International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Cyber-securing Morocco's smart cities: A case review

Chaouki CHOURAIK *, Radouan EL-FOUNIR and Khalid TAYBI

Department of Public Law, Faculty of Legal and Political Sciences, University of Hassan First, Settat, Morocco.

International Journal of Science and Research Archive, 2024, 13(01), 102–112

Publication history: Received on 22 July 2024; revised on 01 September 2024; accepted on 03 September 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.13.1.1619

Abstract

Urbanization and digital transformation are rapidly reshaping cities across Morocco, giving rise to Smart Cities that leverage advanced technologies to enhance efficiency, sustainability, and urban life quality. However, this shift towards interconnected, technology-centric urban environments also presents significant cybersecurity challenges that necessitate careful analysis. This paper explores the cybersecurity issues confronting Smart Cities, with a specific focus on case studies from Moroccan cities. As Morocco embraces Smart City initiatives to address urban challenges and drive economic growth, these developments bring both promise and risk. The increased connectivity and technological integration within Smart Cities offer improved services but also expose cities to a wider range of cyber threats. The interconnectedness of devices and systems in Smart Cities broadens the potential for cyber-attacks, including data breaches and disruptions to critical infrastructure. This review delves into the cybersecurity challenges faced by Moroccan cities as they advance technologically. It identifies vulnerabilities in critical infrastructure such as energy grids, transportation systems, and healthcare networks highlighting the dangers posed by inadequate cybersecurity measures. Moreover, the study underscores the socio-economic impact of cyber threats in Smart Cities, stressing the importance of robust cybersecurity frameworks to safeguard citizen data and maintain urban operations. In conclusion, this research emphasizes the urgent need for comprehensive cybersecurity strategies tailored to the unique challenges of Moroccan Smart Cities. The insights presented aim to deepen understanding of the complex relationship between urbanization, technology, and cybersecurity, and to inform policy decisions, technological deployment, and collaborative efforts towards creating secure and resilient Smart Cities in Morocco.

Keywords: Cybersecurity; Smart Cities; Morocco; Case review

1. Introduction

In an era marked by unprecedented urbanization and technological progress, the concept of Smart Cities has emerged as a transformative approach to addressing the multifaceted challenges confronting urban environments. Smart Cities harness advanced technologies to optimize urban services, enhance resource utilization, and improve the overall quality of life for residents. However, as these cities integrate various technological components, they become increasingly susceptible to cybersecurity threats that can have significant repercussions(1). This paper aims to explore the cybersecurity challenges inherent in Smart Cities, focusing specifically on Moroccan metropolises undergoing rapid digital transformations(2).

Smart Cities signify a paradigm shift in urban development, wherein Information and Communication Technologies (ICT) are seamlessly integrated to optimize infrastructure, services, and communication. These urban environments utilize interconnected sensors, devices, and systems to collect and analyze data, facilitating real-time decision-making and resource management(3). The objective is to create cities that are sustainable, resilient, and responsive to the needs of their inhabitants. Smart Cities encompass a diverse array of sectors, including transportation, energy, healthcare, and governance, all interconnected through a sophisticated digital framework(4).

* Corresponding author: Chouraik Chaouki

In the Moroccan context, the significance of Smart City initiatives is particularly pronounced as these metropolises confront the challenges of rapid urbanization, resource constraints, and the imperative for sustainable development(5). The implementation of Smart City technologies in Moroccan cities holds the potential to address longstanding issues such as traffic congestion, inadequate healthcare, and inefficient resource management. Moreover, it presents an opportunity for leapfrogging traditional developmental stages, enabling Moroccan cities to embrace innovation and technology for accelerated growth(6).

The integration of technology into urban environments is a complex process that involves deploying IoT (Internet of Things) devices, sensors, and advanced communication networks. Smart Cities leverage data analytics and artificial intelligence to derive insights from various sources, enabling predictive modeling and efficient resource allocation. For instance, smart transportation systems utilize real-time data to optimize traffic flow and alleviate congestion, while smart energy grids enhance sustainability by optimizing energy distribution. In healthcare, technology integration facilitates remote monitoring and personalized healthcare services(7).

The interconnected nature of these technologies allows for seamless communication between different components of urban infrastructure, providing a holistic view of the city's operations. While these advancements promise substantial benefits, they also expose Smart Cities to a new set of challenges, particularly in the realm of cybersecurity(8).

As Smart Cities become the focal point of urban development in Morocco, the cybersecurity challenges they face warrant careful scrutiny. The interconnectivity of devices and systems in these cities creates an expansive attack surface, making them vulnerable to a variety of cyber threats(9). This paper posits that the cybersecurity challenges in Smart Cities, especially within the Moroccan context, necessitate focused attention and innovative solutions. Through a case review of representative Moroccan metropolises, we aim to identify specific instances of cybersecurity vulnerabilities and their socio-economic implications(10). Furthermore, the paper seeks to contribute insights that can inform the development of robust cybersecurity strategies tailored to the unique challenges faced by Smart Cities in Morocco(11).

2. Smart City Initiatives in Morocco

The rise of Smart City initiatives in Morocco can be traced back to the early 21st century, coinciding with a surge in urbanization and an increasing demand for innovative solutions to urban challenges. Moroccan governments and municipalities, recognizing the transformative potential of technology, began to embrace the concept of Smart Cities. The initial focus was on leveraging information and communication technologies (ICT) to enhance governance, infrastructure, and service delivery(12).

One of the pioneering efforts in this regard was the implementation of Casablanca Smart city, launched in 2015(13). This project aimed to utilize technology to improve public services, enhance safety, and stimulate economic development. Following this, other Moroccan cities, including Rabat ,Tangier and Benguerir, began exploring Smart City concepts, acknowledging the necessity for sustainable urban development in the face of rapid population growth(14).

In subsequent years, Digital Morocco 2020, A national strategy aimed at promoting digital transformation across various sectors, including smart cities.This emphasis on technology as a catalyst for progress laid the groundwork for more comprehensive Smart City initiatives across the country(15).

The integration of technology into Smart Cities encompasses a diverse range of cutting-edge innovations that collectively contribute to the development of intelligent urban environments. Among the key technologies integrated into Smart Cities in Morocco are the Internet of Things (IoT), which plays a pivotal role by connecting physical devices and sensors to the internet, enabling them to collect and exchange data(16). This connectivity allows for real-time monitoring and management of various aspects of urban life, such as traffic flow, energy consumption, and waste management. The use of big data analytics enables Smart Cities to process vast amounts of information collected from IoT devices, facilitating informed decision-making, predictive modeling, and the identification of patterns that can optimize urban services and infrastructure.

Artificial intelligence technologies, including machine learning and natural language processing, contribute to the automation of processes and the development of intelligent systems(17). In Smart Cities, AI is employed in areas such as traffic management, public safety, and healthcare to enhance efficiency and responsiveness. This includes the integration of advanced technologies into traditional urban infrastructure. Smart grids enhance energy efficiency, intelligent transportation systems reduce traffic congestion, and smart buildings incorporate energy-saving features and automation for improved sustainability. The convergence of physical infrastructure with digital technologies results

in cyber-physical systems, encompassing smart grids, smart transportation, and smart healthcare, creating a cohesive and interconnected urban environment(18).

Smart Cities hold immense promise for Moroccan metropolises, offering a range of potential benefits that address pressing urban challenges and contribute to sustainable development. Through the deployment of smart technologies, cities can optimize the use of resources such as energy, water, and transportation. This efficiency not only reduces costs but also contributes to environmental sustainability. Smart City initiatives aim to enhance the overall quality of life for residents, providing better healthcare services, efficient public transportation, and creating safer urban environments. The integration of technology stimulates economic growth by attracting investment, fostering innovation, and creating job opportunities. Smart Cities become hubs for technological advancements, leading to increased competitiveness on the global stage. Furthermore, Smart Cities leverage digital connectivity to create a seamless urban experience, improving communication, accessibility to services, and real-time information on various aspects of city life(19). With a focus on smart infrastructure and sustainable practices, these cities contribute to environmental conservation through reduced energy consumption, optimized waste management, and green initiatives. (Figure 1 provides initiatives included in Moroccan smart cities)

Table 1 Moroccan Smart cities initiatives

City	Key Initiatives	Focus Areas
Casablanca	Digital transformation, urban mobility, sustainable development.	Traffic management, public transportation, waste management.
Rabat	Sustainable urban planning, renewable energy, smart lighting.	Green urban development, energy efficiency.
Tangier	Smart logistics, automation, traffic management.	Port operations, traffic flow.
Benguerir	Renewable energy research, innovation hub.	Green energy, smart technologies.

In conclusion, the history of Smart City initiatives in Morocco reflects a strategic response to the challenges of urbanization and a commitment to leveraging technology for sustainable development. The integration of key technologies signifies progress but also introduces a new set of challenges, particularly in the realm of cybersecurity. Understanding the historical context and potential benefits of Smart Cities sets the stage for a comprehensive examination of the cybersecurity challenges faced by Moroccan metropolises undergoing digital transformations(20).

3. Cybersecurity Landscape in Smart Cities

The rapid proliferation of Smart Cities introduces a new dimension to the traditional cybersecurity landscape, necessitating a paradigm shift in strategies and approaches. Urban environments, characterized by interconnected systems and a multitude of devices, present a complex web of vulnerabilities that cyber threats can exploit. The conventional focus on securing individual computers and networks must now expand to safeguarding entire city infrastructures(21).

In the context of Smart Cities, cybersecurity extends beyond protecting personal data to ensuring the reliability and security of critical urban systems. This includes transportation networks, energy grids, healthcare services, and governance mechanisms, all of which increasingly rely on interconnected technologies. The interconnected nature of these systems amplifies the potential impact of cyber threats, making them more pervasive and potentially devastating.

The integration of Internet of Things (IoT) devices and sensors across diverse urban sectors vastly expands the attack surface for potential cyber threats. Each connected device becomes a potential entry point, complicating the task of monitoring and securing the entire network comprehensively. Smart Cities operate as intricate webs of interdependent systems, where a cyber-attack on one component can have cascading effects on others, leading to disruptions in essential services. For instance, a breach in the transportation system may adversely affect emergency services, exacerbating the impact of the attack(22).

The extensive collection and analysis of data in Smart Cities raise significant concerns about privacy. The interconnectedness of systems can lead to the aggregation of sensitive information, and any compromise in data security may have severe implications for citizen privacy and trust in the system. Many Smart Cities integrate advanced

technologies into existing, often legacy, infrastructure. This integration poses challenges, as legacy systems may harbor vulnerabilities that are difficult to address, potentially serving as weak links in the overall cybersecurity framework.

The human element remains a vulnerability in the Smart City cybersecurity landscape. From city administrators to citizens, susceptibility to phishing attacks, social engineering, and negligent security practices can compromise the integrity of the entire system. Trust is paramount in the successful implementation of Smart City initiatives. The public must have confidence that their data is secure and that the services they rely on are resilient to cyber threats. A breach of this trust not only undermines the success of Smart Cities but also erodes public confidence in digital governance(23).

The functionality of Smart City infrastructure is crucial for maintaining economic and operational stability. Cyberattacks on critical systems can disrupt services, leading to economic losses, compromised public safety, and a breakdown of essential urban functions. Smart Cities are integral components of national infrastructure, and their compromise can have far-reaching national security implications. Cyberattacks targeting critical urban systems may not only disrupt city functions but also pose threats at a broader geopolitical level. Smart Cities collect and process vast amounts of sensitive data, ranging from personal information to critical infrastructure details. Ensuring the confidentiality, integrity, and availability of this data is imperative to prevent unauthorized access, data breaches, and potential misuse.

The dynamic nature of cyber threats necessitates a proactive and adaptive cybersecurity approach. Smart Cities must continuously evolve their cybersecurity strategies to address emerging threats, vulnerabilities, and attack vectors, ensuring resilience against evolving cyber risks. In conclusion, the cybersecurity landscape in Smart Cities is a critical aspect of their success and sustainability. The interconnected nature of urban systems introduces unique challenges that require innovative and comprehensive solutions. As Smart Cities continue to evolve, the importance of robust cybersecurity measures cannot be overstated. The proactive protection of critical infrastructure, sensitive data, and public trust is essential to realizing the promise and potential benefits of Smart Cities in the digital age. Addressing these challenges head-on will not only secure the urban environments of today but also pave the way for the resilient and secure cities of the future(24).

4. Case Review of Moroccan Smart Cities

Across Morocco, several major cities have embarked on ambitious Smart City initiatives, leveraging technology to drive urban development. Notable among these are Casablanca, Rabat, Tangier, and Benguerir. These cities, with their diverse economic, cultural, and demographic contexts, provide a comprehensive understanding of the challenges and opportunities associated with Smart City transformations in the country. This case review identifies several critical challenges that these cities face, particularly in the realm of cybersecurity(25).

5. Challenges Faced by Moroccan Smart Cities

5.1. Shortage of Skilled Professionals

One of the most pressing challenges is the shortage of adequately trained cybersecurity professionals. The demand for such expertise far exceeds supply, creating a significant gap in the ability to effectively counter the increasing and evolving cyber threats.

5.2. Financial Constraints

Many small and medium-sized enterprises (SMEs) and public institutions are constrained by limited financial resources, making it difficult to invest in comprehensive cybersecurity measures. This financial limitation often leaves these entities more vulnerable to cyberattacks.

5.3. Limited Awareness and Education

A general lack of awareness and education about cybersecurity threats and best practices further exacerbates vulnerabilities. Without proper knowledge, both individuals and organizations struggle to maintain good security hygiene, increasing their susceptibility to attacks.

5.4. Regulatory and Compliance Gaps

Morocco's regulatory framework for cybersecurity is still developing, with incomplete legislation and insufficient penalties. Furthermore, there is a lack of alignment with international standards and industry-specific regulations, making it difficult to enforce strong cybersecurity practices uniformly.

5.5. Cross-Border Threats

The transnational nature of many cyber threats poses additional challenges, as Morocco must navigate varying legal frameworks and limited international agreements. This complexity makes it difficult to trace the origins of attacks and collaborate effectively with foreign authorities.

5.6. Outdated Legacy Systems

Many of Morocco's critical infrastructure systems rely on outdated technology. These legacy systems are inherently more vulnerable to cyber threats due to their incompatibility with modern security protocols, lack of regular updates, and limited access controls.

5.7. Lack of Incident Response Planning

Many organizations in Morocco are unprepared for cyber incidents due to the absence of well-defined incident response plans. This lack of readiness can lead to delayed responses, financial and reputational damage, regulatory penalties, and confusion during a security incident.

The rapid adoption of Smart City technologies, often without comprehensive planning, exacerbates these cybersecurity challenges. Cities frequently integrate advanced technologies into existing infrastructures without fully assessing vulnerabilities, particularly in legacy systems, which become points of weakness susceptible to attacks.

An additional factor is the insufficient awareness and training of both city administrators and citizens. A well-informed user base is crucial for minimizing human-centric vulnerabilities, such as social engineering attacks and poor security practices.

The lack of standardized security protocols across Moroccan Smart Cities further complicates cybersecurity efforts. Each city may implement different technologies and security measures, making it difficult to establish cohesive defense strategies and collaborate on threat intelligence. Limited cooperation and information sharing among Moroccan Smart Cities hinder the collective response to cybersecurity threats. Developing national alliances to share threat intelligence and best practices could significantly enhance the cybersecurity posture of individual cities(26).

In conclusion, this case review of Moroccan Smart Cities undergoing transformation reveals a complex landscape of cybersecurity challenges. Vulnerabilities in critical infrastructure, potential data breaches, and socio-economic impacts underscore the multifaceted nature of the threats these cities face. Addressing the root causes—such as limited cybersecurity infrastructure, rapid technological adoption without robust planning, inadequate awareness and training, lack of standardized security protocols, and insufficient collaboration—is crucial for building resilient and secure Smart Cities in Morocco. These findings highlight the need for strategic investments, comprehensive planning, and collaborative efforts to mitigate cybersecurity risks and ensure the sustainable development of Smart Cities across the Kingdom.

6. Socio-Economic Implications

The impact of cybersecurity threats in Smart Cities extends beyond technical disruptions, influencing the socio-economic fabric of urban communities. As cities increasingly rely on interconnected systems and digital infrastructure, cyber threats pose risks to various aspects of daily life.

Cybersecurity threats can disrupt essential urban services, affecting sectors such as transportation, healthcare, and energy distribution. For instance, an attack on smart transportation systems could result in traffic chaos, complicating daily commutes and impeding the flow of goods and services. Similarly, disruptions in healthcare systems could jeopardize patient care and public health, highlighting the need for secure and resilient services(27).

The economic implications of cybersecurity threats are substantial. Downtime and disruptions caused by attacks on Smart City infrastructure can result in significant financial losses. Businesses may experience operational interruptions, supply chain disruptions, and reduced productivity. These economic repercussions extend beyond individual enterprises, impacting the overall economic stability of the city and its attractiveness to investors(28).

Cybersecurity threats also have profound societal impacts, compromising citizen safety and well-being. For example, attacks on smart surveillance systems or emergency response mechanisms could hinder the city's ability to address

public safety concerns effectively. Additionally, data breaches that expose personal information could erode public trust in Smart City initiatives, leading to reluctance in adopting digital services and technologies.

The political implications of cybersecurity threats are evident in the potential erosion of public confidence in government authorities. Leaders may face scrutiny for inadequate cybersecurity measures, and their ability to govern effectively may be questioned. The fallout from cyber incidents can become a political issue, influencing public opinion and potentially shaping electoral outcomes. The political landscape may also be impacted by the need for swift and effective responses to cyber threats, requiring policymakers to prioritize cybersecurity on their agendas.

A critical aspect of the socio-economic impact of cybersecurity threats is the erosion of citizen trust. In Smart Cities, where digital interactions are integral to daily life, any compromise in cybersecurity can lead to a loss of faith in the reliability and security of digital services. Restoring trust requires transparent communication, robust security measures, and citizen engagement to ensure that the urban community remains actively involved in securing the city's digital infrastructure.

Cybersecurity threats can exacerbate existing socio-economic disparities, disproportionately affecting vulnerable populations. Disruptions in digital services may hinder access to critical resources and information, impacting marginalized communities more severely. Ensuring equity in cybersecurity measures and promoting accessibility to secure digital services is essential for fostering an inclusive and resilient urban environment.

Building resilience against cybersecurity threats requires collaborative responses from urban communities. Encouraging citizens to be vigilant, practice good cyber hygiene, and actively participate in community-wide cybersecurity initiatives is crucial. Community awareness programs, educational campaigns, and the inclusion of diverse voices in planning and implementing Smart City cybersecurity measures can enhance the overall security posture of the city(29).

In conclusion, the socio-economic implications of cybersecurity threats in Smart Cities extend far beyond technical disruptions. The economic, social, and political ramifications underscore the interconnectedness of cybersecurity with the fabric of urban life. A holistic understanding of these implications is imperative for policymakers, city administrators, and citizens alike. By addressing the socio-economic impacts of cybersecurity threats, cities can cultivate resilience, foster economic growth, and ensure that the benefits of Smart City initiatives are realized across diverse urban communities.

7. Cybersecurity Strategies for Smart Cities in Morocco

The evolving cybersecurity landscape in Morocco's Smart Cities presents complex challenges as urban systems become increasingly interconnected. Despite some cities making significant progress in developing cybersecurity frameworks and policies, there remains a pressing need for a thorough evaluation of existing initiatives to identify shortcomings and opportunities for enhancement(29).

A notable turning point in Morocco's cybersecurity efforts occurred in 2011. The establishment of the Directorate General of Information Systems Security (DGSSI) on September 21, 2011, via decree n° 2-11-509, marked a significant milestone in strengthening national security. The DGSSI, operating under the National Defense Administration, has been instrumental in shaping national policies, strategies, and standards for information systems security. This organization collaborates with a diverse array of stakeholders, including government agencies, private sector entities, and international partners, to bolster Morocco's cybersecurity infrastructure and mitigate cyber threats. Its duties encompass the development of legal frameworks governing cybersecurity—ranging from authorizations and certifications to verification methodologies—alongside conducting technological surveillance, audits, and incident response planning. Additionally, the DGSSI promotes best practices in information security and spearheads public awareness campaigns to address cybersecurity risks. Importantly, the Moroccan Computer Emergency Response Team (maCERT) was integrated into the DGSSI from its inception(30).

In 2011, Morocco also introduced Law 31-08 on Consumer Protection, a crucial piece of legislation aimed at strengthening consumer rights and offering legal protections across various commercial activities, particularly online commerce(31). This law sought to shield consumers from unfair practices, guarantee product and service quality, and foster fair competition. Key provisions of the law targeted online commerce, imposing obligations on vendors to provide accurate product descriptions, transparent pricing, and secure payment options. Furthermore, it outlined consumer rights related to information, delivery and return policies, and established mechanisms for dispute resolution, empowering consumer protection associations and government bodies to enforce compliance.

The year 2012 saw Morocco adopt the National Cybersecurity Strategy, also known as the National Strategy for Information System Security (SNSSI). This initiative was pivotal in bolstering the nation's cybersecurity defenses and protecting critical information infrastructure. The strategy's core objectives included safeguarding essential sectors such as energy, finance, and transportation from cyber-attacks, enhancing incident response capabilities, and reinforcing the legal and regulatory frameworks to combat cybercrime. It also emphasized the importance of cybersecurity awareness and education while fostering collaboration between government entities, private enterprises, and international partners(32).

In August 2014, Morocco took another crucial step by enacting Law No. 46-13, which ratified the Council of Europe's Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data. This convention, recognized as the first legally binding international instrument on data protection, highlights the growing significance of privacy in a digital age. Concurrently, the Moroccan Ministry of Industry, Commerce, Investment, and Digital Economy initiated a four-year national campaign to raise cybersecurity awareness. Led by the Moroccan Centre for Polytechnic Research and Innovation (CMRPI), this campaign was designed to promote responsible cybersecurity practices across both the public and private sectors, as well as among citizens of various demographics. Notably, this initiative was a pioneering effort in Africa.

Morocco's commitment to cybersecurity received further recognition in 2015 with the release of the first Global Cybersecurity Index (GCI) by the International Telecommunication Union (ITU). Morocco ranked 24th globally, 3rd in Africa, and 4th among Arab nations. In addition to the GCI, the ITU developed a Cyberwellness Profile for Morocco, which highlighted the country's achievements in legal, technical, and organizational aspects of cybersecurity. While the profile acknowledged Morocco's progress in international cooperation and child online protection, it also pointed out the lack of national or sector-specific research and development initiatives in cybersecurity.

The year 2016 marked another milestone with the enactment of decree No. 2-15-712, which established a framework for safeguarding sensitive information systems within vital infrastructures. This decree, endorsed by the government under the leadership of King Mohammed VI, solidified the national directive for information systems security crafted by the DGSSI. Additionally, in June 2016, Bank Al-Maghrib issued Directive No. 3/W/16, which established critical regulations for credit institutions to conduct penetration tests on their information systems. These developments underscore Morocco's ongoing commitment to fortifying its cybersecurity framework and safeguarding its critical infrastructures against emerging threats.

Establishing robust monitoring mechanisms is crucial for the early detection of cyber threats. By implementing advanced monitoring tools, facilitating threat intelligence sharing, and developing real-time incident response capabilities, Smart Cities can swiftly address emerging threats, thereby minimizing the potential impact of cybersecurity incidents.

Integrating cybersecurity considerations into the design phase of Smart City projects is essential. Adhering to secure-by-design principles ensures that cybersecurity measures are embedded in the development and deployment of technologies, effectively mitigating vulnerabilities that could be exploited in the future.

Collaboration between governments and the private sector is critical for ensuring effective cybersecurity in Smart Cities. Establishing public-private partnerships enhances information sharing, fosters joint threat intelligence efforts, and coordinates responses to cyber incidents. This collaborative approach leverages the expertise and resources of both sectors, leading to a more comprehensive and resilient cybersecurity strategy(33).

Involving cybersecurity experts and industry stakeholders is vital for staying ahead of evolving cyber threats. Governments and Smart City initiatives must engage with the cybersecurity industry to access cutting-edge technologies, threat intelligence, and specialized expertise. This collaboration ensures that Smart Cities can proactively address emerging cybersecurity challenges.

Given that cyber threats often transcend national borders, cross-border collaboration is imperative. Moroccan Smart Cities should actively participate in regional and international cooperation to share threat intelligence, best practices, and lessons learned. Cross-border collaboration enhances the collective cybersecurity resilience of Smart Cities and contributes to a safer digital environment.

Moreover, it is crucial to involve multiple stakeholders, including academia, civil society, and local communities, in cybersecurity efforts. This multi-stakeholder approach brings diverse perspectives, fosters innovation, and promotes inclusivity in the development and implementation of cybersecurity strategies for Smart Cities(34).

In conclusion, securing Smart Cities in Morocco requires a holistic approach that builds upon existing cybersecurity frameworks while integrating recommendations for resilience and emphasizing collaboration between governments, the private sector, and cybersecurity experts. By thoroughly evaluating and strengthening current strategies, Smart Cities can navigate the dynamic cybersecurity landscape, mitigate risks, and lay the groundwork for sustainable and secure digital urban environments. The concerted efforts of all stakeholders will be instrumental in constructing resilient Smart Cities that can thrive amidst cybersecurity challenges.

8. Conclusion

The case review of Moroccan metropolises undergoing Smart City transformations has unearthed critical insights into the cybersecurity challenges faced by these urban environments. Across representative cities such as Casablanca, Rabat, Tangier, and Benguerir, vulnerabilities in critical infrastructure, data breaches, and socio-economic impacts were identified as recurring themes. The examination highlighted the intricate web of interconnected systems, the potential consequences of cyber threats on essential services, and the broader implications for economic stability, social trust, and political resilience.

The urgency for robust cybersecurity measures in Smart Cities cannot be overstated. The interconnected nature of urban systems, coupled with the increasing sophistication of cyber threats, necessitates immediate and comprehensive action. The case review underscores that cybersecurity is not merely a technical concern but a fundamental prerequisite for the success and sustainability of Smart City initiatives. The potential economic losses, disruptions in critical services, and erosion of public trust emphasize the critical need for cities to prioritize and invest in cybersecurity resilience.

In light of the findings, a collective call to action is essential for all stakeholders involved in the development and governance of Smart Cities in Morocco. This includes government bodies, private sectors, academia, cybersecurity experts, and local communities. The following actions are recommended:

8.1. Resource Allocation

Governments and private sectors should allocate substantial resources to build and enhance cybersecurity infrastructure in Smart Cities. This involves investing in advanced technologies, training cybersecurity professionals, and implementing robust monitoring and incident response mechanisms. The potential gains from embracing connected smart cities are great, but they come entangled with significant responsibilities and risks.

8.2. Policy Review

Governments need to continuously review and update existing cybersecurity policies to align with the evolving threat landscape of Smart Cities. These policies should encompass data protection, privacy laws, and sector-specific regulations, providing a comprehensive framework for securing critical infrastructure. These policies must adapt and change in the speed of technology.

8.3. Public Awareness

A concerted effort is needed to raise public awareness about cybersecurity threats and best practices. Educational campaigns targeting citizens, businesses, and government employees can foster a culture of cybersecurity awareness and responsibility. Informed individuals are more likely to contribute to the overall resilience of Smart Cities.

8.4. International Collaboration

Smart Cities in Morocco should actively engage in international collaboration and information sharing to stay abreast of global cybersecurity trends. Learning from the experiences of other cities and leveraging international partnerships can enhance the effectiveness of cybersecurity strategies.

8.5. Stakeholder Collaboration

Governments, private sectors, academia, and local communities should collaboratively develop and implement cybersecurity strategies. Involving diverse stakeholders ensures a holistic approach that considers the unique challenges faced by Smart Cities and facilitates innovation and knowledge-sharing.

8.6. Proactive Cybersecurity

Smart Cities should adopt a proactive stance towards cybersecurity by continuously monitoring the threat landscape and adapting their strategies accordingly. Regular assessments, penetration testing, and scenario-based exercises can help cities stay one step ahead of cyber threats.

In conclusion, the case review of cybersecurity challenges in Moroccan cities has provided a foundation for urgent and decisive action. The recommendations underscore the imperative for immediate investments, policy revisions, public awareness campaigns, and collaborative efforts to fortify the cybersecurity resilience of Smart Cities. The call to action is not just a suggestion but a collective responsibility to safeguard the digital infrastructure, economic stability, and societal well-being of Moroccan metropolises in the era of rapid urbanization and technological advancement. By heeding this call, stakeholders can contribute to the creation of Smart Cities that thrive securely, fostering innovation, inclusivity, and sustainable urban development.

Compliance with ethical standards

Acknowledgments

I am thankful to the Reviewers and Editor for their constructive feedback, which significantly improved the quality of this research. Additionally, I am also grateful to my colleague Radouan EL-FOUNIR and Prof. Khalid TAYBI,for their insightful discussions and valuable input during the research process.

Disclosure of conflict of interest

No conflict of interest has been declared by the authors.

References

[1] Hui CX, Dan G, Alamri S, Toghraie D. Greening smart cities: An investigation of the integration of urban natural resources and smart city technologies for promoting environmental sustainability. Sustainable Cities and Society. 2023; 99:104985.

[2] Kumar H, Singh MK, Gupta MP, Madaan J. Moving towards smart cities: Solutions that lead to the Smart City Transformation Framework. Technological forecasting and social change. 2020; 153:119281.

[3] Rehan H. Internet of Things (IoT) in Smart Cities: Enhancing Urban Living Through Technology. Journal of Engineering and Technology. 2023;5(1):1–16.

[4] Bibri SE, Krogstie J. Environmentally data-driven smart sustainable cities: applied innovative solutions for energy efficiency, pollution reduction, and urban metabolism. Energy Inform. 2020 Dec;3(1):29.

[5] Hajar EM, Abdelghani C. Exploring the emergence of a new smart city model: case analysis of the Moroccan urbanization. In: 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM) [Internet]. IEEE; 2017 [cited 2024 Aug 28]. p. 293–9. Available from: https://ieeexplore.ieee.org/abstract/document/8122188/

[6] Graveline EA, Stahl JM, Elice SJ. Achieving Connectivity Through Smart City Initiatives in Madinat Al Irfane, Rabat, Morocco. 2019 [cited 2024 Aug 28]; Available from: https://core.ac.uk/download/pdf/213002546.pdf

[7] Gupta S, Leszkiewicz A, Kumar V, Bijmolt T, Potapov D. Digital Analytics: Modeling for Insights and New Methods. Journal of Interactive Marketing. 2020 Aug; 51:26–43.

[8] Amini MH, Arasteh H, Siano P. Sustainable Smart Cities Through the Lens of Complex Interdependent Infrastructures: Panorama and State-of-the-art. In: Amini MH, Boroojeni KG, Iyengar SS, Pardalos PM, Blaabjerg F, Madni AM, editors. Sustainable Interdependent Networks II [Internet]. Cham: Springer International Publishing; 2019 [cited 2024 Aug 28]. p. 45–68. (Studies in Systems, Decision and Control; vol. 186). Available from: http://link.springer.com/10.1007/978-3-319-98923-5_3

[9] Silva BN, Khan M, Han K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable cities and society. 2018; 38:697–713.

[10] Darmame K, Kaioua A, Ross E. The Endless Challenge of Local Governance in Casablanca. In: Darmame K, Ross E, editors. Local Governance and Development in Africa and the Middle East [Internet]. Cham: Springer Nature

Switzerland; 2024 [cited 2024 Aug 28]. p. 133–50. (Local and Urban Governance). Available from: https://link.springer.com/10.1007/978-3-031-60657-1_9

[11] Hajar EM, Abdelghani C. Exploring the emergence of a new smart city model: case analysis of the Moroccan urbanization. In: 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM) [Internet]. IEEE; 2017 [cited 2024 Aug 28]. p. 293–9. Available from: https://ieeexplore.ieee.org/abstract/document/8122188/

[12] Kumar H, Singh MK, Gupta MP, Madaan J. Moving towards smart cities: Solutions that lead to the Smart City Transformation Framework. Technological forecasting and social change. 2020; 153:119281.

[13] Mdari YE, Daoud MA, Namir A, Hakdaoui M. Casablanca Smart City Project: Urbanization, Urban Growth, and Sprawl Challenges Using Remote Sensing and Spatial Analysis. In: Yang XS, Sherratt S, Dey N, Joshi A, editors. Proceedings of Sixth International Congress on Information and Communication Technology [Internet]. Singapore: Springer Singapore; 2022 [cited 2024 Aug 28]. p. 209–17. (Lecture Notes in Networks and Systems; vol. 216). Available from: https://link.springer.com/10.1007/978-981-16-1781-2_20

[14] EL ALAOUI A. Determinants of a smart city in Morocco. The Journal of Quality in Education. 2017;7(9):11–11.

[15] Nachit H, Jaafari M, El Fikri I, Belhcen L. Digital transformation in the Moroccan public sector: drivers and barriers. Available at SSRN 3907290 [Internet]. 2021 [cited 2024 Aug 28]; Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3907290

[16] Minoli D, Occhiogrosso B. Internet of Things Applications for Smart Cities. In: Hassan Q, editor. Internet of Things A to Z [Internet]. 1st ed. Wiley; 2018 [cited 2024 Aug 28]. p. 319–58. Available from: https://onlinelibrary.wiley.com/doi/10.1002/9781119456735.ch12

[17] Sarker IH. AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. SN COMPUT SCI. 2022 Mar;3(2):158.

[18] Jovanović Ž, Avdić A, Janković D, Vujičić D. Smart transportation in the service of improving healthcare in smart cities. 2018 [cited 2024 Aug 28]; Available from: https://www.researchgate.net/profile/Dejan-Vujicic/publication/327478069_Smart_Transportation_in_the_Service_of_Improving_Healthcare_in_Smart_Cities/links/5b91bb2ea6fdccfd541f7d7d/Smart-Transportation-in-the-Service-of-Improving-Healthcare-in-Smart-Cities.pdf

[19] Appio FP, Lima M, Paroutis S. Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges. Technological Forecasting and Social Change. 2019; 142:1–14.

[20] Hajar EM, Abdelghani C. Exploring the emergence of a new smart city model: case analysis of the Moroccan urbanization. In: 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM) [Internet]. IEEE; 2017 [cited 2024 Aug 28]. p. 293–9. Available from: https://ieeexplore.ieee.org/abstract/document/8122188/

[21] Baig ZA, Szewczyk P, Valli C, Rabadia P, Hannay P, Chernyshev M, et al. Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation. 2017; 22:3–13.

[22] Khan A, Jhanjhi NZ, Humayun M. The role of cybersecurity in smart cities. In: Cyber Security Applications for Industry 40 [Internet]. Chapman and Hall/CRC; 2022 [cited 2024 Aug 28]. p. 195–208. Available from: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003203087-9/role-cybersecurity-smart-cities-azeem-khan-noor-zaman-jhanjhi-mamoona-humayun

[23] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023;12(6):1333.

[24] Elgazzar RF, El-Gazzar R. Smart Cities, Sustainable Cities, or Both?-A Critical Review and Synthesis of Success and Failure Factors. In: International Conference on Smart Cities and Green ICT Systems [Internet]. SCITEPRESS; 2017 [cited 2024 Aug 28]. p. 250–7. Available from: https://www.scitepress.org/PublishedPapers/2017/63073/

[25] Hanine M, Boutkhoum O, El Barakaz F, Lachgar M, Assad N, Rustam F, et al. An intuitionistic fuzzy approach for smart city development evaluation for developing countries: Moroccan context. Mathematics. 2021;9(21):2668.

[26] Momani BT, Ettoudar M, Alhajaya N, Fayyad M. Securing Privacy: Safeguarding Against Cyber Threats in the UAE and Morocco. Global Privacy Law Review [Internet]. 2024 [cited 2024 Aug 28];5(3). Available from: https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/5.3/GPLR2024018

[27] Demertzi V, Demertzis S, Demertzis K. An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. Applied Sciences. 2023;13(2):790.

[28] Lis P, Mendel J. Cyberattacks on Critical Infrastructure: an Economic Perspective. EBR. 2019;5(2):24–47.

[29] Ma C. Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports. 2021; 7:7999–8012.

[30] Maleh Y, Maleh Y. Cybersecurity in Morocco [Internet]. Cham: Springer International Publishing; 2022 [cited 2024 Aug 28]. (Springer Briefs in Cybersecurity). Available from: https://link.springer.com/10.1007/978-3-031-18475-8

[31] Bennani B, Boukhima A. THE MOROCCAN CONSUMER AND CONSUMER PROTECTION LAW. [cited 2024 Aug 28]; Available from: https://www.researchgate.net/profile/Bennani-Bouchra/publication/349477199_THE_MOROCCAN_CONSUMER_AND_CONSUMER_PROTECTION_LAW/links/6032368a299bf1cc26de1686/THE-MOROCCAN-CONSUMER-AND-CONSUMER-PROTECTION-LAW.pdf

[32] Maleh Y, Maleh Y. Cybersecurity in Morocco [Internet]. Cham: Springer International Publishing; 2022 [cited 2024 Aug 28]. (Springer Briefs in Cybersecurity). Available from: https://link.springer.com/10.1007/978-3-031-18475-8

[33] Liu T, Mostafa S, Mohamed S, Nguyen TS. Emerging themes of public-private partnership application in developing smart city projects: a conceptual framework. Built Environment Project and Asset Management. 2021;11(1):138–56.

[34] Givens AD, Busch NE. Information sharing and public-private partnerships: The impact on homeland security. Homeland Security Rev. 2013; 7:123.