Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P339-cd

Application of Bayesian Networks for real time cyber security crisis classification in passenger ships

Nikolaos P. Ventikos, Alexandros Koimtzoglou, Alexandros Michelis, Angeliki Stouraiti, Vassileios Podimatas

National Technical University of Athens, School of Naval Architecture and Marine Engineering, Division of Ship Design and Maritime Transport, 9 Iroon Politechneiou, Zografou, Athens, 15773, Greece.
E-mail: niven@deslab.ntua.gr, {akoim}{amichelis}{angeliki_stouraiti}{vasileiospodimatas}@mail.ntua.gr

Georgios Potamos

Ministry of Defence, Republic of Cyprus. E-mail: cyberef.pot@army.mil.cy

The shipping industry increasingly relies on Information Technology (IT) and Operational Technology (OT), which undoubtedly improve operations but also jeopardize vessel safety and security. Risks may arise from vulnerabilities in the design, operation, integration, connection and maintenance of these systems, that external or internal threat agents could exploit. This paper presents a cyber-risk assessment model utilizing Bayesian Networks (BN) for real-time crisis classification of cyber security incidents attributed to detected vulnerabilities in the IT and OT systems on passenger ships. The model is part of a crisis classification module under development for the EU-funded project ISOLA, which visions an intelligent security superintendence ecosystem to enhance the existing ship security processes and the protective measures applied onboard passenger ships. ISOLA's services provide functions for continuous surveillance, including cyber security functions. The BN model receives specific IT and OT vulnerability data generated by a specialized ISOLA service and employs Bayesian probabilistic techniques to evaluate any identified vulnerability. The model performs real-time crisis classification of the cyber security-related incident, utilizing a six-level ascending scale for crisis taxonomy and generates relevant warnings to alert the crew and facilitate early detection of potential or actual safety- and security-threatening occurrences.

Keywords: Cyber security, crisis classification, cyber-risk assessment, Bayesian networks, maritime cybersecurity, cyber vulnerability.

1. Introduction

The maritime sector is witnessing a constant growth in digitalization and automation. This trend has resulted in a rapid increase in technological dependency and cyber domain presence across the world fleet. Although digital integration streamlines the ship and ship-to-shore operations, it also exposes the maritime supply chain parties to a higher level of cyber threats; as a matter of fact, the proper operation of the four (4) largest container shipping companies has been compromised by cyber incidents during the last six years (Heering, et al., 2021).

Overall, maritime cyber-attacks exploit existing cyber vulnerabilities to target companies' or ships' systems and data. The implications of these remote threats may include business disruption, financial loss, damage to property, environment and reputation, incident response costs, fines and legal issues (Tam, et al., 2016). The repercussions of cyber-attacks on vessels are far-reaching and complex because of their outcomes that could extend from gaining unauthorized access to commercially sensitive or confidential information (such as passengers and/or cargo data) to supporting other forms of crime (e.g., piracy, theft, fraud, etc.) (BIMCO, 2021). In this regard, shipping companies continue to work on improving the understanding of cyber security challenges and enhancing cyber risk management.

The maritime industry can be proactive in identifying and preventing emerging risks from cyber-attacks by establishing countermeasures

such as implementing cyber security policies and procedures, raising awareness on cyber security by providing appropriate training to crew members, constant monitoring and testing of systems, applying network segmentation and isolation of critical systems, and, conducting cyber-risk assessments on a regular basis.

This paper describes a smart real-time risk assessment and crisis classification tool utilizing a Bayesian Network (BN) for the evaluation of cyber security incidents related to the identification of cyber vulnerabilities in the ship's IT and OT systems and networks. The tool is under development for the EU-funded research project ISOLA. The main objective of the project is the creation, integration, demonstration, and validation of a systematic and automated ship security ecosystem that will enhance the existing ship security framework and protective measures by introducing innovative technologies for real-time sensing, data collection, monitoring, data fusion and analysis, alarming and reporting during security incidents. Among other functions, the ISOLA ecosystem aims to support the situational awareness of the crew members (i.e., Master, Ship Security Officer (SSO), and crew members contributing to security on board) by implementing continuous security monitoring and providing early, external and internal, security threat detection/warning, and facilitate their decision-making process during time-sensitive and stressful circumstances.

Section 2 presents concisely various studies that utilized BNs to model cyber security incidents. In Section 3, the methodology applied for the development of the proposed BN model, is briefly described. Section 4 presents the key parameters identified as critical for cyber security incidents and included in the model, followed by the analysis of the BN model in Section 5 through the description of the main factors and nodes. Then, indicative case studies are presented as a means of validating the BN's functionality. The paper concludes with insights regarding the proposed cyber security BN model as well as the future research that remains to be performed towards the finalization of the model.

2. Background

In an effort to ensure the safety and security of the vessels, passengers and crew members, guidelines and practices have been published to provide a structured framework for assessing and managing cyber risks in the maritime industry (IMO, 2022; Barrett, 2018; BIMCO, 2021; IACS, 2022; DNV-GL, 2016). Various studies have examined the use of BN models as a key tool for the security administration implemented in an enterprise network. BN techniques have been integrated into intrusion detection systems (Bringas, 2007), (Kruegel, et al., 2003) (Valdes & Skinner, 2000) or used as part of a holistic analysis framework that uses the outputs from intrusion detectors (Xie, et al., 2010). Some studies have centered on the pre-deployment planning phase, relying on the security metrics generated by the BN models to reflect the inherent risks in a network (Frigault & Wang, 2008), (Frigault, et al., 2008). While another study has formulated a BN model to address the problem of real-time situation awareness (Xie, et al., 2010). In all these studies, BN models have proven to be an effective approach to network security management.

Quantifying the relevant security risk and appropriately normalizing it afterwards will enhance the vigilance and situational awareness of the crew members associated with critical cyber security threats. To that end, the establishment of a suitable taxonomy of the crisis level and a corresponding classification scheme are considered important. The crisis classification can also be linked directly to a relevant action code and appropriate security measures developed to protect the assets, such as the ship, persons on board and the cargo. Such an approach enables to clearly illustrate the estimated risk level, thus supporting effective decision-making and response to cyber security threats. The criticality of a security incident or threat can be determined based on the level of the associated risk, which can be measured on an ascending scale. There are several crisis taxonomy systems available that assess the level of security risk and adjust the corresponding security measures accordingly. For example, the International Ship and Port Facility Security (ISPS) Code employs a three-level scale to qualify the degree of risk that a security incident will be attempted or will occur, while the Cyber security and Infrastructure Security Agency (CISA) uses a six-level scale to evaluate the cyber security incident risk on a national level. It

is noted that a BN model for crisis classification during piracy or armed robbery incidents on passenger ships developed for the ISOLA project employs a six-level crisis classification scheme (Ventikos, et al., 2022).

3. Methodology

Bayesian network techniques have been applied to intrusion detection systems. The current BN application relies on the knowledge generated by the threat recognition sensor system and provides crisis classification for the detected security events. Although the construction of a BN model for practical security analysis is not trivial (e.g., lack of data in the cyber security domain and overreliance on experts may produce subjective results) BN modelling is still considered a powerful tool that applies to real-time security analysis (Peng Xie, et al., 2010). Fig. *1* presents a functional diagram of the methodology utilized to develop the model.

In general, the first phase of the methodology included the analysis of the various aspects of cyber security management. The key parameters affecting the level of cyber-related risks (e.g. types of software vulnerabilities, vulnerability severity) were identified through a pragmatic approach considering the available cyber security incident datasets (e.g., National Vulnerability Database (NIST)) and literature review.

The second phase was dedicated to the development of the BN model, whereas the primary variables were selected as parent nodes while the secondary as child nodes. The probabilistic relationships between the nodes were established and each node was associated with a CPT. The computed CPTs obtained discrete likelihood values related to individual conditions. The values were assigned in accordance with expert support during interviews.

In the third phase, the initial version of the model was validated by testing several use-case scenarios. The use-case scenarios were obtained by interviewing experts, who derived from the maritime security sector and are employed in the operational and IT domain. The experts supported the scenario-based validation by suggesting specific cyber security case studies corresponding to known crisis levels from the beginning. For each scenario referring to the identification of a vulnerability in a system/network for a given ship condition, an assessment of the potential cyber threat and incident classification was performed and compared to the expert elicitation. To conclude the last phase, the model was consolidated according to the comments provided during the validation.

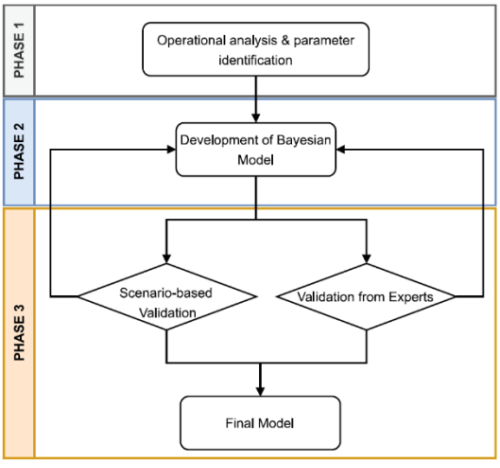

Fig. 1. Schematic representation of the methodology applied for the development of the BN model.

4. Identification of Parameters

A BN model has been developed for the crisis classification of cyber security incidents related to cyber vulnerabilities onboard passenger ships. The model integrates several parameters, including the type and the severity of the identified cyber vulnerability, the system or network on which the vulnerability has been identified, as well as the condition of the ship during the vulnerability assessment process. It should be noted that BN in risk assessment provides a flexible framework and scalability in modelling, which can address parameters by adding nodes that can integrate both quantitative and qualitative datasets and incorporate individual-level or aggregate data, expert opinion, and evidence synthesized from the literature (Kabir & Papadopoulos, 2019).

As a pre-requisite action for the model's activation, a vulnerability scanner provides automated input to the system, containing the results related to the existing weaknesses in the ship's IT and OT infrastructure. Depending on

the capabilities of the identification process, vulnerabilities could vary in accordance with the type of the scanned system/network. Recent studies (Meland, et al., 2021; Akpan, et al., 2022), as well as industry guidance for cyber risk management (BIMCO, 2021), provide insight into the common vulnerabilities onboard ships. The developed model categorizes the possible vulnerabilities by types, including network, endpoint, and application/data, based on a layered cyber security framework (McCallam, 2012). This approach provides flexibility to use the model in conjunction with various vulnerability scanners. Depending on the identification capabilities of the utilized scanner, the model is adaptable to different vulnerabilities assigned to the appropriate types.

Another important parameter is the time required for the scanning process. Depending on the size and complexity of the networks, the duration for the identification may vary. A passenger ship has extensive public and enterprise networks with various systems and characteristics, different from other ship types. With digitalization and automation increasing in the maritime industry, the passenger ship has evolved into a modern multidomain platform (Laso, et al., 2022), combining both IT and OT systems (Kessler, et al., 2018). For this study, the ship's technology is a combination of these systems. The model can assess in real-time the threat and crisis classification level based on the vulnerabilities data extracted from the scanner and entered as input into the model.

The developed model also takes into consideration the condition of the ship. During the vulnerability scanning process, the ship has a specific navigational status (underway, docked, etc.), and may encounter static and dynamic obstacles in the area. In addition, a critical ship operation, such as preparing for departure, may be in progress or about to commence. An identified vulnerability, if exploited by a threat agent, could have an adverse impact on the ship's condition leading to, for example, the loss of propulsion during the docking process or a delay in the departure operation.

5. Development of the Bayesian Model

A BN is a probabilistic model that utilizes Bayes' theorem to capture knowledge about an uncertain domain. The structure of a BN is represented by a directed acyclic graph containing nodes and arcs, where nodes correspond to variables and arcs illustrate the dependencies among them. The dependencies are defined by assigning marginal and conditional probabilities to the nodes. The joint probability of a set of random variables $X = \{X_1, X_2, ..., X_n\}$ can be calculated as the multiplication of probabilities of the parent nodes, denoted as $P(X) = P(X_1, X_2, ..., X_n)$, as shown in Eq.(1) (Pearl, et al., 2003):

$$P(x) = \prod_{i=1}^{n} P\left(X_i | pa(X_i)\right) \quad (1)$$

The presented BN model comprises 5 parent and 3 child nodes, as shown in . The parent nodes represent the model's inputs. The child nodes are derived from the parent nodes, and their interaction is determined by appropriate CPTs. The required data is dynamically fed into the parent nodes through the ISOLA system. Subsequently, a real-time threat assessment is performed, and the probability of the potential cyber threat is calculated on the model's final node. The nodes and their states were evaluated by interviewing five (5) maritime professionals (company security officer, Master, cyber security officer, maritime security trainer, and cyber security consultant) with diverse backgrounds covering both shipboard operations and cyber security. The probability assignment for the states was determined based on the average value of the experts' suggestions, which reached a consensus in general. The nodes of the BN model are described below.

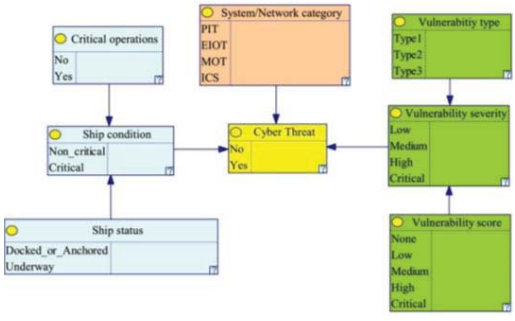

Fig. 2. The developed BN model.

5.1. Ship condition

The level of threat for the safety and security of a ship derived from the identification of one or more cyber security vulnerabilities is significantly influenced by the ship condition. The most important factors of ship condition considered in the BN model are the ship status and the criticality of the ongoing operation.

5.1.1. Ship status

The navigational activity of the ship can be endangered by an occurring cyber security event. Depending on the incident, the level of cyber risk can be directly related to the ship status. For example, a cyber-attack may pose a higher risk to the safety of a sailing vessel compared to a vessel moored at a pier. In this regard, the ship status node enables the correlation between the navigational activity of the ship, which can be provided automatically by e.g. the ship's Automatic Identification System (AIS), and the possibility of the detected vulnerability being exploited to jeopardize the safety of the vessel. The ship status node enables the model to assign a limited value when the ship is docked or anchored, and a high value when the ship is underway.

5.1.2. Critical operations

The crew onboard continuously assess operational risks and apply adequate procedures, as well as risk control measures to safeguard routine and critical shipboard operations for the safety and security of the vessel, including actions that ensure the fully operation of the necessary systems (navigational, surveillance, and industrial ones). If a cyber vulnerability is detected in a critical system for example during docking operations in a port or while the ship is sailing in close proximity with other vessels or during the departure preparation operations, the level of awareness regarding the potential cyber threat should be heightened, as a potential cyber incident could put at risk the safety of the vessel, the persons onboard as well as the protection of the environment, by causing significant damage and losses. Taking into consideration all the above factors, the node 'Critical operations' is examining the cyber security incident in conjunction with the following circumstances:

- The ship has a Closest Point of Approach (CPA) of less than 1 nautical mile (nm) with another ship, obstacle, navigational warning item, or coast.
- The crew performs pre-arrival checks of systems before the ship reaches a port or during the anchorage preparation procedures.
- The crew performs pre-departure checks of systems while the ship is docked in the port, during the departure preparation operations.

5.2. *System/Network category*

The various system types are organized in the model by network categories, according to their functionality. In the case of passenger ships, it is crucial to segregate different networks for safety and security reasons. The onboard networks generally include a large public network (Public IT - PIT) for communication and entertainment, an enterprise network (Enterprise IT/OT/IOT-EIOT) that supports crew and hotel personnel, a maritime OT (MOT) network that comprises navigational, communication and maritime surveillance sensors/actuators linked to the bridge, and an Industrial Control Systems (ICS) network that incorporates ship industrial equipment, sensors/actuators and interfaces with human-machine interfaces and/or management systems. Fig. 3 illustrates the classification of systems based on their respective network types that was utilized in the model. However, depending on the ship-specific IT/OT infrastructure and the vulnerability scanner's coverage, additional categories (i.e., states) can be included in the node.

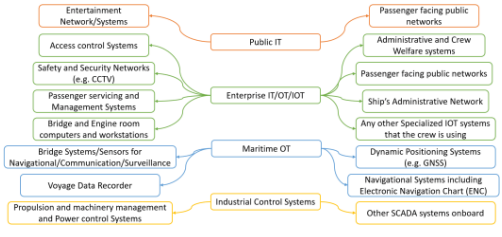

Fig. 3. The classification of ship systems into network categories.

5.3. *Vulnerability severity*

The vulnerability severity indicates the criticality of the identified vulnerability and is determined by the type of vulnerability and its relevant score, which is a numerical representation of the significance of the finding.

5.3.1. *Vulnerability type*

The ISOLA project employs the Dynamic Vulnerability Assessment and Testing Service (DVATS), a digital tool performing vulnerability scanning of the ship's IT and OT assets and prioritization of the determined weaknesses. Any identified vulnerability during the assessment process becomes an input for the BN model. To improve the efficiency of the model, the identified vulnerabilities are classified into three main vulnerability types based on the concept of a layered cyber security framework (McCallam, 2012) as follows:

- Type 1: Network security (New Asset Identified, Open and exposed network identified).
- Type 2: Endpoint security (Unpatched Operating System (OS)).
- Type 3: Application Security (Weak cipher/No encryption).

This node is scalable in terms of the vulnerability types that can be introduced as the node's states.

5.3.2 Vulnerability score

The DVATS assigns a vulnerability score (i.e., DVSS score) to the identified vulnerability. The score is a severity measure for the finding and enables the comparison between vulnerabilities and their prioritization in terms of remedial actions. The higher the score, the higher the associated cyber security risk is. In this paper, the DVSS score follows the CVSS qualitative rating (Singh & Joshi, 2016) in Table 1.

Table 1. Qualitative severity rating scale based on DVSS Score.

DVSS Score	Qualitative Rating
0.0	None
0.1 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 8.9	High
9.0 – 10.0	Critical

5.4. *Cyber threat*

The BN model produces a probability estimation regarding the presence or absence of a cyber threat. A six-level scale is employed to indicate the severity of the cyber security incident, with the Crisis Level (CL) aligned with the threat probability as presented in Table 2.

Table 2. Threat and CL correlation.

Threat	CL	Indicative code of action
0-20%	1 Very low	Situation: Calm/predictable Concern level: Routine Operations: Normal Measures: Current measures apply
20-40%	2 Low	Situation: Normally calm/predictable Concern level: Enhanced Operations: Normal Measures: Enhanced as required
40-60%	3 Medium	Situation: Dangerous/predictable Concern level: Significant Operations: Security Management Team and Master's decision Measures: Significant measures implemented
60-80%	4 High	Situation: Dangerous/unpredictable Concern level: Considerable Operations: Security Management Team and Master's decision Measures: Urgent, very specific and robust measures implemented
80-90%	5 Very high	Situation: Extremely dangerous/unpredictable Concern level: Extreme Operations: Security Management Team and Master's decision Measures: Immediate extreme measures implemented
90-100%	6 Extreme	Situation: Extremely dangerous/unpredictable Concern level: Extreme Operations: Security Management Team and Master's decision Measures: Exceptional and immediate extreme measures implemented.

Additionally, for every CL, a generic action code is proposed, with the relevant measures adjusted according to the crisis level. Consequently, a correlation is established between the escalation of the crisis level and the corresponding elevation of the level of vigilance and preventing actions, which can serve as a basis for a Decision Support System (DSS).

6. Indicative Case Studies

This section presents the application of the developed BN model to assess the CL of a few indicative case studies. The objective is to demonstrate the functionality and sensitivity of the model under different scenarios. It should be noted that during the interviewing sessions, the experts' evaluation relied on their conceptual and empirical capability to determine the specific scenario's crisis level a priori. Therefore, they were able to assess and validate the credibility of the outcomes derived from the BN model.

6.1. *Case study 1*

The passenger ship is docked in a port. During a routine scanning of the ship's IT and OT systems and networks, DVATS identifies a Type 2 vulnerability, with a high DVSS score in a ship's administrative network, i.e., an Enterprise IT/OT/IOT category network. Based on these data, the output of the BN model is a cyber threat probability of 51%, which classifies the scenario as a Crisis Level 3 incident.

6.2 *Case study 2*

The ship sails in the open sea. Whilst DVATS executes a routine scan, it indicates a Type 1 vulnerability, with a Critical vulnerability score, in an integrated navigation bridge system (Maritime OT system). The BN model calculates a threat probability of 78%, corresponding to a Crisis Level 4 cyber incident. In case the ship was performing critical maneuvers e.g., navigating inside a straight, for the same vulnerability identified, the resulting cyber threat probability is 83%, which escalates the Crisis Level to 5.

6.3 *Case study 3*

While the vessel is performing critical maneuvering in an area with dense marine traffic, DVATS identifies a Type 1 vulnerability in an Industrial Control System (e.g., a main engine control system). The tool evaluates the identified vulnerability as Critical i.e., it assigns to it a DVSS score higher than 9. Using these inputs, the BN model assesses the incident as a threat with a 98% probability, which corresponds to Crisis Level 6.

7. Conclusions

This paper presents a Bayesian network model that assesses in real time the potential threat level linked to the existence of vulnerabilities in a ship's IT and OT systems and networks and performs a situation evaluation in the form of crisis classification of the incident. The developed tool utilizes a systematic and flexible methodology that combines BN theory and crisis classification to improve cyber security management onboard. The output of the model provides early warning and improves situational awareness regarding identified cyber security weaknesses that can be exploited by a threat agent. Thus, it promotes the timely application of measures to reduce the risk of exposure to a successful cyber-attack. In this context, the model's contribution can be expanded if it is combined with an appropriate decision support tool (as in the case of the ISOLA project), which will recommend preventive actions to the Master and the cyber security management team based on the crisis classification.

The future steps involve integrating the BN model into the ISOLA ecosystem and validating it onboard a passenger ship in real-case scenarios. Expanding the model to include additional parameters is also in progress. It is worth noting that the presented model is part of an overarching crisis classification module that encompasses multiple security threats. Thus, comparable BN models are under development to model other threats, such as illegal boarding and trespassing, or have already been developed, like a model for piracy and armed robbery attacks (Ventikos, et al., 2022).

Acknowledgement

This work was supported by the Project "ISOLA: Innovative & Integrated Security System on Board Covering the Life Cycle of a Passenger Ships Voyage", which has received funding from the European Union's Horizon 2020 research and innovation programme, EU.3.7. - Secure societies, Protecting freedom and security of Europe and its

citizens under the Topic SU-BES02-2018-2019-2020 - Technologies to enhance border and external security (Grant Agreement number 883302).

References

Akpan, Frank, Gueltoum Bendiab, Stavros Shiaeles, and Michalis Michaloliakos. (2022). "Cybersecurity Challenges in the Maritime Sector." Network 2 (1): 123-138.

Barrett, Matthew. (2018). "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1." NIST Cybersecurity Framework.

BIMCO. (2021). The Guidelines on Cyber Security Onboard Ships. BIMCO.

Bringas, Pablo Garcia. (2007). "Intensive use of Bayesian belief networks for the unified, flexible and adaptable analysis of misuses and anomalies in network intrusion detection and prevention systems." 18th International Workshop on Database and Expert Systems Applications (DEXA 2007). IEEE.

DNV-GL. (2016). "Cyber security resilience management for ships and mobile offshore units in operation." DNVGL-RP-0496.

Frigault, Marcel, and Lingyu Wang. (2008). "Measuring network security using bayesian network-based attack graphs." 32nd Annual IEEE Conference on International Computer Software and Applications. IEEE.

Frigault, Marcel, Lingyu Wang, Anoop Singhal, and Sushil Jajodia. (2008). "Measuring network security using dynamic bayesian network." 4th ACM workshop on Quality of Protection.

Heering, D., O. M. Maennel, and A. N. Venables. (2021). "Shortcomings in cybersecurity education for seafarers." In Maritime Technology and Engineering 5 Volume 1, pp. 49-61. CRC Press.

Hossain, Niamat Ullah Ibne, Farjana Nur, Seyedmohsen Hosseini, Raed Jaradat, Mohammad Marufuzzaman, and Stephen M. Puryear. (2019). "A Bayesian network based approach for modeling and assessing resilience: a case study of a full service deep water port." Reliability Engineering & System Safety, pp. 378-396.

IACS. (2022). "UR E26 Cyber resilience of ships."

IMO. (2022). "Guidelines on maritime cyber risk management." MSC-FAL.1/Circ.3/Rev.2.

Kabir, Sohag, and Yiannis Papadopoulos. (2019). "Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: A review." Safety Science, pp. 154-175.

Kessler, G., J. Craiger, and J. Haass. (2018). "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System." TransNav: International Journal on Marine Navigation and Safety of Sea Transportation 12: 429-437.

Kruegel, C., D. Mutz, W. Robertson, and F. Valeur. (2003). "Bayesian event classification for intrusion detection." 19th Annual Computer Security Applications Conference, 2003. IEEE.

Laso, Pedro Merino, Loic Salmon, Maya Bozhilova, Ivan Ivanov, Nikolai Stoianov, Grigor Velev, Christophe Claramunt, and Yantsislav Yanakiev. (2022). ISOLA: An Innovative Approach to Cyber Threat Detection in Cruise Shipping. Vol. 255, in Developments and Advances in Defense and Security, 71-81. Singapore: Springer Singapore.

McCallam, D. (2012). "An analysis of cyber reference architectures." Presented at NATO 2012 Workshop with Industry on Cybersecurity Capabilities.

Meland, P.h, K. Bernsmed, E. Wille, Ø.j. Rødseth, and D.a Nesheim. (2021). "A Retrospective Analysis of Maritime Cyber Security Incidents." TransNav, International Journal on Marine Navigation and Safety od Sea Transportation 15 (3): 519-530.

NIST. National Vulnerability Database (NVD). https://www.nist.gov/programs-projects/national-vulnerability-database-nvd.

Park, Changki, Christos Kontovas, Zaili Yang, and Chia-Hsun Chang. (2023). "A BN driven FMEA approach to assess maritime cybersecurity risks." Ocean & Coastal Management.

Pearl, Judea, Stuart Russell, and Michael A. Arbib. (2003). "Bayesian networks." In The Handbook of Brain Theory and Neural Networks: Second Edition, pp. 157-160. Cambridge: MIT Press.

Peng Xie, Jason H Li, Xinming Ou, Peng Liu, and Renato Levy. (2010). "Using Bayesian networks for cyber security analysis." 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN). Chicago: IEEE. pp. 211-220.

Singh, U.K., and C. Joshi. (2016). "Quantitative Security Risk Evaluation using CVSS." e World Congress on Engineering and Computer Science. San Francisco. pp. 26-33.

Tam, Kimberly, Kevin Jones, and Maria Papadaki. (2016). "Threats and Impacts in Maritime Cyber Security." Engineering & Technology Reference.

Valdes, Alfonso, and Keith Skinner. 2000. "Adaptive, model-based monitoring for cyber attack detection." Third International Workshop, RAID.

Ventikos, Nikolaos P., Alexandros Koimtzoglou, Alexandros Michelis, Alexandros Rammos, Ioannis Kopsacheilis, and I. Androulakis. (2022). "Utilising Bayesian networks for the crisis classification during piracy or armed robbery incidents on passenger ships." In Sustainable Development and Innovations in Marine Technologies. CRC Press.

Xie, Peng, Jason H Li, Xinming Ou, Peng Liu, and Renato Levy. 2010. "Using Bayesian Networks for Cyber Security Analysis." IEEE/IFIP International Conference on Dependable Systems & Networks (DSN). IEEE. pp. 211-220.