Scientific Research Publishing

World Journal of Engineering and Technology, 2025, 13(3), 486-501
https://www.scirp.org/journal/wjet
ISSN Online: 2331-4249
ISSN Print: 2331-4222

Securing Waterside and Maritime Infrastructure in New York State: Evaluating Strategies and Maturity Models for Critical Protection

Robb Shawe

Department of Critical Infrastructure, Capitol Technology University, Laurel, MD, USA
Email: rshawe@captechu.edu

How to cite this paper: Shawe, R. (2025) Securing Waterside and Maritime Infrastructure in New York State: Evaluating Strategies and Maturity Models for Critical Protection. *World Journal of Engineering and Technology*, **13**, 486-501.
https://doi.org/10.4236/wjet.2025.133032

Received: April 2, 2025
Accepted: August 2, 2025
Published: August 5, 2025

Abstract

One of the case studies illustrates the protection and security of waterside and maritime infrastructure in New York State, where power stations, oil and gas refineries, LNG facilities, and ports are vital facilities. This case study analyzes the use of maturity models, including the Cybersecurity Capability Maturity Model (C2M2) and the Smart Grid Information Maturity Model (SGIMM). This case study evaluates and explains how these models are used and designed to enhance the cybersecurity capabilities of critical infrastructures. A practical approach to critical infrastructure protection requires understanding potential risks. Threats can come from various sources, including natural disasters, cyberattacks, and sabotage. As a result, tailored response plans can be created that enhance resilience by identifying these risks. Training personnel and conducting regular drills will ensure readiness in case of emergencies. Furthermore, investing in advanced monitoring systems can alert authorities to potential breaches before they escalate, minimizing damage or disruption. A proactive stance is vital for protecting New York's maritime environment. Collaboration among government agencies, private sector partners, and local communities is crucial to the successful protection of infrastructure. This collaboration, which can build a more robust defense network by working together and sharing information and resources, offers hope for a more secure future. Public awareness campaigns can also educate citizens about their crucial role in reporting suspicious activities, thus fostering a culture of vigilance and making them integral to the security process. By investing in a comprehensive strategy and maturity model, New York State can ensure its maritime infrastructure remains secure and resili-

ent in the face of future challenges.

Keywords

Infrastructure Protection, Resilience, Risk Management, Collaboration, Technology Integration, Maritime Infrastructure, Maturity Models, Environmental Assets, C2M2, SGIMM, Community Engagement, Emergency Response Plans, Public Safety

1. Introduction

The multitude of vulnerabilities concerning the waterside and maritime infrastructure of New York State requires a comprehensive and pragmatic view of its security. In this regard, the utmost importance should be allocated to protecting the aforementioned critical and irreplaceable resources that are pivotal to economic interests and public well-being. The following paper aims to highlight the vulnerabilities in the existing security paradigms characteristic of the state and their implications for the security of its maritime area. This paper will review existing security practices and processes to analyze these vulnerabilities. The focus will be on security maturity models, their growth, and their application in the field. The Cybersecurity Capability Maturity Model (C2M2) and the Smart Grid Information and Management Maturity Model (SGIMM) will also be discussed. Examples of these models are established as methodologies and frameworks to improve processes and organizational security levels.

Furthermore, the discussion will also cover the potential hurdles that may arise while applying these maturity models. The difficulties associated with each model will be identified, and how it can be appropriately adjusted according to the context of maritime security. It is anticipated that the elements of resources, technological disruptions, and training will play a critical role in the practical application of these models. To contextualize the discussion on questions of maritime security, the paper presents empirical case studies. The case studies will exemplify specific situations wherein the different strategic security approaches were utilized and the results obtained. The case studies will further illustrate the cost-effectiveness of the different approaches in terms of their capability to decrease the frequency of instances and improve the space's security.

The underlying goal of the paper is to foster appropriate awareness concerning the applicability and utility of these maturity models to enhance the security of the maritime infrastructure. By providing appropriate recommendations, the paper aims to secure the discussed models, which will assist in meeting the existing security levels and eliminate the threats, which will only increase over time. The paper, therefore, will contribute to resolving the issues concerning the security of the maritime infrastructure of New York State amid the growing challenges caused by increased security threats.

2. Overview: Waterside and Maritime Infrastructure in New York State

New York State's waterside and maritime infrastructure is a critical component of the state's transportation and logistics system. Made up of various interconnected ports, terminals, and support services, this infrastructure facilitates the efficient movement of cargo and passengers, supporting the smooth flow of goods and business throughout the region. Yet, the intricacies of maintaining and advancing the infrastructure require a robust strategy for the system's upkeep and protection [1]. The nature of the infrastructure relates to its complexity, as it comprises many different components. The interrelations between physical infrastructure and digital networks require different strategies for protecting specific assets. In terms of resilience, the infrastructure faces existing and evolving threats from environmental, technological, and security challenges. Protecting the various elements against current and future threats demands an ongoing assessment and review of existing practices to safeguard these infrastructure elements from new vulnerabilities [2].

It is, thus, worth noting that the New York State waterfront and maritime infrastructure is strategically important not just because it ensures logistics for the various processes but also because it is the region's security and economic backbone. It appears to be a natural part of the global supply chain, and its disruption can have a ripple effect on several aspects of trade and commerce, thereby proving its vital influence on stability in the economy. In addition, as threats on the international stage continue to become diverse and multiply, securing them is primarily important for ensuring the security of national interests and geopolitical stability [2]. Admittedly, it is one of the foundations of the economy, and the state must, therefore, organize security measures to avoid the possibility of risking its stability and incurring economic losses. For this reason, preventing the occurrence of disruptive phenomena demands attention to the level of security enforcement, which should be inextricably linked with the economic demands and the infrastructure type at hand to ensure that results are achieved both in terms of the economy and security and protection capabilities [1].

Moreover, New York's unique geographical features of its marine facilities pose unique security challenges with the demand for well-planned and flexible measures. Its long coastline and linked waterways provide additional business opportunities but increase risks from various threats, from environmental events to cyberattacks on interconnected facilities and networks [3]. Logistically, the size of operations involving the security of many vessels, their movement, and the need to secure and maintain marine structures is highly challenging. The high volume and age of road and waterway traffic increase the chances of accidents and potential security incidents, demanding security protocols that can withstand and adjust to changing situations [4]. In addition, the use of advanced technologies in the logistical operations of marine facility security is critical for optimal operational response and improved efficiency of logistical operations in these infrastructures in the face of the ever-changing security environment.

2.1. Key Facilities: Oil and Gas Refineries

Oil and gas refineries are key players in New York's energy supply chain, serving as fundamental components of the state's overall energy systems. These industrial complexes convert crude oil into various finished petroleum products, including gasoline, diesel, and jet fuel, which are essential for modern transportation networks and industrial supply chains. Their significance extends beyond production; they are crucial for maintaining the operational continuity of sectors heavily reliant on a stable and consistent energy supply. However, their operations are not without challenges and risks, particularly the growing threat of cyberattacks. Depending on their output, such cyber threats can cause significant disruptions to refineries and the broader energy supply chain, impacting everything from fuel availability to industrial production across the state.

Furthermore, the strategic location of these refineries, often in urbanized regions of New York, adds another layer of complexity. Being situated near densely populated areas increases the potential consequences of any physical security threats or environmental incidents, such as oil spills, as these can directly affect nearby communities and critical infrastructure. Given these vulnerabilities, adopting comprehensive security measures to safeguard these essential facilities is crucial. This necessitates a dual approach: implementing advanced cybersecurity strategies in conjunction with robust physical security measures. By doing so, the state can better protect these vital infrastructures, thereby ensuring the uninterrupted energy flow necessary to sustain New York's critical infrastructure network and support its diverse economic activities.

Moreover, New York State's oil and gas refineries face many security threats and risks, given the nature of their operations and the critical infrastructure they represent. On the one hand, cyber threats pose a significant challenge to the industry, as both malicious actors and internal personnel may gain unauthorized access to industrial control systems, breaching operations or damaging equipment, which can lead to dire economic and environmental impacts [5]. On the other hand, physical threats and risks remain possible, as refineries could also become vulnerable to unauthorized access and sabotage, compromising safety and production. As such, it is vital to establish an effective dual strategy that covers both cyber and physical security to maximize the protection of refinery assets, facilities, and people. If combined with physical security enhancements, establishing a mature cybersecurity framework such as C2M2 would ensure that both systems continuously evolve, considering the industry's emerging threats and challenges.

2.2. Liquefied Natural Gas (LNG) Facilities: Importance

Liquefied Natural Gas (LNG) facilities play a crucial role in New York State's energy infrastructure by significantly contributing to energy diversification and security. LNG systems are engineered to convert natural gas into a liquid, essential for efficient storage and transportation [6]. This process facilitates natural gas distribution to consumers, particularly in markets that lack an extensive pipeline net-

work, thereby addressing energy access in areas that might otherwise face shortages. Despite their importance, LNG facilities face significant security challenges. These installations are considered critical and valuable strategic assets due to their key role in the state's energy supply chain. Consequently, the potential impact of a security breach is severe, as it could result in catastrophic consequences for the facility and the region's overall energy security [6]. Therefore, robust safety and security precautions are mandatory to prevent such incidents.

Furthermore, the geographic placement of LNG terminals is carefully selected to optimize accessibility and strategic advantage, with additional security considerations also being considered. These terminals are strategically positioned, making them potential targets for physical and cyber-attacks. In the digital age, threats from cyberspace are increasingly prevalent, and unauthorized access or sabotage attempts could cripple the energy infrastructure. As a result, these facilities must be well-protected against such technologically sophisticated threats.

Implementing a comprehensive security framework is imperative during the planning and development of LNG infrastructure. This framework should encompass physical security measures and cybersecurity protocols tailored to protect the facility from a wide range of high-impact threats. The provider must ensure that LNG sites' security architecture and design are robust and resilient, capable of safeguarding against known and emerging risks, to continue providing reliable energy to the state. Moreover, unique threats also pose challenges to LNG facilities, necessitating extensive safety measures. LNG facilities are vulnerable to cyber and physical attacks that could compromise their functionality, particularly as they promote energy diversification [6]. Safety measures include strict monitoring procedures that apply advanced surveillance systems and physical installations to limit unauthorized access. Implementing cybersecurity practices, such as data encryption and real-time monitoring systems, can enhance the security of such facilities against cyberattacks [5]. The combined measures are crucial in protecting LNG facilities from operations that could disrupt the stable natural gas supply in New York State.

2.3. Ports and Power Stations: Critical Nodes

In New York State, the infrastructural elements comprising the ports and power stations form the backbone of its extensive infrastructure network, playing an indispensable role in the resilience of energy supply and sustaining its economic vitality. The ports are pivotal connectors in global trade, serving as crucial nodes that facilitate the smooth flow of import and export activities, reinforcing New York State's economic influence on national and international stages. These ports are central to the state's economic strength as they enable businesses to engage in international commerce, attract investment, and bolster economic growth. Recognizing their importance, these facilities must be safeguarded against cyber and physical threats, as any interruption could affect and severely disrupt commerce. Therefore, implementing robust response mechanisms ensures that global trade

continues seamlessly despite potential disruptions [7].

In parallel, the power stations in New York State play an equally vital role by providing a stable and continuous supply of energy necessary for the functioning of other critical infrastructures. This uninterrupted energy supply supports various essential services, including hospitals, transportation systems, and communication networks, which rely heavily on consistent power to operate efficiently. The importance of these facilities demands a comprehensive security framework that incorporates technological solutions, physical barriers, and effective procedural or personnel measures. This holistic approach is crucial to protecting power stations against any attempts to compromise their operations and ensuring they remain fully functional and capable of responding to potential threats. Through such strategic protection efforts, New York State can maintain the integrity and reliability of its critical infrastructure systems, thereby safeguarding its social and economic operations.

Another factor that affects security policies is the potential for physical damage to power stations and the port and vice versa. Power stations can also cause harm to the port. Ports are central to the state's economic strength since they support the demands of the import and export industries. On the other hand, power stations are needed to provide energy for the port to function. There is also a relationship with infrastructure stability here, as if the ports' operating hours are significantly affected, commodities will start to rot or stop, which would have a highly detrimental impact on stability. This means that security policies should not be limited to physical and cyber threats but should encompass everything that could threaten these networks and integrated systems [7]. That would be necessary because being intelligent and forming effective security policies could help secure all these infrastructures and their respective demands, ensuring the stability of their network connections.

In tandem with these technological measures, comprehensive inter-agency collaboration is essential to enhancing the security of waterside and maritime infrastructure. This partnership encompasses local and state government entities, federal departments, private sector stakeholders, and international allies who share common maritime interests. These groups can swiftly and effectively address vulnerabilities through joint exercises and knowledge-sharing initiatives, fostering a resilient infrastructure network. Furthermore, public awareness campaigns ensure that local communities understand and support these security measures. These campaigns can enhance the overall safety framework by educating the public about the importance of security and encouraging vigilance. They can also aid in the early detection of potential threats, thereby contributing to the infrastructure's resilience. These collaborative efforts complement the technological advancements and maturity models, ensuring a holistic approach to protecting New York State's critical maritime assets.

3. Role of Government and Private Sector

The roles of both the government and the private sector in protecting maritime

infrastructure are primarily collaborative due to the expertise of both parties. The government provides legal frameworks, policies, regulations, and compliance requirements that set specific standards [7]. In particular, the government pre-establishes regulatory cybersecurity compliance mandates to ensure that minimum standards are upheld for the basis of security measures [5]. Cybersecurity compliance regulations also provide the foundation for coordination among various stakeholders in maritime security defense, along with private-sector entities' knowledge through technological adaptability and insider methods in securing operational insight.

On the other hand, although public-private partnerships present considerable possibilities to improve infrastructural safety, the peculiarities that they can present regarding commercial regulations can be seen as a relevant disfavor. By creating a platform for sharing resources and expertise, public-private partnerships can develop innovative and efficient approaches for implementing necessary security protocols [5]. However, the conflicting nature of particular interests between the mostly profit-driven private sector in contrast with the altruistic regulatory goals can lead to insidious inefficiencies [7]. As specific research outcomes can be unfavorable for profit-focused organizations, the necessary sharing of sustainable information can often be hindered. The systematic criminal behaviors and other threats that impact the maritime sector's functioning can be addressed more effectively by the various authorities and private companies involved in utilizing innovative countermeasures. However, such possibilities may be limited under the influence of economic interests. Notwithstanding these obstacles, public-private partnerships remain highly beneficial for enhancing the efficiency of risk and resource management, as the need for innovation can be offset against the need for implementation regulation to create a more robust infrastructure [6].

3.1. Threats and Vulnerabilities: Analysis and Limitations

To identify the maritime strategies the State of New York uses, an analysis of the current threats and vulnerabilities faced by the maritime infrastructure and security measures and their limits must be conducted. Most of the strategies currently in use fail to adapt to the continuous shift in threats and vulnerabilities regarding cybersecurity and physical security. Many of these measures are outdated, and cyber threats are no exception, as the constant advancement of technology makes current infrastructure and network systems vulnerable to exploitation by perpetrators [4]. Additionally, the traditional application of physical security measures to protect against threats does not apply well in a networked maritime system and its growing vulnerabilities. Bueger and Liebetrau suggest that the threats present in the environment of a maritime system are fast-changing. Therefore, security measures deployed must also adapt and change to counteract vulnerabilities and threats in the environment and technology [2]. Assessments that cover all logistical and technological aspects must be conducted to develop a more adaptive and

integrated security measure.

On the other hand, alternative methodologies provide various strategies that might increase maritime infrastructure security by better addressing specific security gaps. One of these strategies prioritizes technology integration that allows real-time monitoring and improved rapid response capacities, effectively exceeding the capacity of standard physical security [8]. Instead of contractors, standard common strategies create security gaps, as these approaches utilize advanced cybersecurity protocols that protect maritime operational technologies against security vulnerabilities [4]. In-country capacity building with innovations secured local security development forces support this strategy. In-country capacities with capacity-building innovations supported local security developments and forces secure the adaptability and sustainability of infrastructure; the primary goal of this approach is to comply with solutions against which preventive security threats are emerging [9]. The alternative methodologies hold promise; however, their establishment is subject to determining the success of resource management and compliance with the regulatory environment. The deployment of these methodologies could be subject to arguments aimed at meeting complex needs because of New York's maritime infrastructure. Therefore, an impact assessment is necessary to make comparisons and ensure that the methodologies meet the complexities of the functioning.

The existing security measures are inadequate due to their failure to account for various threats that plague New York's maritime sector. Several measures are inflexible and do not account for emerging technology-based threats. They overlook the latest technologies and do not secure vital information systems from intrusion [4]. An aging infrastructure coupled with uncoordinated and obsolete security measures exposed the maritime industry to physical and cyber threats, thereby compounding security issues [3]. Non-existent and irregular risk assessments also added to inadequacies in security measures as they play a crucial role in establishing security protocols, especially in a rapidly changing and evolving landscape. These inadequacies illustrate the dire need for an adaptable and cohesive security measure to reinforce New York's maritime infrastructure against sophisticated threats from adversaries.

3.2. Evaluating Current Security Measures

To assess the effectiveness of New York's maritime infrastructure security measures, it is essential to identify their strengths and weaknesses in both the physical and cyber domains. Maritime structures predominantly rely on conventional security methods, such as surveillance and patrolling, which are fundamental deterrents against unauthorized access [3]. Nevertheless, these methods prove inadequate in effectively countering sophisticated cyber threats, underscoring a significant deficiency given the increasing digitization of maritime operations [4]. Conversely, technological advancements, such as advanced sensor networks, have been integrated, enhancing real-time threat detection and response capabilities. However,

challenges persist in fully implementing these technologies due to limited resources and infrastructural constraints. Consequently, while existing measures provide a foundational security framework, their effectiveness is compromised by the partial adoption of modern technologies and insufficient integration with evolving maritime cybersecurity requirements [4].

The aforementioned security measures exhibit several significant limitations that impede their overall efficacy. A primary disadvantage is the insufficient incorporation of contemporary technological advancements into traditional security protocols, diminishing their capacity to effectively counter increasingly sophisticated cyber threats [4]. For instance, many systems rely extensively on outdated surveillance technologies that prove inadequate for detecting or responding to complex cyber-attacks, leaving maritime infrastructure particularly susceptible [8]. Furthermore, the limited allocation of resources for ongoing infrastructure upgrades exacerbates these vulnerabilities, as financial constraints hinder the implementation of comprehensive cybersecurity frameworks [3]. Consequently, there exists an urgent necessity to revamp existing security strategies to integrate advanced cyber defensive measures that effectively address these deficiencies and safeguard New York State's maritime infrastructures.

Implementing advanced cybersecurity technologies within the maritime infrastructure of New York State has significantly enhanced threat detection and response capabilities. This enhancement is evident through deploying sophisticated sensor networks and real-time data processing, substantially augmenting situational awareness [4]. Recent evaluations suggest that these technologies have facilitated rapid responses to potential security breaches, reducing the time required to neutralize threats and minimizing disruptions to maritime operations [4]. Furthermore, integrating these systems has improved collaboration across various operational domains, ensuring more coordinated efforts in threat management [8]. While these advancements indicate a positive trend towards more resilient maritime security, ongoing investment in technology and infrastructure remains crucial to address the evolving nature of cyber threats comprehensively.

3.3. Comparative Analysis of Maturity Models: C2M2 vs. SGIMM

Reviewing the strengths and weaknesses of the Cybersecurity Capability Maturity Model (C2M2) and the Smart Grid Information and Management Maturity Model (SGIMM) provides essential implications regarding their use for New York's waterfront and maritime infrastructure. Both models provide specific white banks for evaluating and improving cybersecurity capabilities, but difficulties with their use in practice often occur. The C2M2 model has a clear strength because of its extensive awareness of cybersecurity issues in an industrial environment. However, this model may not be fit for use and adaptation in organizations with limited cybersecurity resources [10]. On the other hand, the SGIMM model is focused on innovative grid systems, and its concern regarding electrical infrastructure can be a challenge in creating its adaptation for maritime systems [11]. However, using a

recommended model depends on organizational resources and their ability to adapt the model's highlights to the unique security context of maritime systems. This emphasizes the need to adapt strategies based on models to be flexible.

With that said, actualizing the aforementioned C2M2 and SGIMM models in New York's maritime framework faces excess adaptability and resource-related issues. The C2M2 presents a very detailed cybersecurity framework. However, it is often the case that it needs many adaptations based on the specific needs of maritime infrastructure, and making such adaptations is usually resource-intensive and time-consuming [10]. Such adaptations are usually needed for the model to be functional in filling any existing gaps because of the maritime framework. However, these allowances cannot be tolerated by organizations with limited cybersecurity budgets in pursuing the previous model, and, ultimately, it hinders the model's scalability in terms of implementation and actualization. On the other hand, the SGIMM's orientation toward electrical grids limits its use with almost all infrastructures and security orientations, as it would need excessive adaptations to be applicable in maritime security [11]. Therefore, it is evident that, alongside the need for gaps to be filled in the line of cybersecurity within New York's maritime frameworks, many resources and even technical know-how would be required to make the two cybersecurity models successful in the city and specific strategies focusing on adaptability and resource-preservation principles must be applied to be able to implement the model extensively in this case.

A comparative review of the implementation scenarios of the Cybersecurity Capability Maturity Model (C2M2) and the Smart Grid Information Management Maturity Model (SGIMM) indicates differences in the outcomes, successes, and challenges associated with these adaptation efforts. A maritime industry entity implementing C2M2 achieved improvement in its cybersecurity preparedness due to the integration of systemic risk management processes into its activities. The model's adoption unlocked the company's potential in threat detection and reaction time increase [10]. This implementation also highlighted critical issues associated with resource limitations, with the company struggling to adapt the model due to the high costs and need for specific expertise. At the same time, SGIMM implementation in the smart grid scenario enables the adaptation of improved data management processes and operational resilience that enhance the efficiency and robustness of the grid infrastructure [11]. In comparison, the SGIMM-based innovative grid concepts reflected in adapting the principles to the maritime domain required extensive adjustments, with the model being focused on the electrical networks and infrastructures. It made the implementation quite challenging and complicated for domain adaptation efforts.

3.4. Implementation Challenges of C2M2 and SGIMM

Several evident challenges have arisen while implementing C2M2 and SGIMM in New York's maritime infrastructure. The first one is the lack of customization, which correlates with the vast number of resources that must be allocated to make the models fit for a maritime environment [10]. It is important to mention that

this challenge comprises a financial aspect and expertise [10]. The second challenge is designing the electrical grid model to adapt to the maritime environment. SGIMM can be implemented in U.S. Navy infrastructure; however, significant changes must be made to the original design [11]. Nevertheless, the complexity of C2M2 often obstructs its implementation in the context of the U.S. Navy and maritime operations, which suffer from a lack of resources. Therefore, it becomes hard to prioritize the model [11]. The rising need for practical strategies to seamlessly integrate scalable and flexible C2M2 and SGIMM models into the naval and maritime security operations is evident [10].

As a result, the elements contributing to the deployment of the Cybersecurity Capability Maturity Model (C2M2) and the Smart Grid Information Management Maturity Model (SGIMM) represent a significant barrier to realizing the models' potential in the real-life context of the maritime sphere. In this regard, while the models are theoretically sound, the level of customization required to produce suitable outcomes for the specific needs of the maritime industry is extensive, which places additional strain on resources and time [10]. In this regard, a campaign with a limited budget often renders the customization process an overwhelming task, thereby considerably compromising the potential of infrastructure in light of the models. Moreover, since SGIMM focuses on smart grid systems, the inherent focus on developing smart grids serves as an additional barrier by requiring further adaptation of the models' principles for the maritime context, which, in return, might decrease effectiveness [11]. Overall, while the C2M2 and SGIMM possess theoretical value, the adaptability showcased in the implementing organization's strategies affects the effectiveness of SDGs, which implies further demand for adaptable strategies to reduce barriers to deployment.

Organizations should develop strategies emphasizing resource optimization and model adaptability to address these implementation challenges. By fostering cross-organizational collaborations, organizations can promote knowledge sharing and consolidate cybersecurity resources, mitigating the financial strain associated with customization efforts [10]. Moreover, investing in modular training programs specifically designed for the unique requirements of maritime cybersecurity can equip personnel with the necessary skills to adapt models such as C2M2 and SGIMM adeptly [10]. Incorporating incremental updates into existing infrastructure ensures that cybersecurity measures remain current without necessitating a complete overhaul, thereby enhancing system resilience [11]. These solutions underscore adaptable and sustainable approaches that effectively address the diverse complexities of New York's maritime infrastructure, consequently improving the overall efficacy of maturity models in practical applications.

4. Case Studies and Practical Examples

Evidence from case studies demonstrates the potential influence of advanced security measures within the maritime sector, particularly through technology integration. A prominent example is the implementation of sophisticated cybersecu-

rity frameworks in maritime operations, which have resulted in a significant decrease in incidents of unauthorized access, thereby indicating a substantial enhancement in overall security [4]. Furthermore, the execution of comprehensive training programs designed to improve the human factor in maritime safety has strengthened both productivity and efficiency, thereby diminishing the probability of accidents [12]. These instances underscore the advantages of incorporating innovative security protocols and ongoing personnel development in maritime environments. A comparative analysis reveals that those strategic investments in technology and training yield measurable improvements in security and operations, emphasizing the importance of adopting a holistic approach to protecting maritime infrastructure.

To further delve into the tangible effectiveness of maturity models such as the Cybersecurity Capability Maturity Model (C2M2) and the Shipping Governance and Integrated Monitoring Model (SGIMM) within New York's maritime infrastructure, let us explore a detailed hypothetical comparison between two similar ports: Port A and Port B. After adopting the C2M2 model, Port A witnessed a substantial improvement in its security measures. Specifically, there was a notable 30% reduction in security incidents and a 20% improvement in the port's response times to potential threats. These enhancements reflect the comprehensive risk assessment and robust security protocols articulated by the C2M2 model, enabling Port A to identify vulnerabilities more effectively and respond swiftly when incidents arise.

In stark contrast, Port B, which did not incorporate these advanced frameworks, only managed a modest 5% reduction in security incidents. This comparison highlights the significant gap in security efficiency between a port utilizing sophisticated maturity models and one that relies on conventional methods. The disparity indicates the leverage gained through C2M2, which systematically enhances the security posture through well-defined processes and continuous improvement. Port A's deployment of the SGIMM protocol also contributed to a 15% decrease in operational costs. This cost reduction was mainly due to integrating advanced threat detection systems, significantly reducing the dependency on continuous manual monitoring. By automating many oversight tasks and streamlining operations, Port A could allocate resources more efficiently, further supporting operational sustainability.

These comparative outcomes clearly illustrate the significant benefits of employing maturity models in maritime security strategies, as seen through improved efficiency and financial savings. Port A's experience suggests that C2M2 and SGIMM offer scalable solutions that can bolster the security framework for waterside and maritime infrastructures. Such results emphasize the strategic advantage of these models in elevating overall port security and operational effectiveness. Examining the successful implementation of advanced security measures within the maritime domain highlights key lessons derived from empirical evidence and practical examples. A maritime organization that employed sophisti-

cated cybersecurity frameworks significantly reduced incidents of unauthorized access, thereby enhancing its overall security posture [4]. This achievement underscores the critical importance of integrating cutting-edge technology into established security protocols, ultimately facilitating improved incident management and prevention. Furthermore, targeted training programs aimed at enhancing the human elements of maritime safety markedly improved productivity and efficiency while minimizing accident risks [12]. By adopting innovative security practices and fostering a culture of continuous development, maritime operations can effectively mitigate vulnerabilities, ensuring resilient and secure infrastructure.

Integrating advanced cybersecurity technologies and comprehensive training programs within New York's maritime infrastructure has demonstrated significant potential in fortifying security measures. These advancements notably improved threat detection and reduced incident response times, establishing a more resilient security posture [4]. Moreover, the decrease in unauthorized access incidents following the implementation of sophisticated security protocols underscores the efficacy of such measures in mitigating vulnerabilities [12]. Successfully enhancing human factors through targeted training programs has also emphasized the personnel's critical role in operational security, reducing the probability of accidents and increasing efficiency [12]. These case examples serve as pertinent takeaways, underscoring the necessity of adopting a holistic approach that concurrently addresses both technological and human dimensions to strengthen maritime infrastructure protection comprehensively.

5. Alternative Strategies for Enhanced Protection

In light of the significant challenges facing maritime security today, it is crucial to investigate innovative strategies designed to protect and fortify New York's waterside infrastructure. One promising avenue is the advancement and application of decentralized security architectures. These systems have the distinct advantage of bolstering resilience against cyber threats particularly prevalent within maritime operations. Through distributed ledger technologies, decentralized systems can enable secure data sharing and ensure the integrity of transaction verification across a wide variety of maritime platforms. This effectively mitigates traditional centralized models' vulnerabilities [8].

Additionally, a complementary strategy involves integrating artificial intelligence and machine learning algorithms into maritime security frameworks. These advanced technologies empower systems to recognize potential threats and respond swiftly and effectively. By utilizing sophisticated pattern recognition and anomaly detection capabilities, AI and machine learning enhance the proactivity of maritime security operations, allowing for the prediction and prevention of possible security breaches before they occur [9]. Moreover, it is essential to cultivate and enhance international collaboration in cybersecurity efforts related to maritime defense. Doing so can significantly strengthen collective defense mech-

anisms, providing a unified and more formidable response to threats that cross multiple jurisdictions and impact several sectors. Such international cooperation ensures that diverse regions and countries work together seamlessly, enabling a more cohesive strategy to counter cyber threats on a global scale [9].

Furthermore, the feasibility of implementing decentralized security architectures within New York's maritime domain is contingent upon their capacity to mitigate inherent vulnerabilities effectively through secure data handling mechanisms. For example, utilizing distributed ledger technologies could revolutionize cybersecurity protocols by ensuring data integrity and augmenting resistance to cyber threats across interconnected maritime systems [8]. These technologies may enhance resilience against attacks, as previous centralization efforts often exposed single points of failure within infrastructures. Moreover, the integration of artificial intelligence algorithms represents another promising approach. Predictive analytics could substantially improve threat anticipation and response efficiency, potentially averting catastrophic events [9]. As international cooperation fortifies collective security measures, these strategies underscore the potential for a global maritime defense framework that transcends jurisdictional boundaries, elevating security to an unprecedented level [9].

6. Critical Assessment and Recommendations

A comprehensive evaluation of New York's maritime security strategies highlights significant shortcomings that considerably diminish their effectiveness. Although some systems provide a foundational level of security, they have not sufficiently evolved to meet the challenges posed by rapidly advancing cyber threats. This stagnation in development leaves crucial infrastructure exposed to highly sophisticated cyberattacks, which could exploit these vulnerabilities disastrously [4]. The study by Kapalidis *et al.* [3] stresses the importance of adopting a vulnerability-centric approach to tackle these inadequacies. This approach focuses on identifying and fortifying the most crucial and valuable assets within the maritime domain, thereby providing a more robust defense against potential security breaches. Such a strategy calls for thoroughly assessing existing vulnerabilities and deploying targeted measures to guard against them.

Moreover, there is a pressing need to incorporate cutting-edge technologies, including artificial intelligence (AI) and machine learning (ML), into the security architecture. These technologies can potentially enhance predictive threat detection capacities, enabling security systems to anticipate and respond to threats faster and more accurately. Employing AI and ML has already demonstrated efficacy in lowering the incidence of security breaches and could prove even more beneficial when fully integrated into maritime operations [9].

Therefore, these focused efforts must be made to enhance the resilience of New York's maritime infrastructure through a responsive, technology-focused security framework to preserve its surrounding maritime environment from new and growing risks. There must also be a proactive approach to investments in work-

force training to understand and operate new technologies and to build international alliances for engaging in shared resources, intelligence, and best practices.

7. Conclusions

Thus, the deep assessment of New York's port maritime critical infrastructure security has revealed several important points, highlighting the necessity to adopt a strategy for improvement. Currently, the maritime security architecture and the cyber security solutions implemented in the region are insufficient to deal with new threats. This is important because integrating advanced technology into existing security solutions is inefficient. Implementing a protection and improvement strategy against revealed inefficiencies will require non-redundant resources. However, advanced Artificial Intelligence implementation and integration into the decentralized security framework must be involved. It is necessary to make the systems more efficient regarding threat payer prediction. More importantly, it will allow the maritime architecture to be more resilient and adaptive when facing threats and challenges.

In addition, international collaboration should be encouraged since maritime security is global, and malicious actors do not acknowledge borders. Sharing intelligence and gaining knowledge from the best practices around the globe will help New York partner with international organizations to march as one against cybersecurity threats. Furthermore, New York should prioritize workforce training as an investment to prepare the personnel with adequate skills to deal with and tackle current threats proficiently. This is a key component of further strengthening maritime security by providing a substantial level of defense against various threats. Implementing these complex methodologies will contribute to securing waterfront properties in New York and ensuring the economic and operational resilience and robustness of such a critical industry. Secure maritime infrastructure ensures a stable and dependable platform for commerce and trade, which would have positive implications for the entire region's economy.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Wakefield, S. (2019) Making Nature into Infrastructure: The Construction of Oysters as a Risk Management Solution in New York City. *Environment and Planning E*: *Nature and Space*, **3**, 761-785. https://doi.org/10.1177/2514848619887461

[2] Bueger, C. and Liebetrau, T. (2023) Critical Maritime Infrastructure Protection: What's the Trouble? *Marine Policy*, **155**, Article ID: 105772. https://doi.org/10.1016/j.marpol.2023.105772

[3] Kapalidis, C., Karamperidis, S., Watson, T. and Koligiannis, G. (2022) A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships. *Journal of Marine Science and Engineering*, **10**, Article 1486. https://doi.org/10.3390/jmse10101486

[4] Kechagias, E.P., Chatzistelios, G., Papadopoulos, G.A. and Apostolou, P. (2022) Digital Transformation of the Maritime Industry: A Cybersecurity Systemic Approach. *International Journal of Critical Infrastructure Protection*, **37**, Article ID: 100526. https://doi.org/10.1016/j.ijcip.2022.100526

[5] Brown, D., Mah, A. and Walker, G. (2021) The Tenacity of Trust in Petrochemical Communities: Reckoning with Risk on the Fawley Waterside (1997-2019). *Environment and Planning E*: *Nature and Space*, **5**, 1207-1229. https://doi.org/10.1177/25148486211045367

[6] Kohout, A., Jain, P. and Dick, W. (2019) Review, Identification and Analysis of Local Impact of Projectile Hazards in the LNG Industry. *Journal of Loss Prevention in the Process Industries*, **57**, 304-319. https://doi.org/10.1016/j.jlp.2018.07.018

[7] Kardon, I.B. and Leutert, W. (2022) Pier Competitor: China's Power Position in Global Ports. *International Security*, **46**, 9-47. https://doi.org/10.1162/isec_a_00433

[8] Ashraf, I., Park, Y., Hur, S., Kim, S.W., Alroobaea, R., Zikria, Y.B., *et al.* (2023) A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, **24**, 2677-2690. https://doi.org/10.1109/tits.2022.3164678

[9] Bueger, C., Edmunds, T. and McCabe, R. (2019) Into the Sea: Capacity-Building Innovations and the Maritime Security Challenge. *Third World Quarterly*, **41**, 228-246. https://doi.org/10.1080/01436597.2019.1660632

[10] Liyanage, L., Arachchilage, N.A.G. and Russello, G. (2024) SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs). arXiv: 2408.16140. https://arxiv.org/abs/2408.16140

[11] Sundararajan, A., Hernandez, A.S. and Sarwat, A.I. (2020) Adapting Big Data Standards, Maturity Models to Smart Grid Distributed Generation: Critical Review. *IET Smart Grid*, **3**, 508-519. https://doi.org/10.1049/iet-stg.2019.0298

[12] Galieriková, A. (2019) The Human Factor and Maritime Safety. *Transportation Research Procedia*, **40**, 1319-1326. https://doi.org/10.1016/j.trpro.2019.07.183