September 2022	3 years	Proposes the next generation of open, modular and cybersecure meta-operating system.
NOUS	1 January 2024	3 years	Develops the architecture of a European Cloud Service.
ODEON	1 January 2024	4 years	New framework for the complete life cycle of Data/AIOps.
PQ-REACT	1 September 2023	3 years	Develops a framework for the transition from classical to post-quantum cryptography.
QSNP	1 March 2023	3.5 years	Creates a sustainable European ecosystem in quantum cryptography and communication.
QUBIP	1 September 2023	3 years	Contributes to the EU transition to post-quantum cryptography.
RIGOUROUS	1 January 2023	3 years	Improves the security, privacy and trust in 6G and other computing technologies.
SPECTRUM	1 January 2024	2.5 years	Delivers research in the field of compute and data continuum.

Table 4. Research projects for the security area

Project	Start Date	Duration	Objective
CS-AWARE-NEXT	1 July 2022	3 years	Improved cybersecurity management capabilities to organizations and supply networks.
CyberSecDome	1 September 2023	3 years	Integrates advanced virtuality reality to extend the capability of the security solutions.
DYNABIC	1 December 2022	3 years	Business continuity of critical infrastructures.
DYNAMO	1 October 2022	3 years	Combines business continuity management and cyber threat intelligence.
KINAITICS	1 October 2022	3 years	Explores the attack opportunities of AI-based control and perceptive systems.
ORSHIN	1 October 2022	3 years	Researches on models and tools to protect OSH devices (i.e., IoT ones) from critical threats.

PHOENI2X	1 July 2022	3 years	Develops a Cyber Resilience Framework providing AI for business continuity and recovery, incident response.
QSI	1 October 2022	4 years	Provides expertise to problems in secure communications in the quantum era.
ROBUST-6G	1 January 2024	2.5 years	Addresses the cybersecurity risks introduced by the expansion of the 6G threat landscape.
Sec4AI4Sec	1 October 2023	3 years	Develops security-by-design techniques for AI-augmented systems and AI assets.
SQPRIM	1 July 2023	2 years	Provides hardware-based digital identifiers for encryption and authentication.
SYNAPSE	1 November 2023	3 years	Develops an Integrated Cyber Security Risk & Resilience Management Platform.

Table 5. Research projects for the healthcare area

Project	Start Date	Duration	Objective
AI-driven cardiac ultrasound analysis	1 August 2022	2.5 years	Automates the analysis of heart ultrasound images by using AI.
BioMedAI TWINNING	1 November 2022	3 years	Processes sensitive images and clinical data with the help of AI.
CutCancer	1 January 2023	3 years	Implements cutting-edge approaches in the field of preclinical 3D cancer research.
CYLCOMED	1 December 2022	3 years	Strengths the cybersecurity of software as medical devices.
eBRAIN-Health	1 July 2022	4 years	Generates Digital Twins of patients and healthy controls to study dementia.
ERA_SHUTTLE	1 September 2023	4 years	Proposes a framework to address current health and environmental challenges.
MEDSECURANCE	1 January 2023	3 years	Brings innovation for the Internet of Medical Things.
OH-Boost	1 January 2023	3 years	Research in the domain of One Health (human, animal, environmental health).
SEPTON	1 December 2022	3 years	Develops a cybersecurity toolkit capable of protecting networked medical devices.

Table 6. Research projects for the energy area

Project	Start Date	Duration	Objective
COCOON	18 September 2023	3 years	Safeguards Information Technology and OT environments.
eFORT	1 September 2022	4 years	Increases reliability and resiliency for energy grids.
HYPOBATT	1 June 2022	3.5 years	Interoperable charging solution, cost-competitive performance.
PROMISE	1 October 2022	3 years	Prediction and optimization algorithms for energy transition.
SALTOpower	1 November 2022	3 years	Molten salt for energy storage and dispatchable power production.
SAN4Fuel	1 November 2022	3 years	Production of clean energy sources based on green fuels.
SUNRISE	1 January 2023	3 years	Improves excellence in the power system decarbonization process.
TESTARE	1 January 2023	3 years	Excellence and innovation in Photovoltaic technology testing.

Table 7. Research projects for the environment area

Project	Start Date	Duration	Objective
FONDA	1 January 2023	3 years	Boosts the expertise in modelling reactive nitrogen.
NGS-4-ECOPROD	1 October 2022	3 years	Novel biotechnology products to replace chemical products.

ORCHIDE	1 December 2023	2.5 years	Innovation for image processing applications within Earth Observation satellites.
PaleoMIX	1 January 2023	3 years	Integrates cutting-edge techniques into bioarchaeology for the study of tangible heritage.
PANGEA4CalVal	1 October 2022	3 years	It supports frontier environmental and climate research.
Sol2H2O	1 December 2022	3 years	Strategies for new closed-loop water desalination processes.
CLiCAM	1 September 2023	4 years	Develops technologies in life science and advanced manufacturing and materials.

Table 8. Research projects for the infrastructure area

Project	**Start Date**	**Duration**	**Objective**
aerOS	1 September 2022	3 years	Novel operating system for edge-cloud continuum.
ResilMesh	1 October 2023	3 years	Develops a cyber situational awareness to improve digital infrastructure resilience.
CERTIFY	1 October 2022	3 years	Implements a cybersecurity life cycle management framework for IoT devices.
TELEMETRY	1 September 2023	3 years	Tools that enable continuous assessment in IoT ecosystems.

Table 9. Research projects for the transportation area

Project	**Start Date**	**Duration**	**Objective**
CNS DSP	1 September 2023	3 years	New concept for air traffic management data service providers.
MariTech Talent	1 December 2023	2 years	Skills development program for the maritime industry.
NextETRUCK	1 July 2022	3.5 years	The project will demonstrate innovative and affordable zero-emission e-mobility concepts.
SELFY	1 June 2022	3 years	Develops tools for situational awareness, data sharing, resilience and trust for vehicles.

Table 10. Research projects for the education area

Project	**Start Date**	**Duration**	**Objective**
AIoTwin	1 January 2023	3 years	Spreads excellence in Artificial Intelligence of Things.
BRIDGE	1 October 2022	3 years	Boosts the excellence in cutting-edge research and innovation.
TED4LAT	1 October 2022	3 years	Twinning between research institutions to increase the knowledge in the ICT science.

Table 11. Research projects for the citizen area

Project	**Start Date**	**Duration**	**Objective**
AHEAD	1 September 2023	2.5 years	Proposes a civil security foresight framework.
ATHENA	1 November 2023	3 years	Defense against foreign information manipulation and interference.

Table 12. Research projects for the governance area

Project	**Start Date**	**Duration**	**Objective**
NGI Commons	1 January 2024	3 years	Key governance issues: digital sovereignty and cybersecurity.

4. Results

Once all the projects from the CORDIS database were obtained, they were imported into NVivo 14, a tool for qualitative data analysis. There, each project was processed and assigned a theme based on its objectives. The themes that correspond to a specific area in a large-scale infrastructure have been grouped.

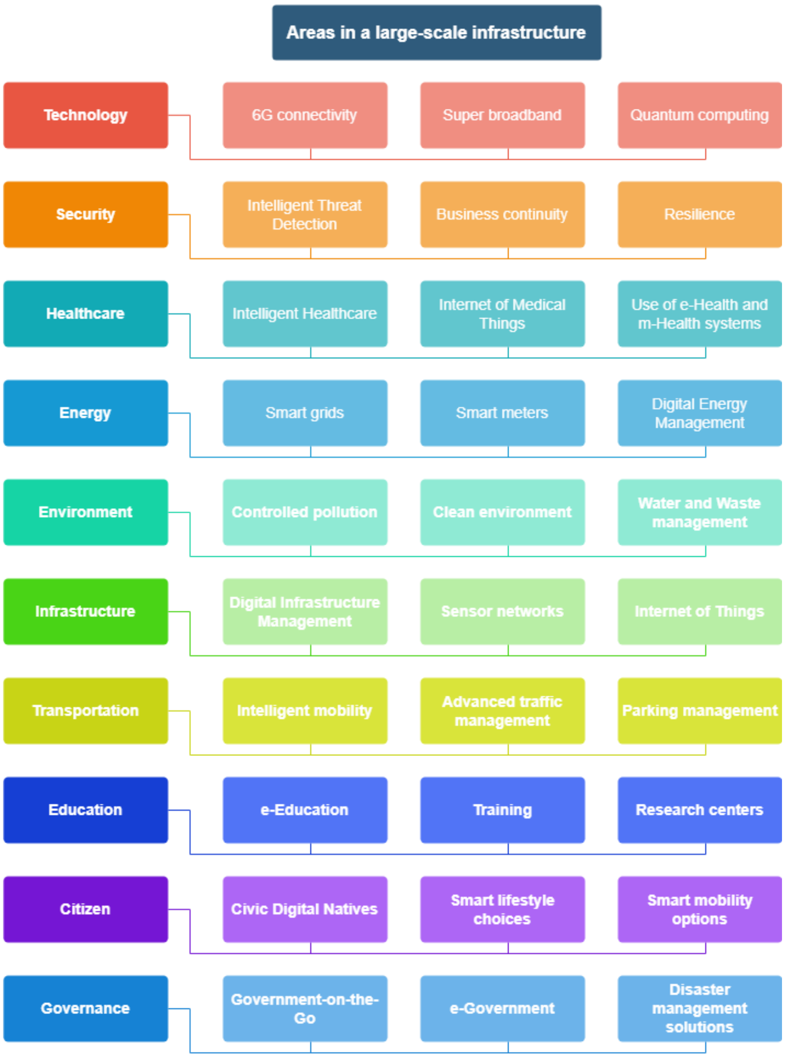

Figure 1. Main areas of a large-scale infrastructure prone to cybersecurity challenges

The areas highlighted in Figure 1 have been identified by reviewing various research papers from the literature (Angelidou, 2014; Eremia, Toma & Mihai, 2017; Khatoun & Zeadally, 2017; Belgaum et al., 2018; Hamid et al., 2019; Radu, 2020). In comparison to the above-mentioned papers, this one is based on modern research projects, most of them having an end date in the future. Cutting-edge technologies are extracted, the current cybersecurity threat landscape for large-scale infrastructures is identified, and efficient countermeasures are proposed. For each area, Table 13 presents the security threats and potential countermeasures. Also, in Table 13 the number of projects from the CORDIS database selected for each domain is specified. The threats column refers to the main cyber-security challenges that target a specific area. Multiple research papers from the literature have been reviewed to define them. The countermeasures column proposes actions that could be taken to defend and prevent cyber attacks. It also contains, for each item, the number of projects it covers. The value represents the sum of all projects that implement or should employ that specific countermeasure. One project may need or contain more countermeasures.

The coverage column displays a mapping between projects and the number of countermeasures they either implement or should employ.

Table 13. The main threats and potential countermeasures

Area	Threats	Countermeasures	Coverage
Technology 16 projects	- Unauthorized access - Man-in-the-middle attacks - Stole research & development data - Vulnerability exploitation	- Vulnerability assessment – 10 projects - Authentication and authorization mechanisms – 6 projects - Intrusion detection systems – 10 projects - Data Loss Prevention systems – 5 projects	- 1 project approaches 4 countermeasures - 2 projects approach 3 countermeasures - 8 projects approach 2 countermeasures - 5 projects approach 1 countermeasure
Security 12 projects	- Code vulnerabilities - Out-of-date database of malware signatures - Killing the anti-virus (AV) process	- Make a more secure code – 7 projects - Keep an up-to-date database of malware signatures – 0 projects - Prevent the AV process from being killed by malicious software – 0 projects - Threat Intelligence data integration – 6 projects - Disaster recovery/business continuity plan – 7 projects	- 1 project approaches 3 countermeasures - 6 projects approach 2 countermeasures - 5 projects approach 1 countermeasure
Healthcare 9 projects	- Sensitive data exposure - Disrupting the services - Eavesdropping sensitive information - Sending fake information - Patients' data alteration	- Secured Wi-Fi networks to guarantee safe handling of confidential information and personal data (e.g., AirTight Networks solutions) – 6 projects - Risk assessment (e.g., Intel healthcare security solutions) – 4 projects	- 2 projects approach 2 countermeasures - 7 projects approach 1 countermeasure
Energy 8 projects	- Unauthorized access and controls - Botnets (e.g., Zeus, Conficker) - Denial of service (DoS) and distributed denial of service (DDoS) attacks	- Intrusion detection and prevention systems (e.g., Snort) – 3 projects - Cyber Threat Intelligence – 2 projects - Risk assessment methodologies (e.g., MEHARI, EBIOS) – 8 projects	- 2 projects approach 3 countermeasures - 1 project approaches 2 countermeasures - 5 projects approach 1 countermeasure
Environment 7 projects	- Attacks against the network and PLCs - System compromise - Vulnerabilities	- Vulnerability patching – 2 projects - Security monitoring solutions – 6 projects - Water Information Sharing and Analysis Center, American Water Works Association – 1 project	- 2 projects approach 2 countermeasures - 5 projects approach 1 countermeasure
Infrastructure 4 projects	- Supply chain attacks - Insecure communication - Weak authentication	- Asset inventory and risk assessment – 3 projects - Security patching and updates – 3 projects - Supply chain security – 3 projects	- 2 projects approach 3 countermeasures - 1 project approaches 2 countermeasures - 1 project approaches 1 countermeasure
Transportation 4 projects	- Braking system disruption - Engine stopping - Displaying false messages at the on-board computer - Changing GPS signals	- The use of cryptography (digital certificates, Public key infrastructure, data encryption) – 3 projects - Solutions for anomaly detection – 1 project	- 1 project approaches 2 countermeasures - 2 projects approach 1 countermeasure - 1 project (i.e., NextETRUCK) does not cover any of these main countermeasures

Education 3 projects	- Data breaches - Personal information compromise - Ransomware attacks	- Anti-malware and anti-virus software – 0 projects - Using strong passwords – 0 projects - Security awareness training – 3 projects	- 3 projects approach 1 countermeasure
Citizen 2 projects	- Cybercrime - Identity theft	- Awareness training – 2 projects - Use of strong passwords – 0 projects	- 2 projects approach 1 countermeasure
Governance 1 project	- Disrupting critical infrastructures - Fiscal fraud - Altered files	- Data Loss Prevention solutions (e.g., Symantec, Fortinet) – 0 projects - Risk assessment methodologies (e.g., MEHARI, EBIOS) – 1 project - Insider threat analysis – 0 projects	- 1 project approaches 1 countermeasure

Based on the Table 13 results, an area of a large-scale infrastructure can be considered vulnerable if one of the proposed security countermeasures is not implemented by a research project. As a result, it can be observed the most vulnerable areas are security, education, citizen, and governance. The proposed mitigation methods strengthen the security posture of the considered areas, making them more resilient to cyber-attacks. For large-scale infrastructure areas to remain secure, future research projects should follow the best security standards and guidelines, such as the ones defined by the National Institute of Standards and Technology (NIST) or the European Union Agency for Cybersecurity (ENISA).

5. Limitations

In this paper, the main cybersecurity challenges for large-scale infrastructures were identified. The obtained results are limited since the search for research projects in the CORDIS database was only for the ″cybersecurity″ and ″infrastructure″ keywords. If other terms had been added in the search, such as ″smart city″ and ″governance″ maybe more results would have been obtained. Thus, the domains of activity would be larger, and the range of identified threats and proposed countermeasures would be bigger. In this way, the study analyzes some areas and might not treat all the domains that large-scale infrastructures are compound of.

6. Conclusions and future work

This paper proposes a model for cybersecurity risk assessment in large-scale infrastructures alongside mitigation techniques and countermeasures. The study employs a qualitative methodology by identifying 66 European research projects from 2022 to 2027 that are related to cybersecurity governance in large-scale infrastructures. They were imported into the NVivo tool for qualitative data analysis. There, they were grouped by their sector of activity so that the most prevalent areas could be identified. The latter were split in the main components based on which the cybersecurity threats were identified.

The results of this work offer significant scientific contributions by identifying security risks in large-scale infrastructure and proposing mitigation techniques and countermeasures for these challenges.

In terms of future work, the authors intend to enrich the current model by presenting some practical use cases where real data breaches can be described. It would be useful since there they could come up with concrete and specific intrusion detection tactics and countermeasures.

REFERENCES

Alam, R. & Ibrahim, H. (2019) Cybersecurity Strategy for Smart City Implementation. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences (ISPRS)*. XLII-4/W17, 3-6. doi:10.5194/isprs-archives-XLII-4-W17-3-2019.

Alamer, M. & Almaiah, M. A. (2021) Cybersecurity in Smart City: A Systematic Mapping Study. *2021 International Conference on Information Technology (ICIT), Amman, Jordan, 2021*. IEEE. pp. 719-724. doi: 10.1109/ICIT52682.2021.9491123.

Almeida F. (2023) Prospects of Cybersecurity in Smart Cities. *Future Internet*. 15(9), 285. doi: doi:10.3390/fi15090285.

Angelidou, M. (2014) Smart City Policies: A Spatial Approach. *Cities*. 41(1), S3-S11. doi:10.1016/j.cities.2014.06.007.

Anindra, F., Supangkat, S. H. & Kosala, R. R. (2018) Smart Governance as Smart City Critical Success Factor (Case in 15 Cities in Indonesia). *2018 International Conference on ICT for Smart Society (ICISS), Semarang, Indonesia, 2018*. IEEE. pp.1-6. doi:10.1109/ICTSS.2018.8549923.

Baig, Z., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N. & Peacock, M. (2017) Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*. 22, 3-13. doi:10.1016/j.diin.2017.06.015.

Belgaum, M. R., Alansari, Z., Jain, R. & Alshaer, J. (2018) A Framework for Evaluation of Cyber Security Challenges in Smart Cities. *Smart Cities Symposium 2018, Brahain, 2018*. IEEE. pp. 1-6. doi:10.1049/cp.2018.1372.

De Bruin, R. & von Solms, S.H. (2015) Modeling Cyber Security Governance Maturity. *2015 IEEE International Symposium on Technology and Society (ISTAS)*, Dublin, Ireland, 2015. IEEE. pp. 1-8. doi:10.1109/ISTAS.2015.7439415.

Demertzi, V., Demertzis, S. & Demertzis, K. (2023) An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. *Applied Sciences*. 13(2), 790. doi:10.3390/app13020790.

Elmaghraby, A.S. & Losavio, M. M. (2014) Cyber Security Challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*. 5(4), 491-497. doi:10.1016/j.jare.2014.02.006.

Elsaeidy, A., Elgendi, I., Munasinghe, K. S., Sharma, D. & Jamalipour, A. (2017) A Smart City Cyber Security Platform for Narrowband Networks. *2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 2017*. IEEE. pp.1-6. doi:10.1109/ATNAC.2017.8215388.

Eremia, M., Toma, L. & Mihai, S. (2017). The Smart City Concept in the 21st Century. *Procedia Engineering*. 181, 12-19. doi:10.1016/j.proeng.2017.02.357.

European Commission. (2022) *InCUBE | Smart Cities Marketplace*. https://smart-cities-marketplace.ec.europa.eu/projects-and-sites/projects/incube [Accessed: 18th January 2024].

European Commission. (2024) *CORDIS | European Commission*. https://cordis.europa.eu/ [Accessed 30th January 2024].

European Union Agency for Cybersecurity (ENISA). *Home | ENISA*. https://www.enisa.europa.eu/ [Accessed 7th February 2025].

Hamid, B., Jhanjhi, N., Humayun, M., Khan, A. & Alsayat, A. (2019) Cyber Security Issues and Challenges for Smart Cities: A survey. *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019*. IEEE. pp.1-7. doi:10.1109/MACS48846.2019.9024768.

Hamza, A., Gharakheili, H. H., Pering, T. & Sivaraman, V. (2022) Combining Device Behavioral Models and Building Schema for Cybersecurity of Large-Scale IoT Infrastructure. *IEEE Internet of Things Journal*. 9(23), 24174-24185. doi: 10.1109/JIOT.2022.3189350.

Jayaraman, B., Thanga Nadar Thanga Thai, M., Anand, A. & Anandan, K. R. (2023) Detecting malicious IoT traffic using Machine Learning techniques. *Romanian Journal of Information Technology and Automatic Control (Revista Română de Informatică și Automatică)*. 33(4), 47-58. doi:10.33436/v33i4y202304.

Jiang, Y., Jeusfeld, M. A., Ding, J. & Sandahl, E. (2023) Model-Based Cybersecurity Analysis. *Business & Information Systems Engineering*. 65(6), 643-676. doi:10.1007/s12599-023-00811-0.

Kalinin, M., Krundyshev, V. & Zegzhda, P. (2021) Cybersecurity Risk Assessment in Smart City Infrastructures. *Machines*. 9(4),78. doi:10.3390/machines9040078.

Khatoun, R. & Zeadally, S. (2017) Cybersecurity and Privacy Solutions in Smart Cities. *IEEE Communications Magazine*. 55(3), 51-59. doi:10.1109/MCOM.2017.1600297CM.

Maleh, Y., Sahid, A., & Belaissaoui, M. (2021) A Maturity Framework for Cybersecurity Governance in Organizations. *Edpacs*. 63(6), 1–22.doi:10.1080/07366981.2020.1815354.

Melaku, H.M. (2023) A Dynamic and Adaptive Cybersecurity Governance Framework *Journal of Cybersecurity and Privacy*. 3(3), 327-350. doi:10.3390/jcp3030017.

Mohamed, N., Al-Jaroodi, J. & Jawhar, I. (2020) Opportunities and Challenges of Data-Driven Cybersecurity for Smart Cities. *2020 IEEE Systems Security Symposium (SSS), Crystal City, VA, USA, 2020*. IEEE. pp.1-7. doi:10.1109/SSS47320.2020.9174388.

National Institute of Standards and Technology (NIST) https://www.nist.gov/ [Accessed 7th February 2025].

Radu, L.-D. (2020) Disruptive Technologies in Smart Cities: A Survey on Current Trends and Challenges. *Smart Cities*. 3(3), 1022-1038. doi:10.3390/smartcities3030051.

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R. & Mehani, O. (2015) Network-level security and privacy control for smart-home IoT devices. *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates, 2015*. IEEE. pp. 163-167. doi:10.1109/WiMOB.2015.7347956.

Ten, C. -W., Manimaran, G. & Liu, C. -C. (2010) Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*. 40(4), 853-865. doi: 10.1109/TSMCA.2010.2048028.

United Nations (2017) *World population projected to reach 9.8 billion in 2050, and 11.2 billion in 2100 | United Nations*. https://www.un.org/en/desa/world-population-projected-reach-98-billion-2050-and-112-billion-2100 [Accessed 18th January 2024].

Vickerman, R. (2007). Cost — Benefit Analysis and Large-Scale Infrastructure Projects: State of the Art and Challenges. *Environment and Planning B: Planning and Design*. 34(4), 598-610. doi: 10.1068/b32112.

Vinnakota, T. (2016). A Second Order Cybernetic Model for Governance of Cyber Security in Enterprises. *2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, India, 2016*. IEEE. pp.706-710. doi: 10.1109/IACC.2016.136.

Yu, D., Zhang, L., Chen, Y., Ma, Y. & Chen, J. (2020) Large-Scale IoT Devices Firmware Identification Based on Weak Password. *IEEE Access*. 8, 7981-7992. doi: 10.1109/ACCESS.2020.2964646.

Yusif, S. & Hafeez-Baig, A. (2021) A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*. 16(4), 490–513. doi:10.1080/19361610.2021.1918995.

Răzvan STOLERIU is a Ph.D. student in computer science, majoring in advanced cyber-security attacks detection, at the National University of Science and Technology POLITEHNICA Bucharest, Romania. He currently works as a threat analyst at a prestigious cyber-security company. He has published articles in specialized journals and volumes of international conferences. His areas of interest include information security, malware analysis, reverse engineering, and network security.

Răzvan STOLERIU este doctorand în Calculatoare și Tehnologia Informației la Universitatea Națională de Știință și Tehnologie POLITEHNICA București, România, specializat în detectarea atacurilor avansate de securitate cibernetică. În prezent, lucrează ca analist de atacuri cibernetice într-o companie de prestigiu. A publicat articole în reviste de specialitate și volume ale conferințelor internaționale. Domeniile sale de interes includ securitatea informațiilor, analiza programelor malware, inginerie inversă și securitatea rețelei.

Ionuț PETRE is a PhD in Engineering and a second-degree scientific researcher at the National Institute for Research and Development – ICI Bucharest. He is the head of the RDI Department for Digital Transformation and Governance and the coordinator of the Digital Transformation Innovation Laboratory. His scientific and academic contributions focus on the Internet of Things (IoT), Big Data, Machine Learning, Software Architectures, Accessibility, Software Platforms.

Ionuț PETRE este doctor inginer și cercetător științific gradul II în carul Institutului Național de Cercetare-Dezvoltare – ICI București. Este șeful Departamentului CDI pentru Transformare Digitală și Guvernare și coordonatorul Laboratorului de Inovare în Transformare Digitală. Contribuțiile sale științifice și academice se concentrează pe Internetul lucrurilor (IoT), Big Data, Învățare Automată, Arhitecturi software, Accesibilitate, Platforme software.

Florin POP is full Professor at the Computer Science and Engineering Department of National University of Science and Technology POLITEHNICA Bucharest, Romania. His main research interests are in large-scale distributed systems, adaptive and autonomous methods, optimization methods, applications for Big Data and IoT systems, Smart Cities. He is senior researcher at ICI Bucharest, member of the Academy of Romanian Scientists and senior member of IEEE (Institute of Electrical and Electronics Engineers).

Florin POP este profesor titular la Departamentul de Informatică şi Inginerie al Universității Naționale de Știință şi Tehnologie POLITEHNICA București, România. Principalele sale interese de cercetare sunt în sisteme distribuite la scară largă, metode adaptive şi autonome, metode de optimizare, aplicații Big Data, IoT și Smart Cities. Florin Pop este cercetător științific gradul I în cadrul Institutului Național de Cercetare-Dezvoltare – ICI Bucureşti, membru al Academiei Oamenilor de Știință din România și membru senior al IEEE (Institutul Inginerilor Electrotehnicieni și Electroniști).