A Serious Game Conceptual Approach to Protect Critical Infrastructure Resilience in Smart Cities

Meisam Gordan, Mona Soroudi, Ili Ko
Postdoctoral Research Fellows, School of Civil Engineering, University College Dublin, Dublin, Ireland

Páraic Carroll, Daniel McCrum
Assistant Professors, School of Civil Engineering, University College Dublin, Dublin, Ireland

Sandra König, Stefan Schauer
Scientists, Austrian Institute of Technology, Safety & Security Department, Vienna, Austria

Lorcan Connolly
Associate, Research Driven Solutions Limited (RDS), Dublin, Ireland

ABSTRACT: Smart cities have become the most popular concept to manage assets and resources in the growing urban environment. To achieve sustainable city development in smart cities, it is imperative that smart development combined with sustainable practices should be integrated within infrastructure management frameworks. To improve resilience, it is essential to understand the interdependencies and cascading effects of Critical Infrastructures (CIs) subjected to cyber-physical threats. As a result of multiple influencing factors as well as the complex mechanisms in the interconnected smart systems of infrastructures, resilience assessment is highly challenging. To facilitate a deeper understanding of the influence of interdependent infrastructures, this paper proposes a novel serious gaming approach. This approach will incorporate the interdependent and cascading effects of infrastructures to improve the resilience scores. It also aids in improved infrastructure preparations to respond to cyber-physical threats with an 'educational' purpose through the mining of data from gameplay records. The serious game concept presented in this paper is being developed as part of the Horizon 2020-funded PRECINCT project (www.precinct.info).

1. INTRODUCTION

As cities have technologically developed steadily over the past decades, infrastructure management has been faced with increased challenges requiring new and efficient methods for infrastructure monitoring (Gordan et al. 2022b; Nguyen et al. 2021; Shirzad-Ghaleroudkhani et al. 2022). Global urbanization requires the development of sustainable and resilient infrastructure, which is one of the sustainable development goals (Xue et al. 2022). Sustainable infrastructures play a critical role in the development of cities, the improvement of their social welfare, and the reduction of their environmental impact (Xue and Xu 2018). Moreover, due to rapid urbanization globally, smart cities have become a hot topic in recent decades (Talebkhah et al. 2021). Europe in particular has put a great deal of effort into devising a strategy to achieve urban growth in a "smart" sense (Orejon-sanchez et al. 2022). In this direction, a smart city is composed of attributes, themes, and infrastructure. Furthermore, since themes are essential to the advancement of a smart city, they can also be considered pillars of the smart city. Infrastructure, which forms the operational platform for smart cities, is an essential feature of these cities (Nathali et al. 2018).

Developing smart cities requires an intricate network of interconnected infrastructures. The transportation industry, electric power, financial institutions, telecommunications networks, and oil and gas supplies are critical sectors that help society function in every way. These infrastructures are critical due to the impacts that their failure can have on the communities' security and well-being. Since these CIs are increasingly linked and automated, their functionalities have also become vulnerable. In other words, cyber-physical threats, human error or a malicious act, faulty equipment, or natural disasters are all real threats that can have serious consequences and given that these infrastructures are all interconnected, their widespread disruptions

cause cascading effects (König et al. 2019; Nguyen et al. 2021).

Interdependent infrastructures pose cascading risks that spread through interconnected infrastructure systems, presenting potentially life-threatening impacts to people in afflicted locations (König et al. 2022). Cascading effects in multi-hazard scenarios have become recognized as a priority in legislation relating to the control of major accident hazards (Chaoqi et al. 2021; Chowdhury and Gkioulos 2021). In addition, serious games have been gaining attention in recent decades for their potential role in addressing this challenging issue (Yamin et al. 2021). Serious gaming refers to a method with a purpose beyond pure entertainment, incorporating both the concepts of system and process complexity (Riel et al. 2017). The purpose of serious games is to simplify reality, providing users with the opportunity to practice decision-making and reflect on the results. Based on the above explanations, this paper presents an innovative approach to detect interlinked CI vulnerabilities in smart cities by using serious games as well as data mining of gameplay records to identify threats or cascading effects. This is due to the fact that a data mining framework is required for trend extraction from gameplay records to identify vulnerabilities to cascading cyber-physical threats.

2. CRITICAL INFRASTRUCTURE (CI)

As not only cyber-physical threats address CIs, but also sub-CIs, therefore before going into the details, it is important to present the existing list of CIs and sub-CIs due to the significant lack of such comprehensive information in the literature. Modern infrastructure systems are known as the foundation of cities. Such systems are considered as complex socio-technical ones that strongly contribute to the supply of goods and services to both private and public users. In infrastructure sectors where assets and networks are crucial for the security and well-being of the city, their failure would negatively impact economics, public health, and/ or security. Therefore, the term Critical Infrastructures (CIs) are used to indicate this importance (Kumar et al. 2021). Moreover, due to these facts, the protection of CIs is considered by decision-makers and urban planners to be of primary concern (Li et al. 2019). In other words, the CIs are physical sectors along with cyber and organizational subsectors and services that a country or community needs to function properly. Each sector and the corresponding subsectors have critical dependencies with other sectors. For instance, the Healthcare sector is highly dependent on Communications, Emergency Services, Energy, Food and Agriculture, Information Technologies (IT), Transportation, and Water sectors. In other words, each CI is in collaboration with other sectors due to its functionalities (Nipa et al. 2022; Ntafloukas et al. 2022; Song and Wu 2021).

3. CONCEPTUAL APPROACH

3.1. Smart City and Sustainable CIs

Globally, the rate of urbanization is accelerating both in developed and developing countries. The world's population is projected to grow to approximately 68% in urban areas by 2050 (Melati 2022). Thus, to facilitate this process, many researchers propose several city-development initiatives. In the same direction, although there is no widely agreed definition for a smart city, numerous attempts are made to reflect the multidimensional and multidisciplinary aspects of what a smart city consists of (Ahad et al. 2020).

Studies investigated the fundamental principles of smart cities in a variety of ways. As the main factors of the smart city, some have focused on digital technologies, while others have concentrated on the physical infrastructure required. Some experts, on the other hand, have emphasized community-centric smart cities, highlighting how physical infrastructure and digital technologies support the public (Calixto et al. 2019). It is commonly accepted that there are three key components for smart cities namely society (community), physical infrastructure, and digital technologies (Schipper and Silvius 2018).

A smart city collects and processes data from its residents and devices to enhance operational efficiency, public communication, and the quality of public services and citizen well-being. A smart city's architecture consists of various components, technically. There are several approaches to indicate how these components are interrelated and coordinated.

The significance of smart CI cannot be overstated due to their roles to provide a framework for the development of smart cities. In general, there are four types of interdependence between CIs including physically, geographically, cybernetically, and logically. Generally, there are five categories in which to analyze these interdependencies comprising agent-based, empirical, economic, system dynamics, and

network (Rinaldi et al. 2001). Among all, empirical and network categories aim to identify risks and failure patterns and focus on topology and flow, respectively.

As mentioned before, intentional cyber-physical attacks such as malware, terrorist-driven exploits, as well as natural hazards like extreme weather, fires, earthquakes, catastrophic implications of climate change and hybrid threats are exposing CIs at risk. Individual CIs such as energy distribution, transportation, and other CIs are the focus of recent studies and innovative approaches (Cantelmi et al. 2021; Ntafloukas et al. 2023; Rehak et al. 2022). However, managing the impact of cascading effects resulting from interdependencies between different types of CIs and their resilience is highly challenging (Osei-kyei et al. 2021). The vulnerability of cities highlights the necessity of strong public-private collaboration to deploy responses from sectors as diverse as food production, telecommunications, and supply chains, as well as a higher level of security for connected essential infrastructure. In this perspective, smart city pervasive connection indicates a rising threat with continuous exposure to new threats that can impact cities' economies, data sources, infrastructures, connected devices, and community safety. To summarize, the interdependencies between CIs, especially their connections to emergency services and smart city systems, must be addressed in a more holistic way to improve public safety and security (PRECINCT 2020).

3.2. Resilience and Cascading Effects

The PRECINCT Resilience Methodological Framework (RMF) is illustrated in Figure 1. The framework has been developed to complement the PRECINCT Ecosystem and approaches adopted for each Living Lab, while bearing in mind the multiple CIs involved. The first step is the definition of the CI, including all relevant parts of it. Subsequently, the service provided by the CI is quantified. The PRECINCT RMF quantifies resilience in terms of the service measures provided by the CI. Examples of service measures may include passenger kms carried by a transport network or the number of patients served by a hospital. The framework requires each service measure to be quantified in monetary terms to compare resilience enhancements across various CIs. Resilience is then quantified in terms of the losses in service due to a specific cyber-physical event. Resilience indicators are used to apportion the losses to specific parts of the CI, which can then be attributed to potential resilience enhancements by setting targets for these indicators. Examples of indicators may include the condition of specific parts of the CI, the practice of emergency plans, or the availability of emergency resources. The percentage of fulfilment of each indicator may be used to give an indication of the relative impact on the CI.

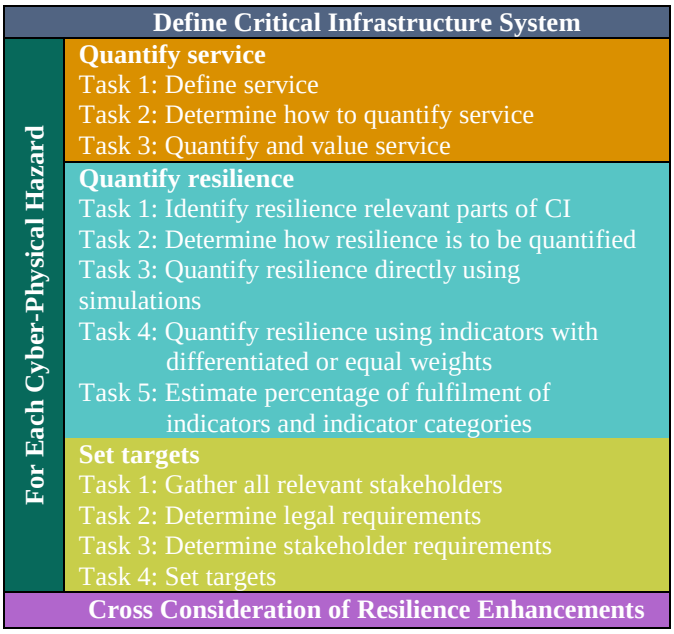

Figure1: PRECINCT Resilience Methodological Framework.

The above steps are carried out for each cyber physical hazard, and subsequently, resilience enhancements are considered in the overall context of the CI network and the threats to which it is exposed. Within the PRECINCT Ecosystem, the impact of resilience enhancements is read from the cascading effects and interdependency graphs. The graphs for each Living Lab will contain output nodes with a certain number of potential states with associated probabilities. By quantifying the losses associated with each state one can quantify the total expected losses given a particular triggering event, for a particular combination of resilience indicator node states. The aim from a resilience optimisation perspective is therefore to minimise these losses by selecting the optimum combination of resilience indicator node states, across all triggering events. The main constraint in the optimisation is of course the budget available to put resilience enhancements in place.

As part of the PRECINCT Living Labs, various optimisation and machine learning algorithms will

be investigated to determine the best strategy for resilience enhancement. Furthermore, the outputs of all potential resilience enhancement combinations will be calculated from the interdependency graphs and used in the back end of the serious game. This will allow the training of users to understand where and when to implement interventions.

The PRECINCT Cascading effects model is an integral part of the RMF, as outlined in Figure 2. In order to evaluate the resilience to a specific trigger event, the monetary losses associated with trigger events must be calculated. The total loss associated with the event is evaluated by multiplying the associated outcome probabilities by the associated monetary losses and summing for all measures of service included in the assessment.

The final step in the RMF involves the setting of resilience targets based on stakeholder issues, legal requirements, and cost-benefit analysis (CBA). CBA requires the calculation not only of the cost of resilience enhancements, but also the impact in terms of the savings made in the event of a hazard occurring. This may be achieved by examining the probabilistic damage states within the cascading effects simulation, given a hazard of a specific magnitude. All indicators are set to their actual values.

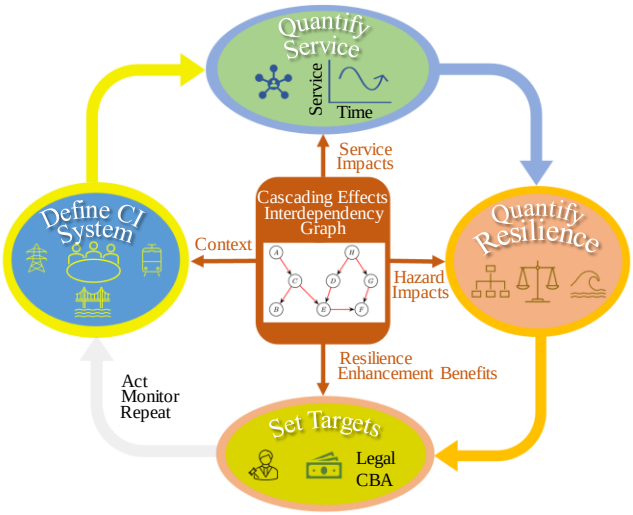

Figure 2: Application of PRECINCT Cascading Effects and Interdependency Graphs to RMF.

3.3. Serious Game

A Serious Game is a computer-based simulation that merges knowledge and skills development with video game-playing aspects to enable active, experiential, situated, and problem-based learning (Johnsen et al. 2018). Developing serious games with sustainability, resilience, and dynamic agendas, taking cognizance of the interconnected infrastructure would lead to more sustainable smarter cities. Therefore, this research aims to improve the CI resilience using serious gaming approach for smart cities to achieve their sustainable development goals.

The proposed architecture of the Serious Game is presented in Figure 3. As it is presented, geospatial data provides the information for the Serious Game's visualization, which is used in the Serious Game's backend. Various spatial formats and geodatabases will be supported in the back-end database. Datasets contain key attribute information that can be queried and filtered via Structured Query Language (SQL) and geospatial web services via spatial or non-spatial databases. Geographic Information Systems (GIS) have filtering capabilities for analysing data to simulate cascading effects, based on the resilience methodological framework, for complex scenarios including cyber- and physical infrastructures compromised. It should be noted that the aforesaid framework will be applied for quantification of resilience and identification of strategies to enhance resilience.

As shown in Figure 3, the Serious Game architecture is divided into the front end and the back end. Serious Games provide an interactive user interface that integrates and communicates with simulations on the back end through an interactive decision support system and scenario specification/building process. Game client development includes the development of the serious gaming front-end in accordance with the Game Design Document, and the back end for storing and analysing individual user interactions. For client development and development architecture, Unity Engine and the corresponding libraries and frameworks for game programming will be used. Applications and games comprise the following activities:

- Establishing a Unity3D project and environment.
- Programming game interactions.
- Game features, e.g., cascading effects and feedback loops.
- Integration of the client application into the backend.
- Communication/data exchange between client and backend.

3.4. Digital Twins

A Digital Twin (DT) is a virtual, cloud-based, representation or the digital coupling of the state of an asset or a process with a functional output. The concept of DTs has been around since the early 2000's. It was first adopted in the space and aircraft industry by NASA and the U.S. Airforce, it gradually found its way to other application domains, e.g., Industry 4.0, Smart Manufacturing, Healthcare and Smart Cities. NASA applied it in its technology roadmap on modelling, simulation, information technology and processing (Shafto et al. 2012). Likewise, DTs, combining data / Internet of Things (IoT) networks, AI and 3D visualisation, have been investigated in the recent years as promising decision support tools for different applications (Gordan et al. 2023). This technology enables companies to create simulations that predict an object or process performance using the physical world's data in real-time. It forms the bridge between the physical and digital objects. This may be associated with the fact that for every physical asset, there exists a digital asset.

There are assets associated with the actual game, such as background graphics and gameplay graphics that assist in making the game an immersive experience for the player, as well as additional media for providing the user with information about the training scenario. It should be noted that the development of the proposed serious game will utilise the inputs from Digital Twins (DT), which includes various databases, e.g., geo spatial data, computed cascading effects, resilience, etc.

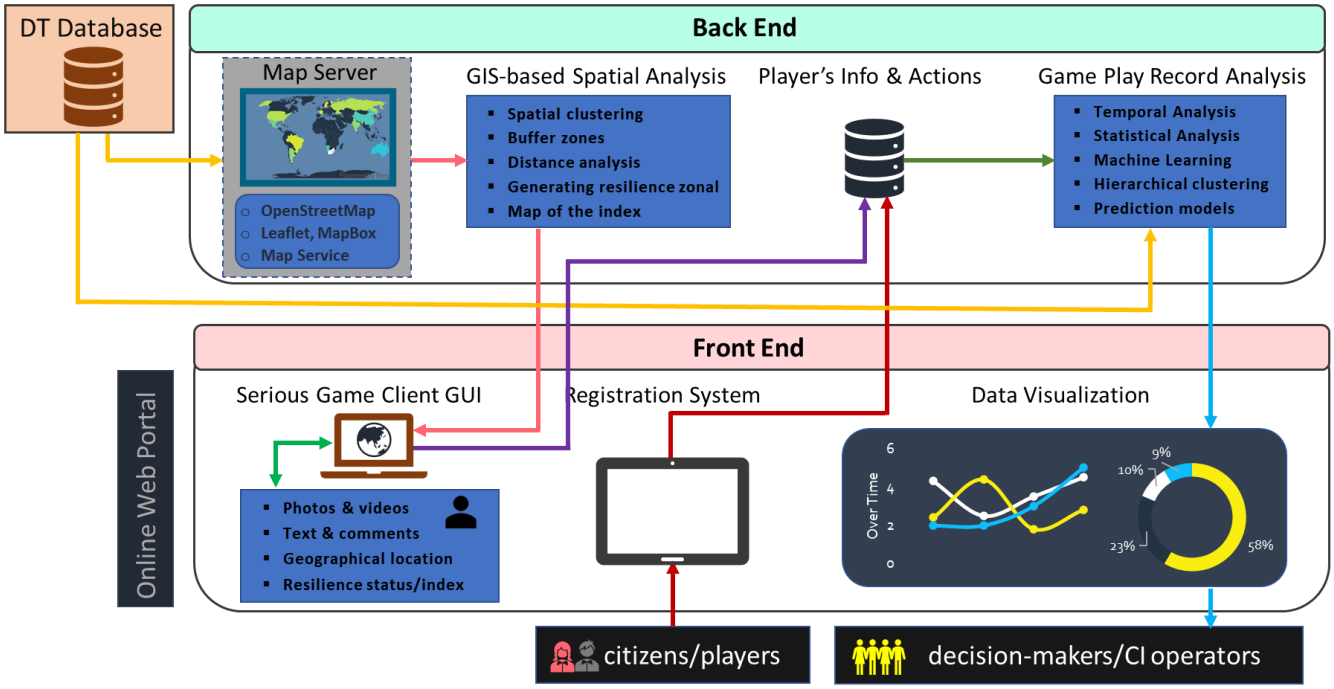

Figure 3: Serious Game system architecture.

The overall steps involved in playing the proposed serious game are shown in Figure 4. Based on an analysis of the gameplay records, the most important output from the Game will be the identification of city/district vulnerabilities (Step 7 in Figure 4). Cascading effects is a key part of this, thus software to 'data mine' the gaming records will be developed to identify trends in attack and defense scenarios and will auto-generate periodic reports of trends identified.

A data mining algorithm will be deployed on the server of the serious game, tracking defined interactions of the user and the system. According to (Hand et al. 2001), data mining is defined as "The analysis of large observational data sets to find unsuspected relationships and to summarize the data in novel ways so that data owners can fully understand and make use of the data". There are three types of data mining techniques which consist of statistical techniques, machine learning techniques and artificial intelligence techniques and each of them has several methods (Gordan et al. 2017, 2022c). For instance, statistical methods include regression analysis, clustering analysis,

decision tree, etc., and machine learning methods such as principal component analysis, case-based reasoning, support vector machine and so forth. Another category with various algorithms is artificial intelligence, e.g. fuzzy logic, genetic algorithm, artificial neural network and particle swarm algorithm. In recent years, these algorithms have also been utilized for structural health monitoring (Gordan et al. 2018, 2020b; a, 2021a; b, 2022d; a; Tan et al. 2020).

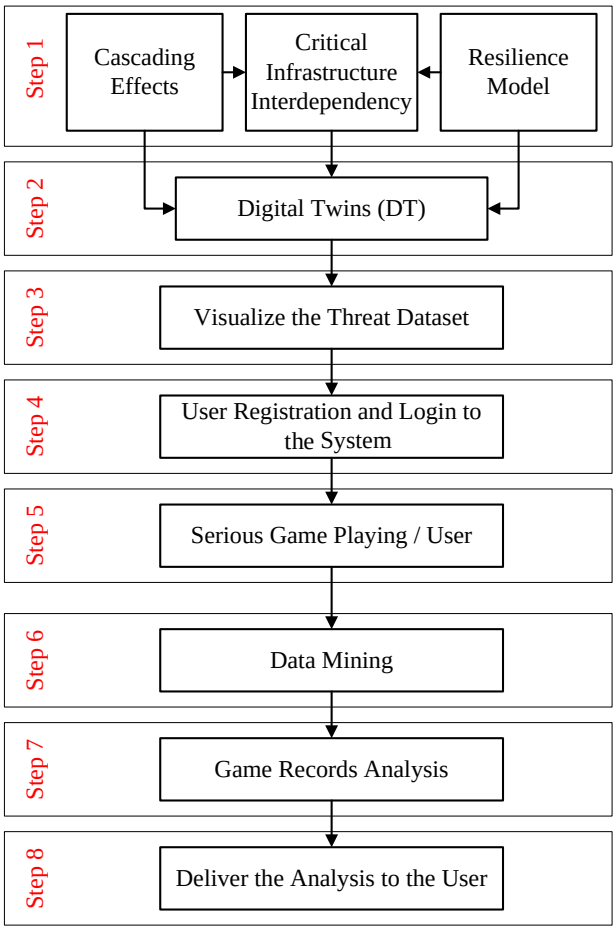

Figure 4: Gameplay stpes of the proposed serious game.

These trends will highlight potentially unidentified interdependencies and cascading effects as well as measures taken by the players to counter them and facilitate the updating of conditional probabilities. Finally, the outputs of the game will be analyzed via the resilience methodological framework, (1) to quantify the system resilience during and after the game is played, and (2) to determine short- and long-term resilience. The effect of alternative strategies on the system resilience will also be assessed, accordingly.

4. CONCLUSION

In the modern society, every city contains many structures as well as infrastructures that the citizens expect to be accessible on demand with reliable functionality, and resilient to cyber-physical threats. Infrastructures are fundamental components for sustainable development in smart city planning. Interdependence and interconnections of urban infrastructures, such as transportation, energy, and communications, cause them to affect each other, inevitably. In addition to the interdependencies and interconnections of smart infrastructure, each infrastructure relies on other infrastructures to operate. For example, the transport network depends on the energy network and communication network to operate. These interdependent infrastructures are vulnerable due to a wide range of threats such as natural or cyber threats. Therefore, in this study, a Serious Game system architecture along with its conceptual approach have been developed accordingly to identify threats or cascading effects in CIs and assess their resilience. The proposed Serious Game will offer an interactive decision support and scenario specification/building user interface that the player interacts with when gaming, which integrates and communicates with back-end simulations. Repeating gameplay of attack scenarios will allow users to understand the resilience of their infrastructure and test mitigation strategies to improve the resilience of their CIs. The output of this research will be beneficial for smart physical, digital, and society infrastructure, as well as the stakeholders of smart cities, e.g., the CIs operators, solution providers, investors, political leaders, and end users. Future work will implement the serious game approach in four Living Labs i.e. Antwerp, Ljubljana, Athens and Bologna.

5. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude and appreciation to University College Dublin, and the PRECINCT project (www.precinct.info) which funded by the European Union's Horizon 2020 research and innovation programme. This work was supported by grant agreement number 101021668.

6. REFERENCES

Ahad, M. A., Paiva, S., Tripathi, G., and Feroz, N. (2020). “Enabling technologies and sustainable smart cities.” *Sustainable Cities and Society*, Elsevier, 61, 102301.

Calixto, V., Gu, N., and Celani, G. (2019). "A critical framework of smart cities development." *Intelligent & Informed, Proceedings of the 24th International Conference of the Association for Computer-Aided Architectural Design Research in Asia (CAADRIA) 2019*, Hong Kong, 685–694.

Cantelmi, R., Di Gravio, G., and Patriarca, R. (2021). *Reviewing qualitative research approaches in the context of critical infrastructure resilience*. *Environment Systems and Decisions*, Springer US.

Chaoqi, F., Yangjun, G., Jilong, Z., Yun, S., Pengtao, Z., and Tao, W. (2021). "Attack-defense game for critical infrastructure considering the cascade effect." *Reliability Engineering and System Safety*, Elsevier Ltd, 216, 107958.

Chowdhury, N., and Gkioulos, V. (2021). "Cyber security training for critical infrastructure protection : A literature review." *Computer Science Review*, Elsevier Inc., 40, 100361.

Gordan, M., Chao, O. Z., Sabbagh-Yazdi, S.-R., Wee, L. K., Ghaedi, K., and Ismail, Z. (2022a). "From Cognitive Bias Toward Advanced Computational Intelligence for Smart Infrastructure Monitoring." *Frontiers in Psychology*, 13.

Gordan, M., Ghaedi, K., Ismail, Z., Benisi, H., Hashim, H., and Ghayeb, H. H. (2021a). "From Conventional to Sustainable SHM: Implementation of Artificial Intelligence in The Department of Civil Engineering , University of Malaya." *3rd IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET2021)*, IEEE, Kota Kinabalu, Malaysia, 1–6.

Gordan, M., Ghaedi, K., and Saleh, V. (2023). *Industry 4.0 - Perspectives and Applications*. IntechOpen Limited, London, UK.

Gordan, M., Ismail, Z., Abdul Razak, H., Ghaedi, K., Ibrahim, Z., Tan, Z. X., and Ghayeb, H. H. (2020a). "Data mining-based damage identification of a slab-on-girder bridge using inverse analysis." *Measurement*, Elsevier Ltd, 151, 107175.

Gordan, M., Razak, H. A., Ismail, Z., and Ghaedi, K. (2017). "Recent developments in damage identification of structures using data mining." *Latin American Journal of Solids and Structures*, 14(13), 2373–2401.

Gordan, M., Razak, H. A., Ismail, Z., and Ghaedi, K. (2018). "Data mining based damage identification using imperialist competitive algorithm and artificial neural network." *Latin American Journal of Solids and Structures*, 15(8), 1–14.

Gordan, M., Razak, H. A., Ismail, Z., Ghaedi, K., Tan, Z. X., and Ghayeb, H. H. (2020b). "A hybrid ANN-based imperial competitive algorithm methodology for structural damage identification of slab-on-girder bridge using data mining." *Applied Soft Computing Journal*, Elsevier B.V., 88, 106013.

Gordan, M., Sabbagh-Yazdi, S.-R., Ghaedi, K., Thambiratnam, D. P., and Ismail, Z. (2022b). "Introduction to Optimized Monitoring of Bridge Infrastructure Using Soft Computing Techniques." *Applied Methods in Bridge Design Optimization - Theory and Practice*, IntechOpen Limited, London.

Gordan, M., Sabbagh-Yazdi, S.-R., Ismail, Z., Ghaedi, K., and Ghayeb, H. H. (2021b). "Data Mining-based Structural Damage Identification of Composite Bridge using Support Vector Machine." *Journal of Artificial Intelligence and Data Mining (JAIDM)*, 9(4), 415–423.

Gordan, M., Sabbagh-yazdi, S., Ismail, Z., Ghaedi, K., Carroll, P., McCrum, D., and Samali, B. (2022c). "State-of-the-art review on advancements of data mining in structural health monitoring." *Measurement*, 193, 110939.

Gordan, M., Siow, P. Y., Deifalla, A. F., Chao, O. Z., Ismail, Z., and Yee, K. S. (2022d). "Implementation of a Secure Storage Using Blockchain for PCA-FRF Sensor Data of Plate-Like Structures." *IEEE Access*, IEEE, 10, 84837–84852.

Hand, D. J., Mannila, H., and Smyth, P. (2001). *Principles of Data Mining*. MIP press.

Johnsen, H. M., Fossum, M., Vivekananda-schmidt, P., Fruhling, A., and Slettebø, Å. (2018). "Developing a Serious Game for Nurse Education." *Journal of gerontological nursing*, 44(1), 15–19.

König, S., Rass, S., Rainer, B., and Schauer, S. (2019). "Hybrid Dependencies Between Cyber and Physical Systems." *Intelligent Computing-Proceedings of the Computing Conference*, Springer, Cham, 550–565.

König, S., Schauer, S., Soroudi, M., Ko, I., Gordan, M., Carroll, P., and McCrum, D. (2022). "Risk Management with Multi-categorical Risk Assessment." *Advances in Modelling to Improve Network Resilience: Proceedings of the 60th European Safety, Reliability, & Data Association (ESReDA) Seminar*, University Grenoble Alpes, Grenoble, France, 105–113.

Kumar, N., Poonia, V., Gupta, B. B., and Goyal, M. K. (2021). "A novel framework for risk assessment and resilience of critical infrastructure towards climate change." *Technological Forecasting & Social Change*, Elsevier Inc., 165, 120532.

Li, Y., Qiao, S., Deng, Y., and Wu, J. (2019). "Stackelberg game in critical infrastructures from

a network science perspective." *Physica A*, Elsevier B.V., 521, 705–714.

Melati, R. G. (2022). "The Strategies of United Nations Development Programme (UNDP) with Global Environmental Facility (GEF) to Promote Sustainable Land Management." *Syntax Literate: Journal Ilmiah Indonesia*, 7(1).

Nathali, B., Khan, M., and Han, K. (2018). "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities." *Sustainable Cities and Society*, Elsevier, 38, 697–713.

Nguyen, T. N., Liu, B.-H., Nguyen, P., Dumba, B., and Chou, J.-T. (2021). "Smart Grid Vulnerability and Defense Analysis Under Cascading Failure Attacks." *IEEE Transactions on Power Delivery*, IEEE, 36(4), 2264–2273.

Nipa, T. J., Kermanshachi, S., and Subramanya, K. (2022). "Development of Innovative Strategies to Enhance the Resilience of the Critical Infrastructure." *Construction Research Congress*, ASCE, 111–120.

Ntafloukas, K., Mccrum, D. P., and Pasquale, L. (2022). "A Cyber-Physical Risk Assessment Approach for Internet of Things Enabled Transportation Infrastructure." *Applied Sciences*, 12(18), 9241.

Ntafloukas, K., Pasquale, L., Martinez-pastor, B., and Mccrum, D. P. (2023). "A Vulnerability Assessment Approach for Transportation Networks Subjected to Cyber – Physical Attacks." *Future Internet*, 15(3), 100.

Orejon-sanchez, R. D., Crespo-garcia, D., Andres-diaz, J. R., and Gago-calderon, A. (2022). "Smart cities' development in Spain : A comparison of technical and social indicators with reference to European cities." *Sustainable Cities and Society*, Elsevier Ltd, 81, 103828.

Osei-kyei, R., Tam, V., Ma, M., and Mashiri, F. (2021). "Critical review of the threats affecting the building of critical infrastructure resilience." *International Journal of Disaster Risk Reduction*, Elsevier Ltd, 60, 102316.

PRECINCT. (2020). "Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection." *European Union's Horizon*, <https://www.precinct.info/>.

Rehak, D., Hromada, M., Onderkova, V., Walker, N., and Fuggini, C. (2022). "Dynamic robustness modelling of electricity critical infrastructure elements as a part of energy security." *International Journal of Electrical Power and Energy Systems*, Elsevier Ltd, 136, 107700.

Riel, W. van, Post, J., Langeveld, J., Herder, P., and Clemens, F. (2017). "A gaming approach to networked infrastructure management." *Structure and Infrastructure Engineering*, Taylor & Francis, 13(7), 855–868.

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). "Identifying, understanding, and analyzing critical infrastructure interdependencies." *IEEE control systems magazine*, IEEE, 21(6), 11–25.

Schipper, R. P. J. R., and Silvius, A. J. G. (2018). "Characteristics of Smart Sustainable City Development: Implications for Project Management." *Smart Cities*, 1, 75–97.

Shafto, M., Conroy, M., Doyle, R., Glaessgen, E., Kemp, C., LeMoigne, J., Wang, L., and April. (2012). *Modeling, Simulation, Information Technology & Processing Roadmap NACA*. National Aeronautics and Space Administration.

Shirzad-Ghaleroudkhani, N., Mei, Q., and Gul, M. (2022). "A crowdsensing-based platform for transportation infrastructure monitoring and management in smart cities." *The Rise of Smart Cities*, Butterworth-Heinemann, 609–624.

Song, Y., and Wu, P. (2021). "Earth Observation for Sustainable Infrastructure : A Review." *Remote Sensing*, 13(1528), 1–20.

Talebkhah, M., Sali, A., Marjani, M., Gordan, M., Hashim, S. J., and Rokhani, F. Z. (2021). "IoT and Big Data Applications in Smart Cities: Recent Advances, Challenges, and Critical Issues." *IEEE Access*, 9, 55465–55484.

Tan, Z. X., Thambiratnam, D. P., Chan, T. H. T., Gordan, M., and Abdul Razak, H. (2020). "Damage detection in steel-concrete composite bridge using vibration characteristics and artificial neural network." *Structure and Infrastructure Engineering*, Taylor & Francis, 16(9), 1247–1261.

Xue, B., Chen, X., Liu, B., Zhao, D., Zhang, Z., and In, J. (2022). "Ontologies representing multidisciplinary decision-making rationales for sustainable infrastructure developments." *Sustainable Cities and Society*, Elsevier Ltd, 77, 103549.

Xue, B., and Xu, H. (2018). "A Whole Life Cycle Group Decision-Making Framework for Sustainability Evaluation of Major Infrastructure Projects." *The 21st International Symposium on Advancement of Construction Management and Real Estate*, Springer, Singapore, 129–140.

Yamin, M. M., Katt, B., and Nowostawski, M. (2021). "Serious games as a tool to model attack and defense scenarios for cyber-security exercises." *Computers & Security*, Elsevier Ltd, 110, 102450.