Classification of Decision Support Systems for Cybersecurity

Marin François, Pierre-Emmanuel Arduin, Myriam Merad

CLASSIFICATION OF DECISION SUPPORT SYSTEMS FOR CYBERSECURITY

Research full-length paper

François, Marin, Université Paris-Dauphine PSL, LAMSADE, CNRS, Paris, FR, marin.francois@dauphine.psl.eu

Arduin, Pierre-Emmanuel, Université Paris-Dauphine PSL, DRM, CNRS, Paris, FR, pierre-emmanuel.arduin@dauphine.psl.eu

Merad, Myriam, Université Paris-Dauphine PSL, LAMSADE, CNRS, Paris, FR, myriam.merad@dauphine.psl.eu

Abstract

As part of a research and development program aimed at providing a decision support system for cyber risk management, we conducted an in-depth analysis of the research, innovation and collaboration environment for decision support technologies and mathematical decision support systems for cybersecurity. We analysed 5,841 documents from three different databases and derived 79 significant documents, each presenting a single decision support system for cybersecurity. We conducted a bibliometric and semantic analysis of all documents to identify the dynamics of collaboration, research trends, and other structural elements, and we analysed these 79 models under 16 risk management evaluation criteria to assess their relevance. This work now allows for a better understanding of the dynamics underlying cyber risk modelling research, an analysis of the models used by academic and private research, a classification of these models regarding these same evaluation criteria, and a taxonomy of decision support systems for cybersecurity.

Keywords: Cybersecurity, decision support systems, risk, bibliometrics.

1 Introduction

The cyber threat landscape is vast and changing at rapid pace (Bortzmeyer, 2019). The risk associated with cyber criminals and cybersecurity issued is increasingly present. The motivations of today's attackers are primarily monetary as attacks against private organisations, institutions or financial channels represent a direct pecuniary gain for these attackers. It is no secret that there are black markets and illegal piracy forums (Ball, 2019). However, as hacking and the use of computers has become more common place, even low-skilled hackers can become part of the cyber-attack ecosystem by purchasing access to corporate infrastructures (Akintaro, 2019). If yet most of the organizations manage risks and incidents better year after year, specifically by increasing their capacity at restoring data after an attack, most of these organizations are unable to use their budget and resources effectively to stop the incidents (Arpagian, 2017). Cybersecurity practices in organisations of all sizes are very uneven today. Some processes are very mature and rigorously controlled, often enforced by legal constraints, others are much less so, often due to lack of time and staff.

As researchers, auditors, the larger the organisation, the more difficult it will be to assess the performance of security practices, given this heterogeneity. However, while the available data continues to grow and data processing technologies promise to make brilliant analyses possible, the scientific community dealing with cyber risk management does not seem to be able to agree on one best decision support system (DSS) over another and the sheer volume of publications on the subject makes the task

of analysis and system architecture very difficult. According to Hatleback (2018), this is because cyber risk management is still in the proto-science stage today. This paper aims at contributing to literature by providing a clear benchmark of cyber DSS and a classification, in a form of a taxonomy. Academic literature now has a significant impact on the direction that companies take in terms of security, and we aim to provide an innovative decision support system for cyber risk management for those same companies. To propose a mathematical model and an adapted management methodology, we studied the existing literature and analysed individually a selection of models according to 16 evaluation criteria (Merad and Trump, 2020). The aim of this research is threefold. We seek a clear understanding of different existing scientific proposals for decision support in cyber risk management, to identify the underlying dynamics of the scientific production environment, such as collaborations, affiliations, or research trends, and we seek to individually assess a representative sample of decision support models against specific criteria, to identify the shortcomings and limitations that our scientific proposal should address. We have also identified certain gaps in the academic literature, notably the absence of a taxonomy of decision support systems for cybersecurity. This article therefore proposes one and aims at contributing to information systems academic literature.

This paper is limited to the observation of the research environment for cyber risk decision support. We will not address the reasons of the dynamics observed in the research environment, as this will be the subject of a further part of our research and development program, accompanied by several field experiences analysis. Also, we will only use academic research as material, as the industry standards and whitepapers will be used in another research aiming at identification of industrial contribution. For researchers wishing to implement one such DSS in an organisation, the material provided in this paper aims to be enough to select the right model depending on 16 criterions of your situation. In this article, we will first present our research and document database sorting methodology, then we will give the key findings of our analysis of environmental dynamics, then we will provide our taxonomy and the results of our evaluation of the sample of decision support models. Finally, we will conclude with the main elements and our future work.

2 Research Design

In this section, we define the elements that constrained our search strategy. Then we present the methodology used to sort the research documents. Finally, we will come back to the possible biases and limits of this method.

2.1 Search Strategy

Scopus[1], Web of Science[2], and OpenKnowledge Maps[3] are popular platforms for building literature reviews due to their extensive coverage of scholarly publications, comprehensive search capabilities, and advanced analytical tools. Scopus is one of the largest abstract and citation databases, covering over 76 million records from over 24,000 journals, conference proceedings, and books. It provides a comprehensive search function that allows users to find relevant articles, conference papers, and book chapters related to their research topic. Web of Science is a leading citation database that covers over 100,000 journals, conference proceedings, and books in various fields, including science, social sciences, and humanities. It offers robust search capabilities, allowing users to refine their search results based on various criteria, such as publication date, author, and keyword. OpenKnowledge Maps is an open-access tool that provides an interactive visualization of research topics and trends. It allows users to explore scholarly literature in a graphical format, which can be particularly helpful for identifying key areas of research and understanding how different topics are related. We used multiple queries when searching these databases to collect relevant articles for our literature review, such as *((TITLE-ABS-KEY ("Cybersecurity") OR TITLE-ABS-KEY ("Information-Security") OR TITLE-ABS-KEY*

1https://www.scopus.com/home.uri
2https://www.webofscience.com/wos/
3https://openknowledgemaps.org/

("infosec")) AND TITLE-ABS-KEY ("risk") AND (TITLE-ABS-KEY ("framework") OR TITLE-ABS-KEY ("methodology")) AND (TITLE-ABS-KEY("Model") OR TITLE-ABS-KEY ("Modeli[zs]ation"))) or more general ones such as (*TITLE-ABS-KEY (((cyber OR information) PRE/1 security) AND "risk" PRE/3 ("model" OR "management"))). A* single query could not capture all the relevant articles in our field, so we used multiple ones with different search terms to broaden our search. We also recognized that researchers in our field may use different terminology to describe the same concept or topic. A list of queries is presented in Fig. 1 (part 1 of the process presented, "*initial data gathering*").

2.2 Document funnel procedure

As cybersecurity is a growing area of research, we quickly found ourselves overwhelmed by too many (5,841) documents for the second part of our analysis. Therefore, we had to develop an article exclusion funnel to draw from the initial batch a sample of articles to be analysed individually. Once the set of documents was collected, we proceeded to extract all the fields present on the platforms (Abstract, Title, Keyword, etc.). This enabled to obtain data formats that could be handled by other tools, such as VOSViewer, to carry out a bibliographic analysis of the documents including extracting the themes that could be grouped together and/or commonly addressed by researchers and analysing the collaborations between researchers and/or actors from outside the academic world. Once these groups have been identified, we can finally extract the corresponding full articles via the OpenKnowledge map platform, targeting the themes observed in the first part of the study. -A diagram of the funnelling procedure is shown in Fig. 1 bellow.

2.3 Limitations

Our objective here is to take advantage of the process presented in order to extract essential information from a large number of documents that would otherwise be difficult to process, identify the key actors in the academic world on cyber risk management issues, identify the key notions used by the researchers in the academic world, use this information to find relevant risk management models and evaluate them with regard to the criteria for evaluating a risk management method. We are limited by the content of the databases and our results could be oriented by the selection of the keywords in the first stage, and the selection of the research themes in the second stage.

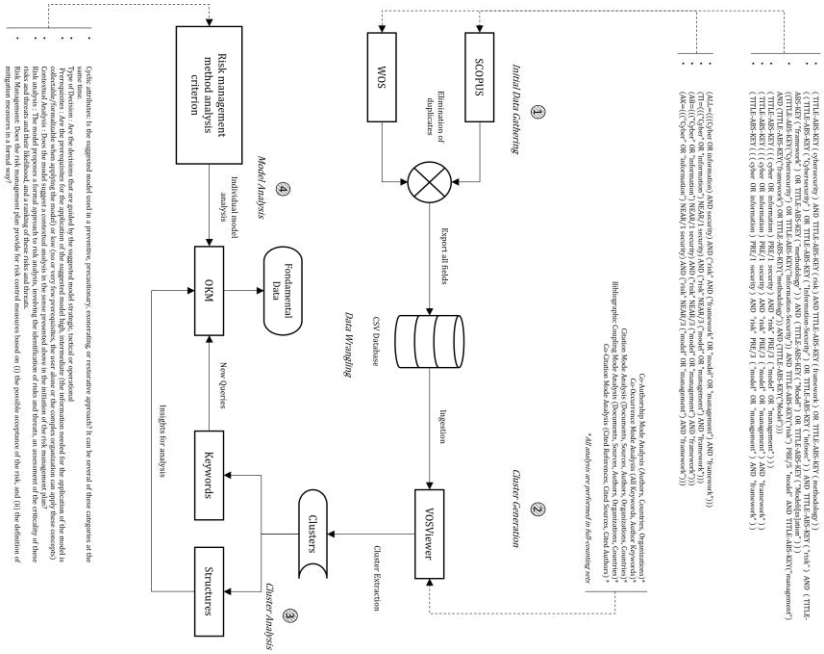


Figure 1. Diagram of the document funnelling procedure

3 Cluster analysis

For our cluster analysis, we used VOSViewer to analyse our full length set of documents (as described in Fig. 1). VOSViewer provides a variety of visualization options that can help researchers to identify patterns, trends, and connections within data.

3.1 Keyword, Co-authorship, and Affiliation Analysis

Clustering on keyword (Fig. 2), we observed the appearance of central notion such as: “risk assessment”, “risk management” which are directly linked to our queries, but also the appearance of new notions, such as “network security”, which is very well represented, without being directly queried. We can already identify four main clusters. In blue: the “risk analysis and safety engineering” cluster, in yellow the “network security and statistics” cluster, in green the “security management and governance” cluster and in red the “privacy” cluster.

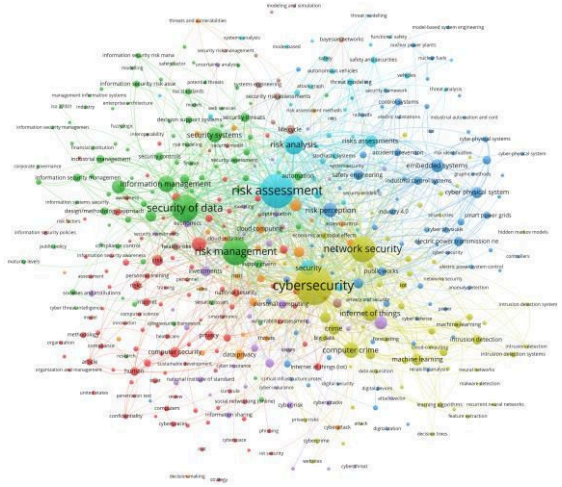
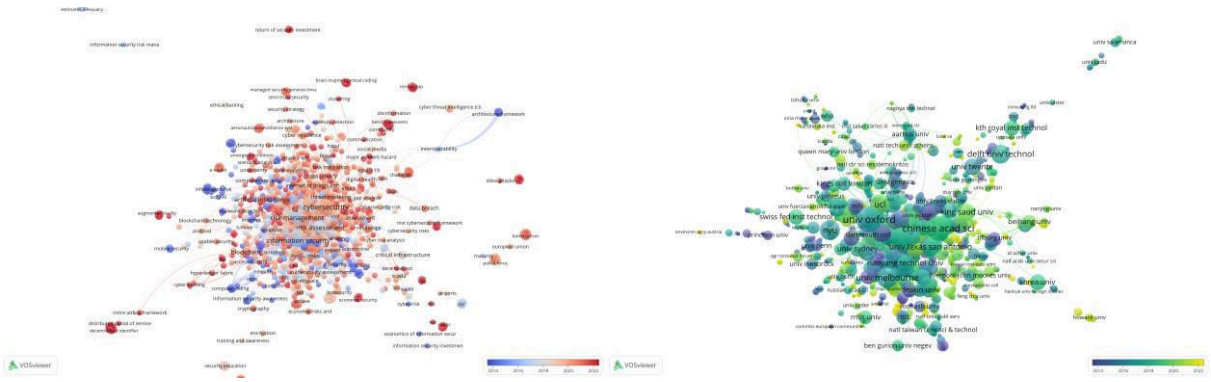


Figure 2. Keywords, no overlay.

By applying a colour overlay representing to the publication date (Fig. 3.a), central notions such as "Cybersecurity" are still widely cited, but we can observe older appearances of the notions of "decision support" (2014), "risk modelling" (2015), or "system analysis" (2016), which despite an important centrality, are gradually replaced by notions linked to new technologies (*e.g.*, "decentralized", "blockchain") or to tools gaining in popularity. This indicates that cybersecurity is a science whose lexical field is rapidly evolving.



(a) (b)

Figure 3. Dynamic keywords (a) and Dynamic Co-authorship clusters (b)

Similarly, we identified the poles of influence over the last few years by filtering the universities with the most publications and collaborations. We identified that despite later publications (2020-2022), some universities manage to obtain a high degree of centrality in the network (Fig. 3.b). This indicates that cybersecurity research is not, according to this graph, a research field where laboratories have to justify a long research history to obtain collaborations and results that solicit interest within the community. We also carried out an analysis of university laboratories' collaborations with institutional actors, and an analysis of country collaborations, which we cross-referenced with the analysis of publication affiliations by country. We note a strong predominance of countries who began research in cybersecurity earlier (Fig. 4). We also observed large connection affiliations between universities and national organisations, such as the NIST (Fig. 5).

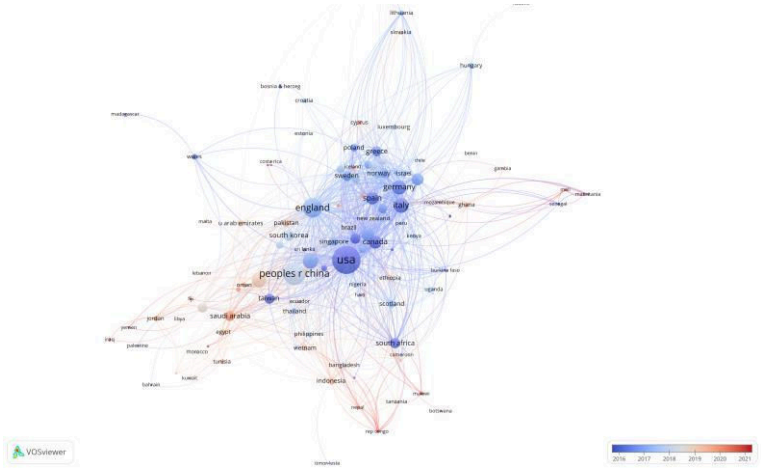


Figure 4. Clusters of countries

Figure 5. Affiliations

3.2 Key findings

After analysing the groups of notions commonly approached by the academic scientific community, we have drawn two major themes of cybersecurity research to focus on when exploring decision support systems technologies: (1) network security and (2) resilience. There is a strong connection between network security and decision support, with notions such as “machine learning”, “simulations”, “discrete events” - which indicates that part of the scientific community approaches the issues of decision support and risk assessment from the perspective of network modelling and analysis and attack simulation. On the other hand, resilience is at the crossroads of security and reliability with a significant number of co-occurrences in articles dealing with infrastructure, network security, modelling, simulation, and threats. Resilience also calls upon the notions of continuity and mission, which do not appear in the other fields. The detailed families of decision support of models have been grouped in a taxonomy presented in Figure 6. Countries that funded cybersecurity academic research the earliest are now the ones that have the most attraction for collaborations with affiliations. We can notice the leadership of Western countries, quickly followed by the People's Republic of China. Universities that are new to the field of cybersecurity research still manage to obtain large volumes of citations on recent concepts. Finally, we observed a very strong attraction of actors such as the NIST for academic research affiliations with universities around the world.

4 Model Evaluation

In this section, we present the findings of our analysis of 79 documents and the models they propose against 16 performance criteria of a risk management methodology. Details of the documents and their classification are available in Appendix B.

4.1 Background for model analysis

Using keywords defined through cluster analysis, we have compiled a database of 79 documents dealing specifically with related topics and presenting a model for decision support. We sorted the articles based on these keywords, whether the authors had a specific risk management model, -number of citations, authors’ affiliation, and year of publication. Finally, we analysed each of the proposed models individually against 16 performance criteria of a risk management methodology (Merad and Trump, 2020). For each risk management methodology or risk analysis and management model, we seek to answer the following questions[4]: **-Cyclic attributes:** Is the suggested model used in a prevention, precaution, exoneration, or recovery approach? It can be several of these categories at the same time. - **Type of Decision:** Is the DSS used for operational, tactical, or strategic decision making? - **Prerequisites:** Are the technical prerequisites for the integration of the suggested model high (lot of data collection and preparation, external sources and intelligence needed), intermediate (the data needed for the DSS is collectable “on the fly”) or low (no or very few prerequisites, the expert user alone can define it). - **Contextual Analysis:** Does the model suggest a contextual analysis in the initiation of the risk management plan? - **Risk analysis:** Does the model proposes a formal approach of risk analysis, involving the identification of risks and threats, an assessment of the criticality of these risks and threats and their likelihood, and a ranking of these risks and threats? -**Risk Management:** Does the risk management plan provide for risk control measures based on (*i*) the possible acceptance of the risk, and (*ii*) the definition of mitigation measures in a formal way? This analysis is summed up in the table in Appendix B. This table can be used by any organisation/researcher in order to identify the best family of model for its problem of cybersecurity risk management as defined Appendix A. As one would not use the same DSS for asserting cybersecurity risk at operational level (e.g., IDS/IPS, ML methods) and to communicate and manage risk at CISO level (strategic risk management). Also, we wanted to analyse if they were some caveats in the model proposed regarding the needs of an ideal security management program (*i.e., satisfying all the criterion*): and we found some, as described in part 4.2.

[4]Background for the choice of these specific criterion is detailed in Annexe A.

4.2 Key findings of model evaluation

None of the research articles dealt with risk management in the exoneration phase, excepted for machine learning systems that can manage unknown threats. This finding is shared by other reviews of the literature on the subject (Ani et al., 2019; Hatleback, 2018). The same applies to the recovery phase, which is covered by only 3 articles, or 3.79% of our base, (Creese, 2013; Holm, 2015 Hong, 2014). On the other hand, we have identified that for 51.89% of the articles (41) the proposed model is suitable for risk management in the precautionary phase, for 78.4% (62) in the prevention phase. Furthermore, 20 documents propose a risk management model that is adapted to both the precautionary and prevention phases. Typical models of the precautionary/preventive double addressing are the detection and simulation models proposed by Cohen (1999) or Kuhl (2007), most of the following papers base their decision support system design on one of them. Finally, some of the models presented go so far as to propose a risk management approach that can be used in the precautionary, prevention, and recovery phases, notably by integrating forms of 'back-testing' following the feared event based on the model used in the previous phases (Hong, 2014).

Regarding system classes, several families of operational research models appear multiple times for risk precaution/prevention decision support. Some researchers only used one type of model for multiple projects (*e.g.* Markov decision processes (*MDP*), -see Abraham, 2015-a,b,c). *MDP* appeared as mathematical support for multiple systems, including stochastic calculus, dynamic games, network graphs, and probabilistic methods. We also observed a strong use of models native to cybersecurity, declined from Markov decision processes such as attack trees who are notably used in the precautionary and prevention phases (Woodard, 2007; Holm, 2014; Hong, 2014; Lippmann, 2005; Valja, 2015; Yusuf, 2015, 2016; O'Neil, 2013). We will analyse this class of systems in-depth in future works, oriented toward threat modelling. Markov decision processes and attack trees are often based on graphs, which are used as representations of computer networks to manage risks by controlling vulnerabilities and developing defences, by allowing the development of new firewall rules and new detection rules. In these models, the authors generally assume that (1) - the network mapping is known, which can be a hindrance to the implementation of the solution, but also that (2) - the critical resources of the network are identified.

Decision Support Systems (DSS) can vary greatly in terms of information granularity, ranging from simple segment representations to packet and protocol simulations. To implement some of them, it is necessary for the organisation to have at least an inventory and mapping of its Information Technology (IT) assets. If one wishes to implement more precise models, *e.g.,* DSS using game theory notions to specify the behaviour of the attacker (Ekin, 2019; Wang J.L., 2021), or to consider and define the levels of exploitability of the network nodes (Miller et al., 2016), the data requirements must be considerably increased. Of all the DSS responding to the analysis needs in the precautionary and prevention phases and using methods based on attack trees and graph network modelling, 61.11% (11) are classified as having significant data requirements, and 38.8% (7) are classified as having intermediary data requirements. Furthermore, regarding the possible categorisation of models according to their contribution to the needs of risk identification, risk assessment, and risk prioritisation, DSS based on graph structures have in many cases satisfied all the steps of the process, or at least partially, with a predominance of the ability of these models to provide solutions for risk assessment and prioritisation. One out of two models requires that threats are already identified. Out of the 21 models proposed, 10 allow for the identification of threats, 16 for their assessment, and 11 for their prioritisation.

As regards the decision-making that should follow the use of these DSS, we observed that these models are primarily designed for tactical decision-making (61%), operational decision-making (38%) and sometimes both (9.52%), mainly depending on the level of precision of the input data. Risk tolerance assessments are generally absent and risk mitigation measures as well. Of all the models we have analysed, only 9 propose risk tolerance measures, or at least mention it, and only 10 propose at least implicitly examples of remediation directly in the model. For the models based on the network graph representation, no model mentions risk tolerance, and only one (Holm, 2014) directly proposes mitigation measures. DSS that take advantage of the mathematical properties of graphs to make them

robust analysis systems, which can be good supports for constrained optimisation decision support systems. It is possible to produce systems that take uncertainty into account, by producing operating likelihood and reachability metrics, with different levels of accuracy possible depending on the data available.

4.3 Classification and limits

From a macro perspective, our analysis has enabled us to identify a taxonomy of risk management decision support models. We have identified eight main families of models, which are presented below. Within these eight families, we have identified 26 sub-families of models. The taxonomy thus formed allows us to map which type of system meets which need. For each sub-family, the literature allows us to identify the strengths and weaknesses of the models belonging to it. It is important to note that several decision support systems benefit from mathematical properties of multiple categories within the taxonomy (*e.g.* Attack-Trees and Threat Modelling). However, we identified for each paper the main contributing field and associated the model with this field. It is also important to note that several categories overlap (*e.g.* machine-learning / statistics). As including the overlap and multiple sources properties would tend to make our taxonomy less readable, we only represented the most representative category for each of the model. With this information in hand, it is appropriate to carry out an in-depth study of the situation of the organization seeking a decision support model to identify the most suitable model. Below is the taxonomy of decision support models that has been developed (Fig. 6).

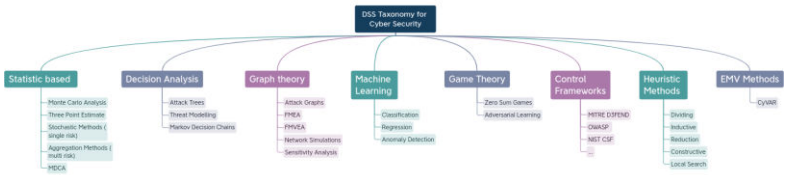


Figure 6. Taxonomy of decision support systems for cybersecurity

Statistic Based methods are useful in high uncertainty environments. Data in the form of time series, such as systems logs offer great potential for statistical analysis. If a value can be attributed to a single event (X) and it its distribution is properly identified, numerous probabilistic and stochastic methods with various levels of precision can be applied to quantify loss distribution, identify trends, patterns, anomalies in data, which is helpful for risk quantification and treatment prioritisation. When significant data is available, multiple events can be combined in risk aggregation methods to analyse events, expected value and probabilities of occurrence. Risk aggregation can take place following various methods and can help identify systematic correlation, which is helpful in crisis prevention. When little data is available, such systems can integrate expert knowledge to make up for missing data (e.g., three-point estimates, maximum value theory, etc.) However, statistic Based methods rely heavily on data and if possible historical data, which may not always be relevant or accurate for current or future scenarios. In addition, statistics-based methods do not always provide a clear understanding of the causes and consequences of security events, which can be important for developing effective security strategies.

Decision Analysis provides systematic and structured approach to decision-making, which can be particularly useful in complex and uncertain cybersecurity environments. Most security architects and engineers will not need additional training to use decision analysis methods such as decision trees and threat modelling. More advanced, semi quantitative methods, such as Markov Decision Chains (MDP) can be used to enhance decision trees. MDP have the advantage of being convertible in other systems such as weighted graphs and could be used for stochastic and probabilistic modelling. Also, special MDP such as HMM (Hidden Markov Models) can be useful in high uncertainty environment, when only partial information is available (*e.g.* no information on all attackers (*hidden states)*, but information on

alerts (*observations*): one could infer the first from the second using HMM). Finally, Decision Analysis Models usually are self-explanatory is enough detail is provided by the designer of the model. Which is very helpful in maintaining the knowledge base of the organisation. However, Decision analysis can be time-consuming and resource-intensive, and may not always be practical for making tactical or operational decisions. It also relies heavily on assumptions and subjective inputs, which can introduce biases and uncertainties into the decision-making process. Additionally, decision analysis may not always account for the dynamic nature of cybersecurity threats, which can change rapidly and unpredictably. Graph theory provides a powerful tool for modelling and analysing complex systems such as computer networks. In more advanced forms, network graphs could be used to represent full information systems, including network topologies, users, computers, and data.

Such representation enhances the analysts for advanced breach consequences exploration, using graph specific algorithms such as path finding algorithms. They allow for in-depth analysis of the information system on a structural perspective: effectiveness of security architecture, optimisation, single points of failures, transmission bottlenecks, etc. Just like MDP, network graphs are a great support for statistical analysis when they are used to constrain simulations. However, Graph theory requires a high level of technical expertise and may not be accessible to all cybersecurity professionals. It relies heavily on assumptions and simplifications, which can limit its accuracy and applicability in complex real-world scenarios. Graph theory may not always account for the dynamic nature of cybersecurity threats and the complex interactions between different network components.

Machine learning provides a very wide range of tools that can be used in multiple stages of the risk management cycle. Logistical regressions and similar models can be used for classification of events and anomaly detection, very effective when used in software such as intrusion detection systems and endpoint detection and response software. Linear regression and similar models can offer prediction capabilities for time series events. This is very useful in network analysis and behaviour analysis. The learning capability of these algorithms make them efficient for high uncertainty and highly changing environment, with the capacity to detect and successfully identify unknown threats. Machine learning methods are a subset of statistic-based methods. On the other hand, Machine learning requires a large amount of high-quality data to be effective, which may not always be available in cybersecurity environments. Additionally, machine learning models can be difficult to interpret, which can make it challenging to understand their underlying logic and decision-making processes.

Game theory inspired models with player representing attackers and defenders, and reward/pay-off systems representing the motivations of each player can be illustrating and analysing attackers' behaviour and assessing security postures. Games can be zero/non-zero sum, most likely non-cooperative, and can be static of dynamic. In a dynamic game, the player follows multiple actions dynamically. This type of set can be represented using MDP, with the same properties of being a great support for stochastic games, where outcomes and « most likely taken » actions can be represented using probabilities. Dynamic game sets can be influenced by threat intelligence and historical data. However, Game theory relies heavily on assumptions and simplifications, which can limit its accuracy and applicability in complex real-world scenarios. It can also be challenging to apply game theory to cybersecurity environments, which are often characterized by incomplete information and asymmetric power relationships. Game theory may not always account for the dynamic nature of cybersecurity threats and the complex interactions between different actors.

Heuristic methods provide a practical and intuitive approach to cybersecurity risk management, which can be particularly useful in situations where there is limited data or time available. They involve using rules of thumb, experience, and common sense to identify and mitigate risks. Heuristic methods can be useful for making tactical and operational decisions, as well as for identifying emerging threats and vulnerabilities. However, Heuristic methods may not always be based on sound scientific principles,

which can limit their effectiveness and reliability. They can also be vulnerable to cognitive biases and subjective judgments, which can introduce errors and uncertainties into the decision-making process. Heuristic methods may also be less effective at identifying complex and emerging threats, which may require more sophisticated analytical techniques.

Finally, Expected Monetary Value (EMV) methods provide a quantitative approach to cybersecurity risk management, which can be useful for assessing the financial impact of security events and making decisions based on expected outcomes. They involve calculating the expected value of different decision alternatives and assessing their associated risks and rewards. EMV methods can be useful for making strategic decisions and for optimizing resource allocation. EMV methods are the most likely way to communicate cyber risk to non-technical decision makers. EMV methods may not always account for non-financial impacts of security events, such as reputational damage or loss of customer trust. They may also be less effective at predicting rare or black swan events, which can have a significant impact on an organization's finances.

5 Conclusions and future works

Our analysis enabled us to identify the categories of DSS for cybersecurity and particularly cyber risk management from which we could draw our inspiration to provide a proposal adapted to our organisation. From a more theoretical point of view, this analysis enabled us to map the models according to 16 evaluation criteria. DSS leveraging network simulations allowed to measure more precisely the criticality of vulnerabilities in the context of an organisation, notably by analysing the structural properties of networks and their topologies, or the centrality metrics of assets. These DSS are mainly used to produce protection rules and effectively reduce the attack surface of an organisation by simulating large numbers of configurations under certain optimisation constraints. However, DSS for cyber risk management are almost exclusively offered for tactical and/or operational use. They never address the issue of risk tolerance, and they almost never address the response to risk. Thus, the authors propose very effective models for evaluating and sometimes prioritising risk responses, but the possible responses must be sought by the user elsewhere. As these models are aimed at expert populations (tactical and/or operational decision support) this is not a problem in principle, but these models are therefore difficult to implement in an immature company. In future work, we will compare this mapping of DSS proposed by academia with the evolution of industry standards, the evolution of the legal framework related to cybersecurity, and the evolution of the attacker profile, in order to understand what other dynamics are driving this work.

References

Abraham, S, Nair, S., (2015), A Novel Architecture for Predictive CyberSecurity Using Non-homogenous Markov Models (2015). Available at: https://ieeexplore.ieee.org/document/7345354.

Akintaro (2018) “Darknet and black market activities against the cybersecurity: a survey,” The Midwest Instruction and Computing Symposium.(MICS), North Dakota State University [Preprint].

Algarni, A., Thayananthan, V. and Malaiya, Y.K. (2021) “Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems,” Applied Sciences, 11(8), p. 3678. Available at: https://doi.org/10.3390/app11083678.

Andrade, R.O. (2021) Big Data Analytics Architecture for Cybersecurity Applications. Available at: https://doaj.org/article/f8ea5bbf766d4122acc417a5b8734dfc.

Ani, U.D. et al. (2019) “A Review of Critical Infrastructure Protection Approaches: Improving Security through Responsiveness to the Dynamic Modelling Landscape,” arXiv (Cornell University) [Preprint]. Available at: https://doi.org/10.48550/arxiv.1904.01551.

Antczak, J. (2020) “CYBERSECURITY COSTS IN AN ENTERPRISE UNIT,” Edukacja Ekonomistów I Menedżerów [Preprint]. Available at: https://doi.org/10.33119/eeim.2020.55.6.

Applebaum, A. et al. (2016) "Intelligent, automated red team emulation," Annual Computer Security Applications Conference [Preprint]. Available at: https://doi.org/10.1145/2991079.2991111.

Arpagian, N. (2017) "Les entreprises sont devenues hypersensibles au risque numérique," SéCurité & StratéGie [Preprint]. Available at: https://doi.org/10.3917/sestr.027.0060.

Ball, M. et al. (2019) "Data Capture and Analysis of Darknet Markets," Social Science Research Network [Preprint]. Available at: https://doi.org/10.2139/ssrn.3344936.

Basto-Fernandes, V. (2017) A Comparison of Cybersecurity Risk Analysis Tools. Available at: http://hdl.handle.net/2086/15669.

Bortzmeyer, S., Souissi, M. and Schafer, V. (2019) "Cybermenaces, enjeux et sécurité," Flux [Preprint]. Available at: https://doi.org/10.3917/flux1.118.0059.

Carriegos, M.V. et al. (2021) "On Aggregation and Prediction of Cybersecurity Incident Reports," IEEE Access, 9, pp. 102636–102648. Available at: https://doi.org/10.1109/access.2021.3097834.

Chronopoulos, M., Panaousis, E. and Grossklags, J. (2018) "An Options Approach to Cybersecurity Investment," IEEE Access, 6, pp. 12175–12186. Available at: https://doi.org/10.1109/access.2017.2773366.

Cohen, F. (1999) "Simulating cyber attacks, defences, and consequences," Computers & Security, 18(6), pp. 479–518. Available at: https://doi.org/10.1016/s0167-4048(99)80115-1.

Creese, S., Goldsmith, M., Moffat, N., (2013) CyberVis: Visualizing the potential impact of cyber attacks on the wider enterprise (2013a). Available at: https://ieeexplore.ieee.org/document/6698979.

Creese, S., Goldsmith, M., Moffat, N., (2013) CyberVis: Visualizing the potential impact of cyber attacks on the wider enterprise (2013b). Available at: https://ieeexplore.ieee.org/abstract/document/6698979/.

Creese, S., Goldsmith, M., Moffat, N., (2013) CyberVis: Visualizing the potential impact of cyber attacks on the wider enterprise (2013c). Available at: https://ieeexplore.ieee.org/abstract/document/6698979/.

Ekin, T. (2019) Augmented Probability Simulation Methods for Non-cooperative Games. Available at: https://arxiv.org/abs/1910.04574.

Fagade, T., Maraslis, K. and Tryfonas, T. (2017) "Towards effective cybersecurity resource allocation: the Monte Carlo predictive modelling approach," International Journal of Critical Infrastructures, 13(2/3), p. 152. Available at: https://doi.org/10.1504/ijcis.2017.088235.

Galinkin, E. et al. (2022) "Simulation of Attacker Defender Interaction in a Noisy Security Game," arXiv (Cornell University) [Preprint]. Available at: https://doi.org/10.48550/arxiv.2212.04281.

García-Teodoro, P. et al. (2009) "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computers & Security, 28(1–2), pp. 18–28. Available at: https://doi.org/10.1016/j.cose.2008.08.003.

Hatleback, E. (2018) "The protoscience of cybersecurity," The Journal of Defense Modeling and Simulation, 15(1), pp. 5–12. Available at: https://doi.org/10.1177/1548512917737635.

Hong (2014) What Vulnerability Do We Need to Patch First? Available at: https://ieeexplore.ieee.org/document/6903625.

Hughes, J. (2013) Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. Available at: https://doaj.org/article/7b2d5bc4f5d44ddc8fc5cd5a0adca9c4.

Valja, M., Korman, M., Shahzad, K., (2015), Integrated Metamodel for Security Analysis,IEEE Xplore Login (no date a). Available at: http://ieeexplore.ieee.org/docurnent/7070437.

Xie, P., Li, J.H., Ou, X., (2010), Using Bayesian networks for cyber security analysis,IEEE Xplore Login (no date b). Available at: http://ieeexplore.ieee.org/docurnent/5544924/.

Ivanova, Y. (2017a) "Modelling the impact of cyber attacks on the traffic control centre of an urban automobile transport system by means of enhanced cybersecurity," MATEC Web of Conferences, 133, p. 07001. Available at: https://doi.org/10.1051/matecconf/201713307001.

Ivanova, Y. (2017b) "Modelling the impact of cyber attacks on the traffic control centre of an urban automobile transport system by means of enhanced cybersecurity," MATEC Web of Conferences, 133, p. 07001. Available at: https://doi.org/10.1051/matecconf/201713307001.

Ivanova, Y. (2019) "Trends in the use of high technology solutions for cybersecurity of critical infrastructure," Godišnik Na Departament Telekomunikacii [Preprint]. Available at: https://doi.org/10.33919/ytelecomm.19.6.4.

Kalinin, M.O., Krundyshev, V. and Zegzhda, P.D. (2021) "Cybersecurity Risk Assessment in Smart City Infrastructures," Machines, 9(4), p. 78. Available at: https://doi.org/10.3390/machines9040078.

Kavak, H. (no date) Simulation for Cybersecurity: State of the Art and Future Directions. Available at: https://digitalcommons.odu.edu/vmasc_pubs/56.

Keskin, O.F. et al. (2021) "Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports," Electronics, 10(10), p. 1168. Available at: https://doi.org/10.3390/electronics10101168.

Kim, I.-J. et al. (2022) "Mission-Based Cybersecurity Test and Evaluation of Weapon Systems in Association with Risk Management Framework," Symmetry, 14(11), p. 2361. Available at: https://doi.org/10.3390/sym14112361.

Kissoon, T. (2020) "Optimum spending on cybersecurity measures," Transforming Government: People, Process and Policy, 14(3), pp. 417–431. Available at: https://doi.org/10.1108/tg-11-2019-0112.

Koïta, M. et al. (2022) "A generic learning simulation framework to assess security strategies in cyber-physical production systems," Computer Networks, 218, p. 109381. Available at: https://doi.org/10.1016/j.comnet.2022.109381.

Kour, R., Thaduri, A. and Karim, R. (2020) "Predictive model for multistage cyber-attack simulation," International Journal of Systems Assurance Engineering and Management, 11(3), pp. 600–613. Available at: https://doi.org/10.1007/s13198-020-00952-5.

Kuhl (2007) Cyber attack modeling and simulation for network security analysis. Available at: https://ieeexplore.ieee.org/abstract/document/4419720/.

Kuhl, M.E. (2007) "Cyber attack modeling and simulation for network security analysis" (2007a). Available at: https://ieeexplore.ieee.org/document/4419720.

Kuhl, M.E. (2007) "Cyber attack modeling and simulation for network security analysis " (2007b). Available at: https://ieeexplore.ieee.org/abstract/document/4419720/.

Kuhl, M.E. (2007) "Cyber attack modeling and simulation for network security analysis" (2007c). Available at: https://ieeexplore.ieee.org/abstract/document/4419720/.

Kuzmenko, O.V. (2021) Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system. Available at: https://essuir.sumdu.edu.ua/handle/123456789/85701.

Lee, D. et al. (2021) "Cy-Through: Toward a Cybersecurity Simulation for Supporting Live, Virtual, and Constructive Interoperability," IEEE Access, 9, pp. 10041–10053. Available at: https://doi.org/10.1109/access.2021.3051072.

Lee-Urban, S. et al. (2016) "Two Complementary Network Modeling and Simulation Approaches to Aid in Understanding Advanced Cyber Threats," Advances in Intelligent Systems and Computing [Preprint]. Available at: https://doi.org/10.1007/978-3-319-41932-9_33.

Levy, Y. and Gafni, R. (2021) "Introducing the concept of cybersecurity footprint," Information & Computer Security, 29(5), pp. 724–736. Available at: https://doi.org/10.1108/ics-04-2020-0054.

Lippmann, R.P., Ingols, K.W. and Lab, M.I. of T.L.L. (no date) An Annotated Review of Past Papers on Attack Graphs, DTIC. Available at: https://apps.dtic.mil/sti/citations/ADA431826.

Mabie, D. and Schuster, D. (2020) "Lessons Learned in Leveraging Existing Simulations for Cybersecurity Training, Evaluation, and Research," Proceedings of the Human Factors and Ergonomics Society ... Annual Meeting, 64(1), pp. 425–429. Available at: https://doi.org/10.1177/1071181320641095.

Mąkosa, G. (2021) "Risk management as a determinant of cybersecurity," Nowoczesne Systemy Zarządzania, 14(3), pp. 67–80. Available at: https://doi.org/10.37055/nsz/132731.

Mbanaso, U.M. (2019) Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. Available at: https://doaj.org/article/22542d6394a8404682fc4945c0e6d65d.

Merad, M. and Trump, B.F. (2020) Expertise Under Scrutiny, Risk, systems and decisions. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-20532-4.

Miller, S. et al. (2016) "Modelling Cyber-Security Experts' Decision Making Processes using Aggregation Operators," arXiv (Cornell University) [Preprint]. Available at: https://doi.org/10.48550/arxiv.1608.08497.

Milov, O. et al. (2019) "Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems," Eastern-European Journal of Enterprise Technologies, 2(9 (98)), pp. 56–66. Available at: https://doi.org/10.15587/1729-4061.2019.164730.

Rasche, G., Allwein, E., Moore, M., (2007), Model-Based Cyber Security (2007). Available at: http://ieeexplore.ieee.org/document/4148957.

Moreira, F. et al. (2021) "Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology," IEEE Access, 9, pp. 129605–129618. Available at: https://doi.org/10.1109/access.2021.3113178.

O'Neill, P. (2013) Protecting Critical Infrastructure by Identifying Pathways of Exposure to Risk. Available at: https://doaj.org/article/bdf9af02d19c4f1aa682f1ea44657888.

Holm, H., Shahzad, K., Buschle, M., (2015) P2 CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language (no date). Available at: https://ieeexplore.ieee.org/document/6990572.

Holm, H., Shahzad, K., Buschle, M., (2015) Quantifying & minimizing attack surfaces containing moving target defenses (2015). Available at: http://ieeexplore.ieee.org/document/7287449.

Rahmani, K.R. et al. (2022) "Lightweight Cyber Security for Decision Support in Information Security Risk Assessment," European Journal of Electrical Engineering and Computer Science, 6(1), pp. 24–31. Available at: https://doi.org/10.24018/ejece.2022.6.1.391.

Razikin, K. and Soewito, B. (2022) "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," Egyptian Informatics Journal, 23(3), pp. 383–404. Available at: https://doi.org/10.1016/j.eij.2022.03.001.

Roldán-Molina, G. (2017) A Decision Support System for Corporations Cybersecurity Management. Available at: http://hdl.handle.net/2086/15670.

Salin, H. (2022) Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams. Available at: http://urn.kb.se/resolve?urn=urn:nbn:se:ltu:diva-90199.

Șandor, A., Tont, G. and Simion, E. (2022) "A Mathematical Model for Risk Assessment of Social Engineering Attacks," TEM Journal, pp. 334–338. Available at: https://doi.org/10.18421/tem111-42.

Sasai, K. et al. (2022) "Multiagent-Based Data Presentation Mechanism for Multifaceted Analysis in Network Management Tasks," Sensors, 22(22), p. 8841. Available at: https://doi.org/10.3390/s22228841.

Wang, Y., Lin, C., Wang, Y., (2009) Security Analysis of Enterprise Network Based on Stochastic Game Nets Model (2009). Available at: http://ieeexplore.ieee.org/document/5199442/.

Yusuf, S.E., Mengmeng, G., Hong, Jin B., (2016) Security Modelling and Analysis of Dynamic Enterprise Networks (2016). Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7876345.

Shaikh, F.A. and Siponen, M. (2022) "Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity," Computers & Security, 124, p. 102974. Available at: https://doi.org/10.1016/j.cose.2022.102974.

Nicol et. Al., (2003), Simulation of large scale networks using SSF (2003). Available at: http://ieeexplore.ieee.org/document/1261480/.

Cermak, M., (2022), SoK: Applications and Challenges of using Recommender Systems in Cybersecurity Incident Handling and Response (no date). Available at: https://is.muni.cz/publication/1860604.

Tagarev, T. (2020) "Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives," Future Internet, 12(4), p. 62. Available at: https://doi.org/10.3390/fi12040062.

Thompson, B.J. and Morris-King, J. (2018) "An agent-based modeling framework for cybersecurity in mobile tactical networks," The Journal of Defense Modeling and Simulation, 15(2), pp. 205–218. Available at: https://doi.org/10.1177/1548512917738858.

Vulnerability Modelling for the Analysis of Network Attacks (2008). Available at: http://ieeexplore.ieee.org/document/4573035/.

Wang, J.-L. and Neil, M. (2021) "A Bayesian-network-based cybersecurity adversarial risk analysis framework with numerical examples," arXiv (Cornell University) [Preprint]. Available at: https://doi.org/10.48550/arxiv.2106.00471.

Wiig, K. M. (1999). Comprehensive knowledge management., Available at: http://www.krii.com/downloads/comprehensive_km.pdf

Woodard, M. et al. (2021) "Survivability evaluation and importance analysis for cyber–physical smart grids," Reliability Engineering & System Safety, 210, p. 107479. Available at: https://doi.org/10.1016/j.ress.2021.107479.

APPENDIX A

In the academic field, decision making refers to the process of selecting a course of action from a set of alternatives based on certain criteria or objectives. The process typically involves identifying the problem or decision to be made, gathering, and analysing information, evaluating alternatives, and choosing the best course of action. Decision making is a complex process that involves considering multiple factors, such as risk, uncertainty, and trade-offs, and can be influenced by cognitive and behavioural biases. In general, the decision support systems are designed to help decision-makers to make better decisions by providing them with the necessary data, analysis, and information to decide. Decision support refers to the use of technology, tools, and techniques to assist in the decision-making process. Decision support systems (DSS) are computer-based systems that provide information and support for decision-making activities. DSS can be used to automate parts of the decision-making process, such as data collection and analysis, and can also provide visualizations, models, and other forms of information to help decision makers understand and evaluate the decision situation. DSS can help decision makers to make more informed decisions by providing them with the necessary data, analysis, and information to plan. Three levels of decisions are illustrated in organisations. Each type of decision has very specific characteristics that allow it to be identified. First, there is the level of scientific constraints in the decision-making process. It can be weak, intermediate, or strong. Secondly, there is the scope of impact of the decision. It can be local, regional, national, or wider. Finally, there is the content of the information. This can be very specific, intermediate, or more general. According to the positioning of these three indicators, it is possible to group decisions into three main groups: strategic decisions, which have a very broad impact, leave little room for the scientific dimension, and are based on global information. Then there are tactical decisions, which have a smaller impact, leave an intermediate place to the scientific dimension, and are based on more precise and more restricted information than strategic decisions. Finally, there are operational decisions, which are the opposite of strategic decisions. This means that they have a very limited impact and are based on very specific and precise information, where the scientific dimension is essential. The levels of decision are also discussed in complexity theory by Wiig, K. M. (1999).

As for the definition of risk management, we refer to it through the risk management cycle proposed by Merad and Trump (2020) The authors propose four distinct risk management phases, which are distinguished according to two parameters. Three phases are positioned upstream of the crisis (or feared event), and one post-crisis. Firstly, the exemption phase, which is characterised by an unknowable risk, no historical event allows us to suspect a hazard (H) greater than 0, and the phenomenological uncertainty linked to the event is total. This is followed by the precautionary phase. In the precautionary phase, the hazard (H) may still be 0 in the absence of historical events, however phenomenological events reduce the uncertainty of the existence of a risk. The risk is suspected but not proven. Then, whether the phenomenological elements confirm the certainty of the risk of crisis, historical elements

with an increasing hazard (H) indicate that the risk is proven. We are then in the prevention phase, it is now a question of reducing the stakes and the threats, which will be produced by the increasing hazard (H). If, however, the feared event occurs, then we switch to the last phase, that of recovery. The distinction between the recovery phase and the prevention phase is not only based on the temporality in relation to the crisis, or on the two parameters of hazard (H) and phenomenology, but also on the degree of information available. We will look at the latter later. It is important to note that any organisation can be in different phases for different risks simultaneously. Behind this relatively simple model lies a much greater complexity and subtlety that is more difficult for risk managers to instrument, especially cyber risk. For example, it is difficult to say whether a zero-day vulnerability, i.e., one that is unknown to the publisher of the targeted software or component, is to be placed in the exemption zone (total uncertainty) or in the precautionary zone (phenomenology, we know that this type of event can occur, but we have no information on the vulnerability). This means that the model is not sufficient. It is also necessary to qualify the information and the uncertainty.

The decisions taken can be reflected at different levels, and on multiple stage of the risk management cycle, and organizations that must make decisions for IT and cyber risk management are no exception. For example, consider strategic decisions: for the 'long cycle' of the organisation, i.e., its tasks and substantive changes, this type of decision is applicable. Indeed, if we analyse these decisions via the angle defined here: the risk is proven (small attacks/attempts take place every day, directly or indirectly targeting the organisation), and we must operate so that the feared event of the long cycle (i.e., a large-scale cyber-attack seriously damaging the issues defined as those of the information system) does not occur. So we are in a situation that carries the attributes of strategic decision-making: international, low granularity of information, implementation of large-scale risk management policies. A CISO might take the decision to deploy a common master image on all PCs in the organisation to facilitate the management of the fleet to keep it safe. In parallel, the organisation (and this refers to our observation on the risk management life cycle: the organisation may be in several phases at the same time) is also required to make tactical decisions. For example, when the decision to implement large-scale policies is taken by a team dedicated to cybersecurity (e.g., deployment of a specific security solution on a specific type of equipment, but on a large scale), this decision falls within the tactical domain. Finally, we could also find the organisation in pure operational decision making. In these situations, we observe that the decision making is done by people with a similar level of expertise (e.g., within a cyber security team). These decisions are made every day to solve very specific problems on a scientific basis. For example, in the qualification of an incident, or in the audit of a specific IT configuration.

Finally, it should be noted that decisions of a certain type are not directly linked to a phase of the risk management cycle, although this may seem counter intuitive. For example, when a cybersecurity team conducts its daily operations of patching and hardening systems, the organisation is then positioned in the precautionary phase of the cycle: the risk of exploitation by a malicious actor is suspected. However, daily operations can also take place in the exoneration phase. This is particularly the case when groups of attackers exploit so-called zero-days vulnerabilities. Although the position in the cycle is not specific to one type of decision, it seems that some organisations, because of their structure and therefore the characterisation of decisions, but also by the level of uncertainty they face, are more likely to be always on one side or the other of the cycle. Institutions that use proprietary technologies and/or are particularly targeted by highly sophisticated malicious actors are more likely to be in the exemption phase than the average company. It would therefore seem that in order to correctly interpret an organisation's position in the cycle, and to deduce the appropriate risk management methodology, it is necessary to take into account the information shared with its environment, as this makes it possible to discriminate between the exemption and precautionary phases, but also the information shared internally and the type of decision resulting from it (according to the criteria for discriminating between decisions), as this makes it possible, for example, to delimit the prevention phase and the precaution phase. Most decisions that are taken in the precautionary and prevention phase are made in an uncertain environment, however, in the recovery phase, the information system operators are often in the most advanced knowledge phase, if resilience measures have been applied. Therefore, one of the problems of crisis/resilience management

is the ability of the organisation to move out of the uncertain environment and rely on known elements. For example, during the reconstruction of the IS with the replication times, supplier contracts, etc. This provides us with a representation of the uncertain according to two parameters, namely the exhaustiveness of the information and its completeness. Thus, it is based on 16 criteria related to the notions of risk management as defined by Merad and Trump (2020) that we have carried out our model analysis. The 16 criteria used are directly derived from the elements discussed above (e.g., phase of the cycle, type of decision) or are derived from them.

APPENDIX B

Article Title	*Source*	Exoneration	Precaution	Prevention	Recovery	Strategic	Tactical	Operational	Significant data needs	Intermediary data needs	Low data needs	Contextual analysis	Risk Identification	Risk Evaluation	Risk Prioritisation	Risk Tolerance measure	Mitigation plan
Exploitability analysis using predictive cybersecurity framework			x	x				x		x			x	x	x		
Novel Architecture for Predictive CyberSecurity Using Non-homogenous Markov Models	https://ieeexplore.ieee.org/document/7345354		x	x				x		x			x	x	x		
A Predictive Framework for Cyber Security Analysis Using Attack Graphs	https://arxiv.org/ftp/arxiv/papers/1502/1502.01240.pdf		x	x			x	x		x			x	x	x		
Intelligent, Automated Red Team Emulation	https://doi.org/10.1145/2991079.2991111 https://calders.mitre.org/			x			x			x			x	x			
Simulating Cyber Attacks, Defences, and Consequences	https://www.sciencedirect.com/science/article/pii/S0167404899801151		x	x		x	x			x				x	x		
Development of a Cyber Attack Simulator for Network Modeling and Cyber Security Analysis	https://scholarworks.rit.edu/cgi/viewcontent.cgi?https=redir			x				x		x			x				
CyberVis: Visualizing the Potential Impact of Cyber Attacks on the Wider Enterprise	https://ieeexplore.ieee.org/document/6698979			x	x		x	x	x			x	x	x	x		
Categorizing Threat: Building and Using a Generic Threat Matrix	https://www.energy.gov/sites/default/files/oeprod/Documen		x	x		x	x			x		x		x	x		
Anomaly-based network intrusion detection: Techniques, systems and challenges	https://www.sciencedirect.com/science/article/pii/S0167404808000692			x				x	x	x	x			x			
P2 CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language	https://ieeexplore.ieee.org/document/6990572		x	x	x				x			x	x	x	x		x
What Vulnerability Do We Need to Patch First ?	https://ieeexplore.ieee.org/document/6903625		x	x	x			x	x	x					x		
Cyber attack modeling and simulation for network security analysis	https://ieeexplore.ieee.org/document/4419720		x	x			x			x				x	x		
Two Complementary Network Modeling and Simulation Approaches to Aid in Understanding Advanced Cyber Threats	https://link.springer.com/chapter/10.1007/978-3-319-41932-9_33			x			x	x	x	x				x			
Evaluating and Strengthening Enterprise Network Security Using Attack Graphs	https://www.11.mitedu/mission/cybersec/publications/publ		x	x				x		x		x	x	x	x		
Vulnerability Modelling for the Analysis of Network Attacks	http://ieeexplore.ieee.org/document/4573035/			x				x		x				x	x		
Simulation of large scale networks using SSF,	http://ieeexplore.ieee.org/document/1261480/		x					x	x				x	x			
Model-based risk assessment for cyber physical systems security	http://ieeexplore.ieee.org/document/4148957			x				x	x			x	x				
"Quantifying & minimizing attack surfaces containing moving target defenses"	http://ieeexplore.ieee.org/document/7287449		x	x				x	x	x			x	x	x	x	x
Integrated Metamodel for Security Analysis,	http://ieeexplore.ieee.org/document/7070437		x	x			x	x	x	x			x	x	x		
Security Analysis of Enterprise Network Based on Stochastic Garne Nets Model,	http://ieeexplore.ieee.org/document/5199442/			x			x	x		x					x		
Using Bayesian networks for cyber security analysis	http://ieeexplore.ieee.org/document/5544924/		x	x				x	x	x				x	x		
Security Modelling and Analysis of Dynamic Enterprise Networks	http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=78		x	x				x	x	x				x	x		
A Mathematical Model for Risk Assessment of Social Engineering Attacks	https://doi.org/10.18421/TEM111-42			x			x	x			x		x	x	x		
An agent-based modeling framework for cybersecurity in mobile tactical networks	https://doi.org/10.1177/1548512917738858		x				x		x					x			
Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems	https://doi.org/10.15587/1729-4061.2019.164730			x			x	x	x						x		
Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system (2021)	https://essuir.sumdu.edu.ua/handle/123456789/85701		x	x			x		x					x	x		
Predictive model for multistage cyber-attack simulation	https://link.springer.com/article/10.1007/s13198-020-00952-5			x				x		x				x			
Simulation Model of a Fuzzy Cyber Attack Detection System	https://dx.doi.org/10.5281/zenodo.7247963			x				x	x				x	x			
Mission-Based Cybersecurity Test and Evaluation of Weapon Systems in Association with Risk Management Framework	https://doi.org/10.3390/sym14112361			x			x	x		x		x	x	x	x	x	x
A generic learning simulation framework to assess security strategies in cyber-physical production systems (2022-12-09)	https://hal.archives-ouvertes.fr/hal-03863682			x				x		x				x			x
Modelling the impact of cyber attacks on the traffic control centre of an urban automobile transport system by means of enhanced cybersecurity	https://doi.org/10.1051/matecconf/201713307001			x			x		x					x			x
A Review of Critical Infrastructure Protection Approaches: Improving Security through Responsiveness to the Dynamic Modelling Landscape	https://dx.doi.org/10.48550/arxiv.1904.01551	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
Protecting Critical Infrastructure by Identifying Pathways of Exposure to Risk	https://doaj.org/article/bd9af02d19c4f1aa682f1ea448578		x	x			x	x	x			x	x	x			
Trends in the use of high technology solutions for cybersecurity of critical infrastructure	https://dpi.nbu.bg/index.php/YT/article/view/339			x			x			x				x			
T3SF (Technical Tabletop Exercises Simulation Framework)	https://dx.doi.org/10.5281/zenodo.7247963			x			x		x					x	x		x
A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs	http://hdl.handle.net/11573/1554749		x			x	x		x			x		x			
On Aggregation and Prediction of Cybersecurity Incident Reports	https://doi.org/10.1109/ACCESS.2021.3097834		x					x	x					x	x		
Simulation-Based Cyber Data Collection Efficacy	https://dx.doi.org/10.48550/arxiv.1905.09336		x					x		x				x			
The protoscience of cybersecurity	https://dx.doi.org/10.1177/1548512917737635	NA	NA	NA	NA	x			NA	NA	NA	NA	NA	NA	NA	NA	
Lessons Learned in Leveraging Existing Simulations for Cybersecurity Training, Evaluation, and Research	https://dx.doi.org/10.1177/1071181320641095		x	x			x		NA	NA	NA	x					
Simulation for Cybersecurity: State of the Art and Future Directions	https://digitalcommons.odu.edu/vmasc_pubs/56			x			x	x	x					NA	NA		
Cy-Through: Toward a Cybersecurity Simulation for Supporting Live, Virtual, and Constructive Interoperability	https://doi.org/10.1109/ACCESS.2021.3051072			x				x	x					x	x		
Augmented Probability Simulation Methods for Non-cooperative Games	https://dx.doi.org/10.48550/arxiv.1910.04574		x	x				x	x					x			
Simulation of Attacker Defender Interaction in a Noisy Security Game	https://dx.doi.org/10.48550/arxiv.2212.04281			x				x	x					x	x		x
A Bayesian-network-based cybersecurity adversarial risk analysis framework with numerical examples	https://dx.doi.org/10.48550/arxiv.2106.00471		x	x				x		x				x	x		x
Cybersecurity data science: an overview from machine learning perspective	http://hdl.handle.net/1959.3/456449	NA	NA	NA	NA	NA	x	NA	NA	NA	NA	NA	NA	NA	NA	NA	
Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment	https://doi.org/10.37055/nsqi/132731		x			x				x		x	x	x		x	
Cybersecurity Risk Assessment in Smart City Infrastructures	https://doi.org/10.3390/machines9040078			x				x	x					x	x		
A Decision Support System for Corporations Cybersecurity Management	http://hdl.handle.net/2086/15670		x				x	x				x		x	x		
Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams	http://urn.kb.se/resolve?urn=urn:nbn:se:ltu:diva-90199		x					x		x				x			x
Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports	https://doi.org/10.3390/electronics10101168		x				x					x	x		x		
Risky business: Fine-grained data breach prediction using business profiles			x				x			x				x	x		
Multicriteria decision framework for cybersecurity risk assessment and management	http://rt.nure.ua/article/view/245207			x			x			x				x			
Information Security Risk Assessments following Cybersecurity Breaches : The Mediating Role of Top Management Attention to Cybersecurity	http://urn.fi/URN:NBN:fi:jyu-202211015055		x			x	x					x	x				
CYBERSECURITY COSTS IN AN ENTERPRISE UNIT	https://econjournals.sgh.waw.pl/EEM/article/view/2353		x				x					x	x				
Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems	https://doi.org/10.3390/app11083678			x			x		x					x			
Introducing the concept of cybersecurity footprint	https://dx.doi.org/10.1108/ics-04-2020-0054																
Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management	https://dx.doi.org/10.48550/arxiv.1707.02653			x			x			x	x			x			
Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity	https://doaj.org/article/7b2d5bc4f5d44ddc8fc5cd5a0adce8c4			x				x		x				x	x		
Developing Security Assurance Metrics to Support Quantitative Security Assurance Evaluation	https://hdl.handle.net/11250/3041939			x			x	x		x				x	x		
A data-driven approach to cyber risk assessment	http://hdl.handle.net/11566/269582			x		x			x					x		x	
Security Events and Vulnerability Data for Cybersecurity Risk Estimation	http://hdl.handle.net/11572/197812		x				x		x					x	x		
MAGIC: A Method for Assessing Cyber Incidents Occurrence	http://hdl.handle.net/11566/304519		x	x		x	x		x					x	x		
Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework	https://doaj.org/article/c225420d394a8404682fc4945c0e6d65d			x			x	x		x					x	x	
Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology	https://doi.org/10.1109/ACCESS.2021.3113178			x				x			x			x			
Optimum spending on cybersecurity measures	https://dx.doi.org/10.1108/bfp-11-2019-0112			x		x	x			x				x	x	x	
Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives	https://doi.org/10.3390/f12040062		x				x			x			x	x	x		
Technical threat intelligence analytics: what and hw to visualize for analytic process	http://ktu.lub.lt/KTU:ELABAP087089929&prefLang=en_US		x	x				x	x					x			
Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework	https://doi.org/10.1016/j.eij.2022.03.001			x			x	x				x	x	x	x		
Multiagent-Based Data Presentation Mechanism for Multifaceted Analysis in Network Management Tasks	https://doi.org/10.3390/s22228841		x					x	x				x	x			
Big Data Analytics Architecture for Cybersecurity Applications	https://doaj.org/article/f8e49bbf7f66d122acc417a9a8734dfc			x				x	x				x	x			
Towards effective cybersecurity resource allocation:the Monte Carlo predictive modelling approach	https://hdl.handle.net/19830/asf16e7-1a35-4c32-a5e2-adb268dc8d70			x			x			x				x	x		
SoK: Applications and Challenges of using Recommender Systems in Cybersecurity Incident Handling and Response	http://ktu.lub.lt/KTU:ELABAP087089929&prefLang=en_US			x				x	x						x		
An Options Approach to Cybersecurity Investment	https://doi.org/10.1109/ACCESS.2017.2773366		x				x			x				x			
Lightweight Cyber Security for Decision Support in Information Security Risk Assessment (2022)	https://dx.doi.org/10.24018/ejece.2022.6.1.391		x	x				x			x			x	x		
A Comparison of Cybersecurity Risk Analysis Tools	http://hdl.handle.net/2086/15669			x				x			x				x		
Adaptive decision support systems for cyber security	http://repository.kpi.kharkov.ua/handle/KhPI-Press/42931			x				x	x					x	x		
Designing a decision support system for the weakly formalized problems in the provision of cybersecurity	http://journals.uran.ua/eejet/article/view/90506			x				x		x			x				
Modelling Cyber-Security Experts' Decision Making Processes using Aggregation Operators	https://doi.org/10.48550/arxiv.1608.08497		x	x				x		x			x				