Influence Diagrams in Cyber Security: Conceptualization and Potential Applications

Sabarathinam Chockalingam[1] and Clara Maathuis[2]
[1]Institute for Energy Technology, Halden, Norway
[2]Open University of the Netherlands, Heerlen, The Netherlands

sabarathinam.chockalingam@ife.no
clara.maathuis@ou.nl

Abstract. Over the last years, cyber-attacks are increasing in organizations especially due to the use of emerging technologies and transformation in terms of how we work. Informed decision-making in cyber security is critical to prevent, detect, respond, and recover from cyber-attacks effectively and efficiently. In cyber security, Decision Support System (DSS) plays a crucial role especially in supporting security analysts, managers, and operators in making informed decisions. Artificial Intelligence (AI)-based techniques like Bayesian Networks, Decision Trees are used as an underlying approach in such DSSs. Furthermore, Influence Diagrams (IDs) possess the capability to support informed decision-making based on its existing applications in other domains like medical. However, the complete capability and potential of IDs are not utilised in cyber security especially in terms of its explainable nature for different stakeholders and existing applications in other domains. Therefore, this research tackles the following research question: "What are potential applications of Influence Diagrams (IDs) in cyber security?". We identified applications of IDs in different domains and then translated it to design potential applications for cyber security issues. In the future, this will help both researchers and practitioners to develop and implement IDs for cyber security-related problems, which in turn will enhance decision-making especially due to its explainable nature for different stakeholders.

Keywords: Cyber security, Decision making, Incident response, Influence diagrams, Graphical model.

1. Introduction

Using technologies such as Artificial Intelligence (AI)/Machine Learning (ML), Internet of Things (IoTs), robotics redefines and enhances the way in which we work and live (Olan *et al.*, 2022). However, such technologies present numerous opportunities and at the same time some threats to both organizations and individuals. One such threat is the cyber threat which refers to any situation or event that may have the potential to negatively affect an organization's operations, assets, or people by impacting Confidentiality, Integrity, and Availability (CIA) of an information system. Notably, due to the increased usage of technologies, there has been a rise in cyber-attacks in both the Information Technology (IT) and Operational Technology (OT) environment (Lallie *et al.*, 2021; Prajapati and Singh, 2022). Successful cyber-attacks, which are not addressed effectively in a timely manner, can have dire consequences ranging from financial impact to reputational loss (Leroy, 2022). Therefore, it is extremely important to be aware of such threats and know how to deal with it effectively through relevant prevention, detection, response, and/or recovery measures that in turn would also lead to responsible and sustainable use of technologies in organizations.

To that end, Decision Support System (DSS) in cyber security help security analysts, managers, and operators to make informed decisions especially on risk mitigation measures/response strategies (Rees *et al.*, 2011; Buzdugan, 2020). For instance, Chockalingam et al. developed a decision support that help operators in distinguishing attacks and technical failures for the *"incorrect sensor measurements*" problem in floodgates (Chockalingam *et al.*, 2021). In such DSSs, AI/ML approaches like Bayesian Networks (BNs), decision trees, neural networks are used an underlying approach (Li, 2018; Chockalingam *et al.*, 2021). Importantly, the field of cyber security continued to evolve during recent years especially due to the existing capabilities as well as recent developments within the field of AI. This mainly support the application of its approaches for building intelligent solutions in cyber security that would be able to predict data breaches (Wilde, 2016), detect cyber-attacks (Adepu and Mathur, 2016), respond to cyber-attacks (Chockalingam, 2021), and/or recover from cyber-attacks (Manasa and Kumar, 2022) effectively and efficiently.

However, although a vast plethora of AI/ML-based techniques dealing and capturing uncertainty are used in different cyber security applications, the use of Influence Diagrams (IDs) in this domain, is scarce. An ID is a simple visual representation of a decision-making process (Howard and Matheson, 2005) and also a generalization of BNs which consists of both qualitative and quantitative components. The essential foundation to On the other hand, IDs possess the capability to be useful for cyber security applications especially based on their existing applications in other domains like agriculture (Jensen and Jensen, 2013), medical (Owens, Shachter

and Nease Jr, 1997; Baio *et al.*, 2006), safety (Matviykiv, 2013; Wang, Huang and Zhang, 2013) in addition to its explainable nature that aid effective visualization of complex decision problems to different stakeholders (Weflen, MacKenzie and Rivero, 2022), which is an essential aspect for cyber security decision making. Therefore, this paper aims to fill this gap by addressing the following research question (RQ): "What are potential applications of Influence Diagrams (IDs) in cyber security?". The research objectives (ROs) are:

- **RO1.** To identify existing applications of IDs in different domains.
- **RO2.** To translate the identified applications to design potential applications of IDs for cyber security problems.

The rest of this paper is structured as follows: Section 2 provides an essential foundation to IDs followed by our research methodology in Section 4. Section 5 describes identified applications of IDs in different domains followed by the potential applications of IDs in cyber security. Finally, Section 6 highlights conclusions and future work directions.

2. Background – Influence Diagrams: Key Components and An Example

Together with decision trees, IDs are an effective visual representation for decision models. The same underlying mathematical concept and processes are graphically represented differently in IDs and decision trees (Owens, Shachter and Nease Jr, 1997). IDs are an extension to BNs with two additional type of nodes including decision and utility in addition to uncertainty nodes (or chance) nodes (Åström *et al.*, 2014). ID consists of three different types of nodes which include: (i) uncertainty (or chance) nodes represented as oval, (ii) decision nodes as rectangle, (iii) utility nodes represented as diamond. Decision nodes associate with actions that the decision maker has direct influence over, whereas chance nodes reflect events that are not under the decision maker's control (Lacave, Luque and Diez, 2007). Utility nodes represent the preferences of the decision maker. Utility nodes cannot be parents of chance or decision nodes.

An example ID is shown in Figure 1. The uncertainty nodes in the shown example are: *"Cyber Security Risk Level"*, and *"Cyber Security Awareness".* The decision node in the shown example is *"Cyber Security Training Needed or Not"* and the utility node is *"Value"*. Furthermore, in this example ID, we provided example values to the Conditional Probabilities Tables (CPTs) of the uncertainty nodes and example utilities for different policies in the utility node. This ID can be used by managers to determine an expected utility when they decide to provide cyber security training or not. For instance, in this example, the expected utility when they make a decision to provide cyber security training is 4800, whereas the expected utility when they make a decision to not provide cyber security training is 300. In this case, they can make a choice to provide cyber security training, which provides highest expected utility compared to the other choice and therefore optimal.

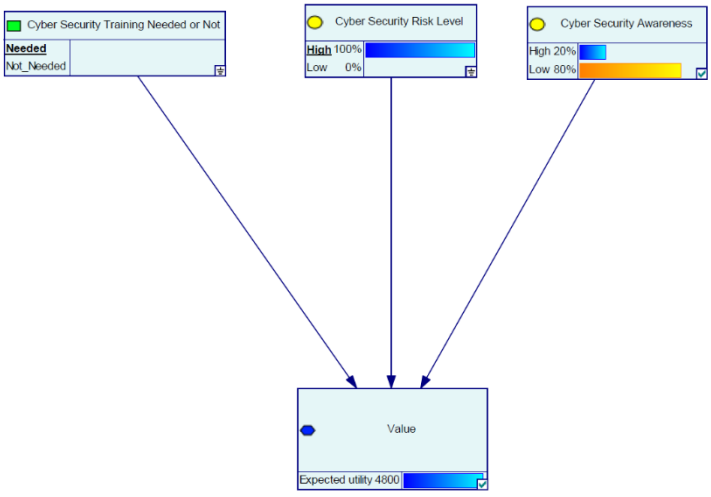

Figure 1. An Influence Diagram – Example

3. Research Methodology

The aim of this research is to provide awareness and understanding on the existing use of IDs in different application domains and potential applications of IDs in the cyber security domain. To that end, the following

RQ is formulated in this study: "What are potential applications of Influence Diagrams (IDs) in cyber security?". To address this RQ, an extensive literature review is conducted to build conceptual designs as a socio-technical artefact using the Design Science Research methodology (Peffers *et al.*, 2007; Peffers, Tuunanen and Niehaves, 2018). Accordingly, the following research phases are considered in this process.

In the first phase (i.e., problem definition and aim), the problem that should be investigated is analyzed in its corresponding context and the objective of this research is defined. Correspondingly, while a vast set of AI applications in the cyber security domain exists and their effectiveness was proved in tackling both knowledge and data characterized issues and challenges, still issues remain, old ones come back to live through new perspectives, and (un)expected new ones are born. However, a technique that is barely known and used in the cyber security domain are IDs (Li, 2018; Zhang *et al.*, 2022). To be able to investigate their potential applications in cyber security, an extensive literature review is conducted using keywords such as *"cyber security"*, *"influence diagrams"*, and *"application"* that are coupled in different combinations as queries used in scientific databases such as ACM, IEEE, Scopus, and Web of Science. Hence, an in-depth understanding of what IDs mean, how they can be characterized, and how they function is gathered followed by a series of various corresponding applications in different fields including agriculture, medical, military, and safety.

In the second phase (i.e., solution design), underlying structure with diverse types of nodes and model purpose are gathered from existing applications to build the artefact that this paper proposes, i.e., conceptual designs that captures the purpose, characteristics, and architecture of IDs for potential cyber security applications. In the third phase (i.e., evaluation), conceptual designs proposed is typically evaluated through instantiation/demonstration based on building a series in different cyber security applications such as cyber risk management. However, this phase is out of the scope of this paper. In the final phase (i.e., communication), the results in the context of this research in addition to possible future research directions are communicated by means of this publication and future presentations.

4. Existing Applications of Influence Diagrams

This section describes applications of IDs in different domains including agriculture, medical, military and safety.

Jensen et al. presented a Decision Support System (DSS) prototype based on IDs for the management of fungal disease (mildew) in winter wheat (Jensen and Jensen, 2013). In this prototype, there are four different variable types: (i) static information, (ii) dynamic information, (iii) decisions, and (iv) utilities. Static information includes variables like soil type, plant density, winter wheat variety, whereas dynamic information includes variables like weather, disease incidence, remaining time to harvest. Furthermore, decisions include dose of treatment variable and utilities include value of yield, cost of treatment, and value of disease induced yield loss. This prototype can help to determine the optimal decision on the dose of treatment considering evidence from other variables.

Baio et al. developed a decision model based on IDs for performing cost-effective analysis of influenza vaccination in the Italian elderly population (Baio *et al.*, 2006). In this decision model, strategy is the decision node which has the following states: do not vaccine, standard vaccine, and innovative vaccine. Furthermore, the decision node is influenced by other variables that are in the developed decision model like reduction in events generated by standard vaccine, reduction in events generated by innovative vaccine, occurrence rate of events, costs of GP visits, costs of standard vaccine, and costs of innovative vaccine. This decision model can help to determine the cost-effective decision on the influenza vaccination considering the evidence from other variables in the model. Furthermore, Owens et al. developed an ID for a medical decision problem on whether to perform PCR and whether to treat (Owens, Shachter and Nease Jr, 1997). In this ID, there are five different variables: (i) obtain PCR?, (ii) treat?, (ii) PCR result, (iv) HIV status, and (v) Quality Adjusted Life Expectancy (QALE). The first two variables correspond to decision nodes, whereas PCR result and HIV status correspond to deterministic node. Finally, variable is the utility/value node.

Wang et al. proposed a novel method based on IDs for fault troubleshooting of electromechanical products (Wang, Huang and Zhang, 2013). The ID for automotive engine fault troubleshooting proposed includes three different types of nodes: (i) uncertainty nodes, (ii) decision nodes, and (iii) utility nodes. Uncertainty nodes are fault causes of automotive engine failure which include variables like fire fault (ignition timing error, ignition signal cutting off, ignition coil failure). Decision nodes has the states repair and not repair. Utility nodes mainly provide information on the cost of the decision from the diagnostic engineers' perspective. This ID supports diagnostic engineers to repair a faulty component with highest expected utility to repair. Matviykiv et al. developed a DSS based on IDs for shock and vibration mitigation while drilling (Matviykiv, 2013). The developed

DSS based on ID consists of three diverse types of nodes: (i) uncertainty nodes, (ii) decision node, and (iii) utility nodes. Uncertainty nodes include variables such as actual life of a downhole tool, actual vibration severity, expected tool life at the end of the run after mitigation, expected vibration severity after mitigation. Decision node is whether to mitigate or not which has the following states: mitigate, ignore. Finally, there are two different utility nodes in the developed DSS based on IDs: utility function which reflects the level of tool preservation, utility function which reflects the negative effect of ineffective decision. Jeet et al. developed an approach based on ID for estimating staff training in software industry (Jeet *et al.*, 2009). The developed ID consists of four chance nodes: (i) newly appointed staff, (ii) lack of experience with project environment, (iii) lack of experience with project software, and (iv) staff not well versed with quality standards. In addition, the decision node is the staff training with the states "Yes" and "No". Finally, the utility node in the developed ID is the cost of conducting this training.

Tailby et al. discuss at a hypothetical level existing tensions between different nations (Tailby, Coyle and Gill, no date). They propose an ID, which integrates relevant political factors with military factors for military strategic planning through military capability development. To that end, they consider a scenario-based analysis for identifying critical missions and capabilities necessary to conduct missions robustly. This proposed model contains variables related to aspects such as defense preparation and Course of Action (CoA) execution, and through its extension integrates feedback loops. Moreover, this model is simulated by conducting war games in a multidisciplinary perspective, i.e., not only with military players, but also with diplomatic and government players. Based on the results obtained, this model proves to be: (i) useful for tackling different dimensions of uncertainty in such a complex domain like the military domain, (ii) helpful when presenting its results to its users, and (iii) supportive for generating conditions and assumptions for further analytical studies in this domain. Staker proposed a theoretical ID for military decision-making support for launching an attack on the enemy (Staker, 1999). This proposed model considers intelligence and enemy strength as uncertainty nodes (random variables), launch attack as the decision node, and commander satisfaction as the utility node. Bilusich et al. developed two IDs for conducting both military and civil-military operations based on the military adaptive campaigning strategy through gaining insights into multiple military and civilian related environments (Bilusich, Bowden and Gaidow, 2011). The proposed models make sure the coherent operational approach, development and communication of military Commander's intent in conducting the respective military operation/civil-military operation, distribution of roles, and the interactions between actors involved together with their definition. Among the variables embedded in the first model are law and order, lead humanitarian aid provision, and acceptable economic environment, and in the second model variables like military actors and population are included.

Bergdahl proposed an ID that allows integration of aircraft dynamics, preferences of the pilots, and the uncertainty of decision-making in a structural and transparent manner for providing military air combat support (Bergdahl, 2013). This model contains nodes such as threat situation assessment, combat state, and overall evaluation. With this model, its player (i.e., the pilot)) is able to analyse air combat tactics and manoeuvring that could further assist in autonomous decision-making processes embedded by systems like military air combat simulators. Mengmeng et al. developed an extended ID for evaluating Systems of Systems Architecture (SoSA) by using an anti-missile architecture case (Mengmeng *et al.*, 2018). This model contains type of nodes like the process phases of an anti-missile, radar characteristics such as receive guidance and detect threat, and battalion command like send command and receive preparedness. Moreover, taking into consideration the novelty of this proposed model and its probabilistic nature, further research is necessary for grasping an in-depth perspective on SoSA while case scenarios have to be further defined and simulated to obtain a proper and realistic probabilistic extraction from the case scenarios conducted. These above-mentioned ID applications in the military domain show that they can be used for different objectives that range from task assessment, insights gathering, to decision-making support for both the agents involved in conducting military operations as well as the ones impacted by their effects.

The relevant aspects from the abovementioned ID applications are adapted and used to suit the potential ID applications in cyber security which will be detailed in Section 5.

5. Potential Application of Influence Diagrams in Cyber Security

This section describes conceptual designs for different potential applications of IDs in cyber security that are translated from existing applications of IDs in other domains. We identified and described three different applications which include: (i) response selection, (ii) cyber security training, and (iii) risk management.

5.1 Application Design 1: Response Selection

In case an operator observes an undesired top event in CIs, an operator needs to determine the nature of cause (i.e., attack or fault) in addition to the root causes (i.e., attack vector in case of an attack and failure cause in case of a fault), and corresponding effective response strategies. For this purpose, we adapted the application from Wang et al. proposed for fault troubleshooting of automotive engine (Wang, Huang and Zhang, 2013) to suit our application as shown in Figure 2. In our application, the uncertainty nodes include attack and fault, which are the nature of the cause in addition to attack vectors and failure causes which are the root causes. This notion is mainly adapted to suit our application from Wang et al., where they used fault causes of automotive engine failure (example: ignition timing error, ignition signal cutting off) (Wang, Huang and Zhang, 2013). Furthermore, we also adapted decision node where they had the states repair and not repair. In our application, we chose decision nodes with states including different response alternates and no response. We used costs corresponding to each decision as the utility node. This ID can support operators to choose optimal response strategies corresponding to each attack vector/failure causes based on their expected utility. The key components of this application design includes: **Deterministic Node** – Undesired Top Event, **Uncertainty Nodes** – (i) Attack/Fault (Nature of the Cause); (ii) Attack Vectors$_{1...m}$ / Failure Causes$_{1...n}$ (Root Cause), **Decision Nodes** – Decision Node$_{A1..m}$ (Response alternates in addition to no response to each attack vector) / Decision Node$_{F1..n}$ (Response alternates in addition to no response to each failure cause). **Utility Nodes** – Cost (expected utility of each response decision).

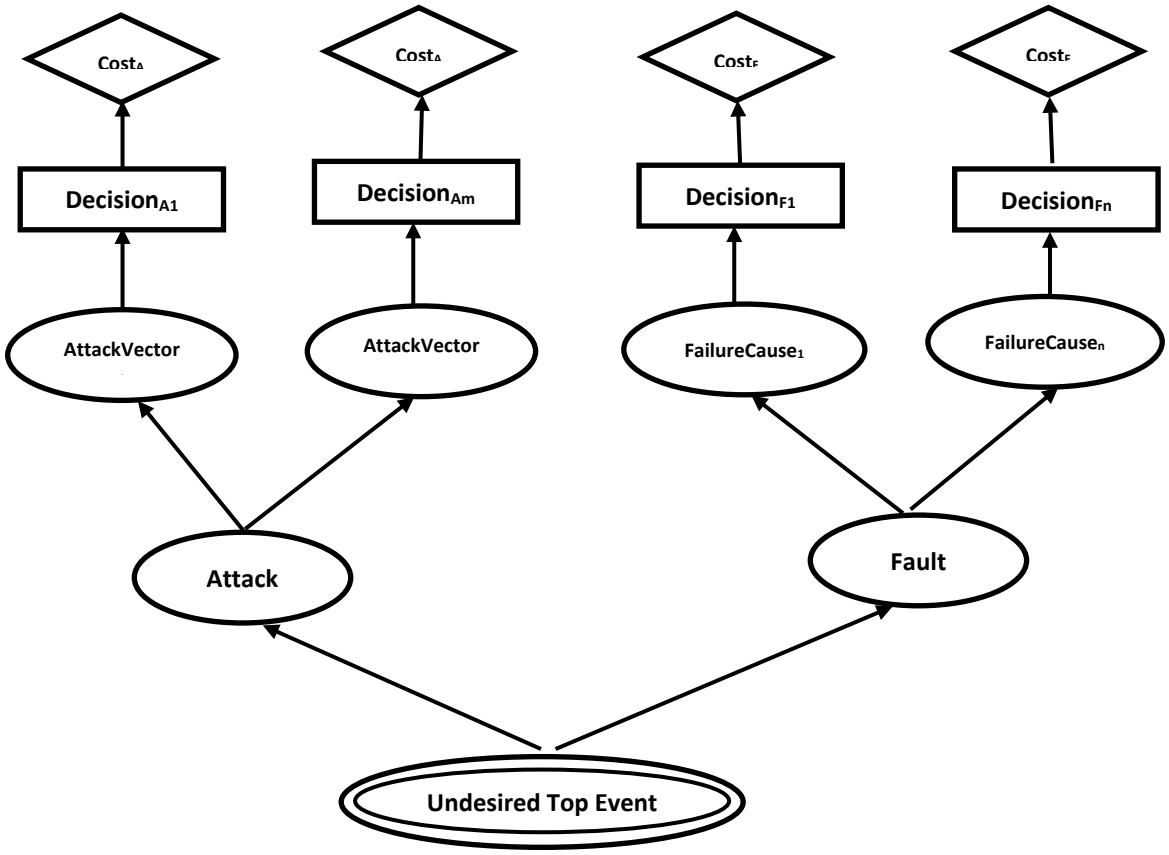

Figure 2. Design for Potential Application of IDs in Cyber Security – Response Selection

5.2 Application Design 2: Cyber Security Training

In organizations, it is important to provide decision support for management to prioritize group of personnel who need cyber security training and who do not need cyber security training. To that end, we adapted ID developed by Jeet et al. for estimating staff training in software industry (Jeet *et al.*, 2009) to suit our application as shown in Figure 3. They had four different chance nodes that are mainly related to skills and capabilities of a staff member (example: lack of experience with project software). We adapted it as skills and capabilities of a group of personnel in terms of cyber security in addition to the risk factors corresponding to a group of personnel and organization that suit our application. Furthermore, we adopted the notion of the decision node from (Jeet

et al., 2009) and used it as cyber security training with states needed or not needed. Finally, the decision node in our application corresponds to expected utility of providing cyber security training or not providing cyber security training. The key components of this application design include **Uncertainty Nodes** – competence level (within cyber security) (Beginner, Intermediate, Advanced); organization's cyber threat level (Low, Medium, High), handles confidential data (True/False), handles critical systems (True/False), **Decision Nodes** – cyber security training (True/False), **Utility Nodes** – expected utility of providing cyber security training and not providing cyber security training.

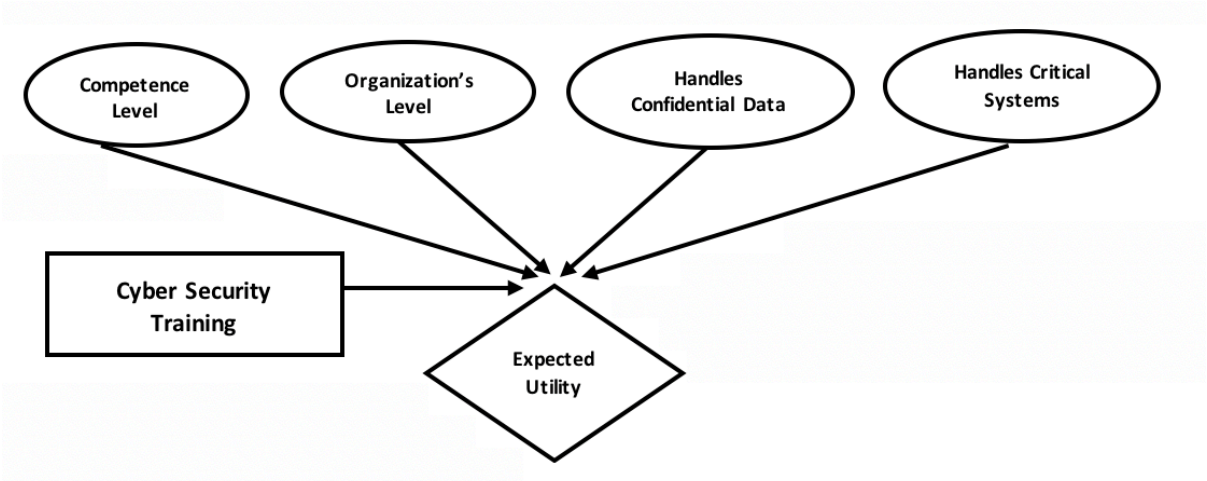

Figure 3. Design for Potential Application of IDs in Cyber Security – Cyber Security Training

5.3 Application Design 3: Cyber Risk Management

Cyber risk management plays an important role to put in place effective risk mitigation strategies. There is a need for decision support to put in place effective mitigation strategies to prevent a cyber-attack instead of responding to cyber-attack as in the case of our application design 1. The mitigation strategies could be to accept, avoid, transfer, or mitigate a risk depending on their impact and likelihood. We adapted the key components and structure from existing IDs proposed by Matviykiv et al. and Baio et al. (Baio *et al.*, 2006; Matviykiv, 2013) as shown in Figure 4.

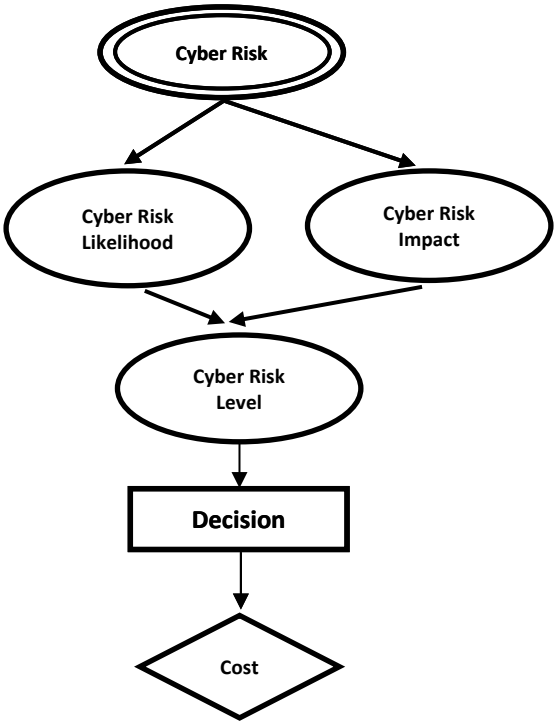

Figure 4. Design for Potential Application of IDs in Cyber Security – Cyber Security Training: Risk Management (Variant 1)

The key components of our variant 1 design include **Deterministic Node** – cyber risk (specific risk: true/false), **Uncertainty Nodes** – cyber risk likelihood (Likely/Possible/Unlikely), cyber risk impact (Significant/Moderate/Minor), cyber risk level (High/Medium/Low), **Decision Node** – Decision (Risk Mitigation Strategy: Accept/Avoid/Transfer/ Mitigate), **Utility Node** – Cost (this is the total cost associated with implementing risk mitigation strategy and ineffective decision).

In some cases, it is also important to choose a specific mitigation measure between different alternates within each mitigation strategy. We need to decide which mitigation measure to put in place in case we choose the strategy to mitigate the risk as our strategy. Therefore, we provide the design for this purpose as variant 2. The only difference between variant 1 and 2 is the states of risk mitigation strategy. Here in variant 2, we mainly look into specific risk mitigation measures instead of overall risk mitigation strategy. The key components of variant 2 include **Deterministic Node** – cyber risk (specific risk: true/false), **Uncertainty Nodes** – cyber risk likelihood (Likely/Possible/Unlikely), cyber risk impact (Significant/Moderate/Minor), cyber risk level (High/Medium/Low), **Decision Node** – Decision (Risk Mitigation Measure: different risk mitigation measures instead of high level strategy), **Utility Node** – Cost (this is the total cost associated with putting in place a specific risk mitigation measure and ineffective decision).

6. Conclusions and Future Work Directions

DSS provides an important foundation to make informed decisions within cyber security. Such DSSs are mainly developed using AI-based approaches like BNs, neural networks, and decision trees. IDs have the capability to be an effective underlying approach for DSS within cyber security especially due to its existing applications in other domains like medical in addition to its feature of easily explainable to different stakeholders ranging from personnel with technical and non-technical background. However, there is a lack of ID applications within cyber security. Therefore, in this research, we identified different existing applications of IDs in other domains including agriculture, medical, military, and safety. We then translated the identified existing applications of IDs into designs for potential applications in cyber security including response selection, cyber security training, and cyber risk management. In the future, we will implement provided designs and measure the effectiveness of IDs in cyber security applications through use-case approach.

References

Adepu, S. and Mathur, A. (2016) 'Using process invariants to detect cyber attacks on a water treatment system', in. *ICT Systems Security and Privacy Protection: 31st IFIP TC 11 International Conference, SEC 2016, Ghent, Belgium, May 30-June 1, 2016, Proceedings 31*, Springer, pp. 91–104.

Åström, H. *et al.* (2014) 'An influence diagram for urban flood risk assessment through pluvial flood hazards under non-stationary conditions', *Journal of water and climate change*, 5(3), pp. 276–286.

Baio, G. *et al.* (2006) 'Object-oriented influence diagram for cost–effectiveness analysis of influenza vaccination in the Italian elderly population', *Expert Review of Pharmacoeconomics & Outcomes Research*, 6(3), pp. 293–301.

Bergdahl, C. (2013) 'Modeling Air Combat with Influence Diagrams'.

Bilusich, D., Bowden, F.D. and Gaidow, S. (2011) *Applying influence diagrams to support collective C2 in multinational civil-military operations*. DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA).

Buzdugan, A. (2020) 'Review on use of decision support systems in cyber risk management for critical infrastructures', *Journal of Engineering Sciences*, (3), pp. 134–145.

Chockalingam, S. *et al.* (2021) 'Bayesian network model to distinguish between intentional attacks and accidental technical failures: a case study of floodgates', *Cybersecurity*, 4(1), pp. 1–19.

Chockalingam, S. (2021) 'Using Decision Trees to Select Effective Response Strategies in Industrial Control Systems'.

Howard, R.A. and Matheson, J.E. (2005) 'Influence diagrams', *Decision Analysis*, 2(3), pp. 127–143.

Jeet, K. *et al.* (2009) 'An Influence Diagram Based Approach for Estimating Staff Training in Software Industry', *Journal of Intelligent Systems*, 18(4), pp. 267–284.

Jensen, A.L. and Jensen, F.V. (2013) 'MIDAS-an influence diagram for management of mildew in winter wheat', *arXiv preprint arXiv:1302.3587* [Preprint].

Lacave, C., Luque, M. and Diez, F.J. (2007) 'Explanation of Bayesian networks and influence diagrams in Elvira', *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(4), pp. 952–965.

Lallie, H.S. *et al.* (2021) 'Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic', *Computers & security*, 105, p. 102248.

Leroy, I. (2022) 'The relationship between cyber-attacks and dynamics of company stock: the role of reputation management', *International Journal of Electronic Security and Digital Forensics*, 14(4), pp. 309–317.

Li, J. (2018) 'Cyber security meets artificial intelligence: a survey', *Frontiers of Information Technology & Electronic Engineering*, 19(12), pp. 1462–1474.

Manasa, S. and Kumar, K.P. (2022) 'Digital Forensics Investigation for Attacks on Artificial Intelligence', *ECS Transactions*, 107(1), p. 19639.

Matviykiv, T.M. (2013) 'Use of influence diagrams for decision support in drilling automation', *Journal of Global Research in Computer Science*, 4(4), pp. 1–7.

Mengmeng, Z. *et al.* (2018) 'Functionality evaluation of system of systems architecture based on extended influence diagrams', *Journal of Systems Engineering and Electronics*, 29(3), pp. 510–518.

Olan, F. *et al.* (2022) 'Artificial intelligence and knowledge sharing: Contributing factors to organizational performance', *Journal of Business Research*, 145, pp. 605–615.

Owens, D.K., Shachter, R.D. and Nease Jr, R.F. (1997) 'Representation and analysis of medical decision problems with influence diagrams', *Medical Decision Making*, 17(3), pp. 241–262.

Peffers, K. *et al.* (2007) 'A design science research methodology for information systems research', *Journal of management information systems*, 24(3), pp. 45–77.

Peffers, K., Tuunanen, T. and Niehaves, B. (2018) 'Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research', *European Journal of Information Systems*, 27(2), pp. 129–139.

Prajapati, S. and Singh, A. (2022) 'Cyber-Attacks on internet of things (IoT) devices, attack vectors, and remedies: a position paper', *IoT and cloud computing for societal good*, pp. 277–295.

Rees, L.P. *et al.* (2011) 'Decision support for cybersecurity risk planning', *Decision Support Systems*, 51(3), pp. 493–505.

Staker, R. (1999) *Military information operations analysis using influence diagrams and coloured Petri Nets*. ELECTRONICS RESEARCH LAB SALISBURY (AUSTRALIA).

Tailby, M.D., Coyle, G. and Gill, A. (no date) 'The Application of Influence Diagrams for the Development of Military Experiments'.

Wang, Y.S., Huang, Y.P. and Zhang, R.J. (2013) 'Decision Strategy for Fault Troubleshooting Using Bayesian Influence Diagram', in. *Applied Mechanics and Materials*, Trans Tech Publ, pp. 541–545.

Weflen, E., MacKenzie, C.A. and Rivero, I.V. (2022) 'An influence diagram approach to automating lead time estimation in Agile Kanban project management', *Expert Systems with Applications*, 187, p. 115866.

Wilde, L. (2016) 'A Bayesian Network Model for predicting data breaches caused by insiders of a health care organization'.

Zhang, Z. *et al.* (2022) 'Artificial intelligence in cyber security: research advances, challenges, and opportunities', *Artificial Intelligence Review*, pp. 1–25.