Jyrki Isokangas

STRATEGIC CYBERSECURITY ANALYSIS

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2021

ABSTRACT

Isokangas, Jyrki
Strategic Cybersecurity Analysis
Jyväskylä: University of Jyväskylä, 2021, 93 pp.
Cybersecurity, Master’s Thesis
Supervisor: Kari, Martti J.

The generally accepted assumption is that offensive actions have an advantage in cyberspace, and the defender’s role is to react. Insecure cyberspace is taken as a default state. Furthermore, cybersecurity is no longer a purely technical discipline but evolving towards a strategic and geopolitical concept, also impacting national security. Reactive and purely technical cybersecurity is not valid anymore. The advantage of an attacker should be changed to the defender. The task is challenging, but it may be achieved with strategic analysis supporting proactive cybersecurity decisions. The objective of this master’s thesis is to determine what means strategic cybersecurity analysis and how the results of the analysis can be utilized in cybersecurity development. The approach is practical, presenting a model for the analysis. The research strategy is based on constructive research, aiming to produce an innovative construction for cybersecurity analysis. The research utilizes a qualitative research methodology with an abductive approach. The deductive part of the research is based on the theories of ontology and threat ontology. The construction of the model is executed inductively, and the data analysis is based on template analysis. The strategic cybersecurity analysis model includes a cyber threat, a target system, cyberspace and interaction of all these elements. The entities are categorized into subclasses in the model, identifying their parts, qualities, processes, and locations. The last phase of the analysis focuses on the interaction of the cyber threat, the target system and cyberspace, providing an in-depth understanding of how these entities impact each other. The presented analysis model results should provide knowledge on designing and developing own cybersecurity in the future. The utilized dynamic spatial ontology theory supported analyzing the spatial (actors) and temporal entities (their processes) separately. The threat ontology supported identifying a threat, a target and the environment, and cyberspace. The model is threat-based and focuses on future adversaries, own cybersecurity controls and cyberspace. It can reveal the most likely cyber threats, their intentions, capabilities, and available opportunities. Furthermore, it identifies the required future cybersecurity capabilities for proactive cybersecurity and, eventually, gaining an advantage. Due to the practical approach, the results of this research are not comprehensive to determine strategic cybersecurity analysis from every possible angle. Therefore, this research should be considered a step towards increased understanding of cybersecurity in a strategic context. Every step of this model constitutes a viable topic for future research.

Keywords: cybersecurity, strategic, analysis, decision-making, constructive research

TIIVISTELMÄ

Isokangas, Jyrki
Strategic Cybersecurity Analysis
Jyväskylä: Jyväskylän yliopisto, 2021, 93 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Kari, Martti J.

Kyberturvallisuudessa hyökkääjällä on oletuksena etulyöntiasema ja puolustajan tehtävänä on lähinnä reagoida. Lisäksi kybertilan turvattomuus on yleisesti hyväksytty tosiasia. Kyberturvallisuutta ei voida pitää enää pelkästään teknisenä haasteena, vaan sillä on entistä suurempi strateginen ja geopoliittinen rooli, sekä vaikutus jopa kansalliseen turvallisuuteen. Pääosin reagoiva ja tekninen kyberturvallisuus ei kykene vastaamaan edessä oleviin haasteisiin. Hyökkääjän etulyöntiasema tulisi saada siirrettyä puolustajalle. Tavoite on haastava, mutta se voi olla saavutettavissa strategisella analyysillä, joka kykenee tukemaan ennakoivaa kyberturvallisuuden päätöksentekoa. Tämän pro gradu -tutkimuksen tavoitteena on määritellä mitä tarkoittaa strateginen kyberturvallisuuden analyysi, ja miten analyysin tuloksia voidaan hyödyntää kyberturvallisuuden kehittämistä koskevassa päätöksenteossa. Tutkimus perustuu konstruktiiviseen tutkimusstrategiaan, ja tavoitteena on tuottaa kyberturvallisuuden strategisen analyysin malli tunnistetun ongelman ratkaisemiseksi. Kyseessä on laadullinen tutkimus, jonka deduktiivinen vaihe perustuu ontologian ja uhkan ontologian teorioihin. Kyberturvallisuuden analyysin malli on muodostettu induktiivisesti, ja data on analysoitu käyttäen mallien analyysiä (template analysis). Kyberturvallisuuden strategisen analyysin malli käsittää kyberuhkan, kohteena olevan informaatiojärjestelmän, kybertilan sekä kaikkien näiden vuorovaikutuksen. Toimijat luokitellaan alaluokkiin, jotta niiden osat, ominaisuudet, prosessit ja sijainnit kyetään tunnistamaan. Mallin viimeinen vaihe keskittyy kyberturvallisuuden toimijoiden vuorovaikutukseen, tuottaen syvällistä tietoa toimijoiden vaikutuksista toisiinsa. Analyysin avulla saavutettu ymmärrys luo edellytykset tietoon perustuvaan päätöksentekoon oman kyberturvallisuuden kehittämiseksi. Vaikka tutkimuksessa käytetyt teoriat eivät ole kyberturvallisuuden alalta, ne tukevat hyvin kyberturvallisuuden toimijoiden tunnistamista ja analyysia. Muodostettu malli on uhkaperustainen, ja se keskittyy tulevaisuuden uhkiin, kyberturvallisuuteen ja kybertilaan. Sen avulla kyetään arvioimaan todennäköisimmät kyberuhkat, sekä tunnistamaan oman kyberturvallisuuden kehittämistarpeet. Nämä mahdollistavat ennakoivan päätöksenteon, ja ehkä jopa etulyöntiaseman saavuttamisen. Käytännöllisestä lähestymistavasta johtuen, tutkimus ei ole kokonaisvaltainen kuvaus strategisesta kyberturvallisuuden analyysistä, vaan enemmänkin askel kohti kyberturvallisuuden ymmärtämistä osana strategista kokonaisuutta. Esitetyn analyysimallin jokainen vaihe mahdollistaa oman jatkotutkimuksensa.

Asiasanat: kyberturvallisuus, strateginen, analyysi, päätöksenteko, konstruktiivinen tutkimus

I wish to acknowledge the support provided by Suomalaisen Strategisen Tutkimuksen ja Seurannan Tukisäätiö (STRATU) for this research.

FIGURES

TABLE OF CONTENTS

1 GAINING THE ADVANTAGE

1.1 Motivation and research questions

The generally accepted assumption is that offensive actions have an advantage in cyberspace, and the defender's role is to react. There are probably several reasons for this situation. In cyberspace, any attacker can have several options for penetrating the target system; one individual can possess a capability to disable a whole infrastructure; the source of an attack is difficult to determine; the domain itself is continuously changing and global. Likewise, the processes and practices in cybersecurity are mainly based on the information security traditions, where the threat is determined based on the own system vulnerabilities. There are likely numerous other reasons why the offensive actions have the advantage.

The situation is challenging and can become intolerable in the future. Currently, cyberspace is charged with malicious behaviour, like crime, harassment, denial of service, hostile information collection, information manipulation and near war-like activities, among other things. Numerous actions have been introduced to increase cybersecurity, but eventually, insecure cyberspace is accepted as a default state. In a worst-case scenario, cyberspace will not support the desired objectives of individuals, companies or nations. The solution is simple; change the advantage from offensive actions to defence. Unfortunately, the execution is more complicated than the solution. Secure cyberspace requires that the cyberattacks are challenging to execute; attacks require vast resources gaining limited results and include a significant risk. In many cases, the primary cybersecurity solution has traditionally been a technical one.

The role of cybersecurity is changing. Geers (2011) argues that cybersecurity has evolved from a purely technical discipline to a strategic and geopolitical concept, impacting even national security (Geers, 2011). Sigholm and Bang (2013) emphasize that the role of state-affiliated groups has increased in cyberattacks. These groups are not interested in short-term financial gain. Their objective is to support national interests by gaining access to military or otherwise classified information regarding research and innovation, trade, and technology (Sigholm & Bang, 2013). Regardless of the perspective, cybersecurity includes always the challenge of an appropriate balance between the positive aspects, security costs and risks of cyberspace (Kramer, 2009).

Information security provides the basis for the technical aspect of cybersecurity. At the other end of the line exists strategic cybersecurity. The first one is focused on details, the latter on the societal and national aspects of cybersecurity. Presumably, gaining an advantage in cyberspace will eventually require also technical capabilities. However, to invent, develop and use the right skillsets to enhance cybersecurity, a strategic understanding of the threat, target and cyberspace itself are required.

The objective of this master's thesis is to determine what means strategic analysis of cybersecurity and how the analysis can be utilized in developing cybersecurity.

The research questions are:

- What means strategic analysis of cybersecurity?
    - What are the actors and their relations affecting security in cyberspace?
    - How can the actors, their activities and cyberspace categorized and analyzed?
    - What is included in the analysis process?
    - What are the results of the analysis, and how they can be utilized?

1.2 Research methods

This type of exploratory research aims to find new perspectives examining insufficiently comprehended phenomena (Hirsjärvi, Remes & Sajavaara, 2009). Even if information security and cybersecurity are well researched, the approach typically emphasizes the technical side. The strategic dimension of cybersecurity is not well known. This research aims to find new perspectives of cybersecurity, increase the understanding of its strategic impact and enable a proactive approach to cybersecurity.

This research utilizes a qualitative research methodology, and the research strategy is based on constructive research. It creates an innovative construction for cybersecurity analysis to solve practical problems (Lukka, 2003). The approach is abductive. The research begins with a deductive approach, based on theories of ontology and threat ontology. The construction of the strategic cybersecurity analysis model is inductive, based on collected and analyzed data. The data analysis is executed based on theory-related content analysis using templates. A template analysis includes a list of categories representing the themes revealed from the collected data. Data collection, analysis and the construction of the model were closely intermingled. The analysis guided the data collection and the construction of the model, making the whole process interactive. The primary sources of the research were information security, risk management, ontology, intelligence, and military planning and wargaming literature.

The reliability and validity of the research constituted a significant challenge. The researcher aimed to solve the challenge utilizing relevant theories, obtaining sources from different disciplines, constantly triangulating material, comparing data to theory and utilizing inter-coder reliability. Furthermore, the researcher used content and construct validation. Lastly, the researcher described the research methods and process as detailed as possible. The description of the research methods can be found in chapter 2.

1.3 Main results

The approach to the research objectives is practical. Strategic cybersecurity analysis is described based on the constructed analysis model. The description also includes the rationale behind the construction, defining the phenomenon. Strategic analysis means focusing on future cybersecurity. The objective is to provide reliable and valid information that support timely decisions regarding own cybersecurity design, development and deployment. The key element of the analysis is a threat. Without a cyberthreat, cybersecurity remains uncompromised. On the other hand, a threat constitutes a threat only when it has a target to interact in cyberspace. Therefore, the strategic analysis model is threat-based, and it includes a cyber threat, a target system, cyberspace, and their interaction. (see Little & Rogova, 2006.)

The analysis model identifies future threats, own information systems and cybersecurity control development, and the changes taking place in future cyberspace. These elements are divided into detailed parts, including their internal and external relations. Eventually, these detailed and subdivided elements are combined with the construct that enables the analysis. The main challenge in the process is data and information collection. However, the strategic cybersecurity model supports identifying the elements where the data must be collected, and the type of data required in the analysis. Furthermore, the model supports identifying concealed information. Identifying any of the elements, their characteristics, processes, or spatio-temporal locations can reveal the other related but currently hidden elements.

This model does not provide a panacea for increased cybersecurity. However, it may help to construct and classify the phenomenon. It can reveal the most likely cyber threats, their intentions, capabilities, and available opportunities. It can also reveal what kind of value own information systems present as a target, identify own cybersecurity controls and how they operate. Furthermore, the model enables identifying own intentions, capabilities and opportunities of cybersecurity. The analysis can provide an understanding of cyberspace development. It can indicate the ways to modify cyberspace to increase own capabilities and decrease adversary's opportunities. The interaction analysis can provide a profound understanding of how the different elements conflict in cyberspace and provide a rich description of cybersecurity for the decision-makers.

This research answers all the research questions. However, the results are not comprehensive enough to determine strategic cybersecurity analysis from every possible angle, and they cannot fully define the content of strategic cybersecurity analysis. This research can be considered as a step towards increased understanding of cybersecurity in a strategic context. This research aims to broaden the approach of cybersecurity. It aims to perceive cybersecurity as a strategic phenomenon. Cyberthreats, target systems, and cyberspace might be significant entities by themselves, but they are even more interesting as part of the larger strategic influencing. This model supports the analysis of cybersecurity. However, it can be used in cybersecurity analysis also in a broader context of a threat landscape.

For future research, every step of this model constitutes a viable topic for further examination. Furthermore, examining this model as part of cybersecurity decision-making would provide increased knowledge about the feasibility of the model. The strategic analysis of cybersecurity is one tool for proactive decision-making. Future research should also identify other elements of decision-making supporting proactive cybersecurity.

1.4 Terminology

According to the Merriam Webster Dictionary (2020), analysis means studying a complex phenomenon for understanding the nature or the essential characteristics of it. Analysis can also mean dividing a whole into smaller components, separating a whole into its parts, or identifying ingredients of a substance. Analysis can also mean writing a report of a study (Merriam-Webster, 2020). Heuer (1999) argues that the essence of analysis is to divide a problem into its components, assess each part separately, and then combine them to reach a decision (Heuer, 1999).

A strategy is the science and art of employing political, economic, psychological, and military forces of a nation to afford the maximum support to adopted policies. A strategy can include management, knowledge and skills to achieve an advantage over the opponent. A strategy is the art of devising or employing plans toward a goal. Anything strategic is something of great importance within an integrated whole. It is also essential for accomplishing the required effect. (Merriam-Webster, 2020) These definitions apply mainly to the nation-states and the institutions of the countries. In the corporate world, strategy defines the business areas where a company will compete, preferably with a competitive advantage. The strategic level decisions have a long-term impact; they profoundly affect the operations, and they use significant resources of the company. (Andrews, 1997)

Merriam-Webster (2020) describes cybersecurity as measures taken to protect a computer system against unauthorized access or attack (Merriam-Webster, 2020). The Vocabulary of Cybersecurity (2018), published by the Finnish Security Committee, determines cybersecurity as a state where users can trust cyberspace and the operations are secured. Cybersecurity includes actions that allow proactively control and tolerate cyber threats and their impacts. Typically, compromised cybersecurity is a result of an information security threat. In some cases, correcting the disruptions in the physical world require actions in the cyber domain. Cybersecurity is the security of a digitalized and networked society and organization. It supports the security of the operations of different organizations in the cyber domain. (Vocabulary of Cyber Security, 2018) Hundley and Anderson (1995) call protecting government, business, individuals and society from deliberate threats as cyberspace security. Protection against unintentional or accidental threats is called cyberspace safety (Hundley & Anderson, 1995). Both of these dimensions can be included in the currently used term cybersecurity.

Based on the terminology, the strategic analysis of cybersecurity should focus on a complex phenomenon that resides in cyberspace and can cause large-scale effects. The analysis aims to understand the actors, their characteristics, components, features, objectives, relationships and actions in cyberspace. Strategic means understanding the phenomenon and its impacts at a political, economic, military and information domains. The results of cybersecurity analysis should have long-term and extensive effects. The analysis should provide information and knowledge for decision-making, capability design and development, operations and the use of resources. Strategic also determines the level of the analysis. With the strategic analysis of cybersecurity, an organization should gain an advantage over the adversary by anticipating cyber events and preparing accordingly.

1.5 Previous research

The background of strategic cybersecurity analysis exists in information security, especially in risk assessment. Typically, the focus of risk assessment is on information security investments. Due to the quantitative nature of investments, the literature includes several studies on measuring information security allocations, either quantitative, qualitative or combined.

Feng and Li (2011) remind that a quantitative approach considers information security risks as a function of a threat probability and the expected loss. However, they claim that quantitative methods do not support assessing the failure of multiple security controls or multiple threats (Feng & Li, 2011). Lo and Chen (2012) claim that quantitative risk assessment methods require significant resources to collect data of all the relevant elements. Usually, this means that part of the necessary data is unavailable. On the other hand, they remind that qualitative risk assessment methods are based on judgment, intuition, and experience, decreasing reliability (Lo & Chen, 2012). Karabacak and Sogukpinar (2005) remind that quantitative risk analysis uses statistical tools and qualitative analysis adjectives to represent risks. Intensive quantitative measures are not suitable for risk analysis in current information systems. However, qualitative risk analysis depends on individuals participating in the process, and subjective results are possible (Karabacak & Sogukpinar, 2005).

Baskerville (1993) has identified the same challenges, claiming that quantitative methods lack reliable statistical data and require complex matrixes in the process. Improving the quantitative reliability of the analysis can destroy its interpretative validity. From a scientific point of view, risk analysis is an imprecise predictive technique. However, finding a better alternative is a challenge. He approves the use of experts in threat or cost assessment, but eventually, the number of variables means incomplete risk estimation accuracy. However, risk management provides a common discussion channel with the management. (Baskerville, 1991; Baskerville, 1993.)

In the ideal world, cybersecurity investments are based on assessed risks, threats, and vulnerabilities. In real life, they can be based on costs, productivity, or other organizational constraints. Security control selection can also be based on non-monetary, technical, non-technical and social aspects, aiming to optimize several conflicting objectives. (Yevseyeva, Basto-Fernandes, Emmerich & van Moorse, 2015.)

In the strategic analysis, the essential question is identifying the threat, the target system, and assessing their interaction in cyberspace. Information security literature offers several options. Lo and Chen (2012) introduced a hybrid procedure for risk level evaluation. Their approach utilizes experts with diverse professional backgrounds. Furthermore, their model identifies the relationships between risk controls (Lo & Chen, 2012). The risk analysis model presented by De Gusmao, Silva, Silva, Poleto and Costa (2015) utilizes decision theory and fuzzy logic, combining quantitative and qualitative assessment. Their model identifies and evaluates the sequence of attacks to an information system, using scenarios and event trees (De Gusmao, Silva, Silva, Poleto & Costa, 2015). Karabacak and Sogukpinar (2005) introduced an information security risk analysis method for complex information systems, called Information Security Risk Analysis Method (ISRAM). The main difference to other risk analysis methods is that it allows the managers and staff to participate in the process with a survey to identify information security problems (Karabacak & Sogukpinar, 2005).

Cavusoglu, Raghunathan and Yue (2014) claim that decision theory and other traditional risk analysis methods alone are not appropriate for security investment decisions due to the strategic nature of the security problem. Decision theory is applicable in situations where nature is the only opponent. Modelling the interaction between the attacker and defender requires game theory. Their research compared the use of game theory and decision theory in information security investments. (Cavusoglu, Raghunathan & Yue, 2014) Fielder, Panaousis, Malacaria, Hankin and Smeraldi (2014) examined cybersecurity investments based on scenarios and game theory, aiming to optimally allocate cybersecurity resources. Different targets have different weights in their model, but the attacker is unaware of the defender's resources. The model utilizes cybersecurity scenarios, including targets and attacks, but do not identify the interdependencies between the actions (Fielder, Panaousis, Malacaria, Hankin & Smeraldi, 2014).

Feng and Li (2011) presented a model based on a quantitative and qualitative approach, identifying the significant impact of uncertainty. Their risk assessment model is based on improved evidence theory, utilizing information security index weights. Uncertain evidence is treated with fuzzy measure, and expert inputs are used at the individual evidence level. The model also provides a method of testing the evidential consistency, reducing the uncertainty of the evidence. Their model decomposes risks into its subcomponents and identifies appropriate controls and their interrelationships. (Feng & Li, 2011.)

Saleh and Alfantookh (2011) claim that the traditional risk management methods focus overly on the technology and propose mainly technical solutions. Their risk management framework includes human, organizational, strategic and environmental factors. The structural dimensions of their model include the risk management scope and assessment criteria. The scope consists of strategy, technology, organization, people, and environment. In the assessment criteria, various standards can be utilized. The procedural dimensions include process and assessment tools, using six-sigma DMAIC-model (define, measure, analyze, improve, and control). (Saleh & Alfantookh, 2011.)

Compared to most of the introduced cybersecurity models, Huang, Hu and Behara (2008) have a slightly different approach. Instead of starting the process from the vulnerabilities, they argue that security threats should be identified before security investments are made based on vulnerabilities. Their model analyzes optimal security investment strategies in various scenarios, focusing on risk-averse decision-maker. They claim that the game-theory approach is appropriate when modelling specific security technology with limited actors and actions. The traditional risk-return analysis is appropriate when determining information security investments addressing multiple security threats and counteracting technologies. (Huang, Hu & Behara, 2008.)

Kwan and Johnson (2014) focused on cybersecurity in healthcare. They used a Cox proportional hazard model to demonstrate the importance of proactive security investments. Their results indicate that proactive security investments are associated with fewer security failures. Learning from previous security failures supports continuous security improvement, but constantly changing security threats decrease the effectiveness of reactive strategies. Typically, a reactive strategy is considered cost-effective because proactive strategies can cause overinvestments due to the threats' uncertainty. They remind that the results may not be directly generalized to other environments. (Kwan & Johnson, 2014.)

Above mentioned research addressed information security and cybersecurity investments, utilizing different theories depending on the objectives and situations. Most of the studies are relatively theoretical, apply in confined environments and do not analyze the actual interaction of the cyber threat and the target system. However, the literature includes also studies covering interaction and cybersecurity from a more strategic angle.

Hu, Liu, Chen, Zhang and Liu (2020) introduced a stochastic evolutionary game for modelling cyberattack and defence. They refer to traditional warfare, where the decision-making and an optimal strategy impact the warfare results. They emphasize the importance of game theory when modelling cyberattack and defence. However, they criticize that typically game models include only rational players. They identify the impact of the environment and individual factors affecting the players. The strategy selection includes a social behaviour with inertia and randomness. (Hu, Liu, Chen, Zhang & Liu, 2020.)

Jalali, Siegel and Madnick (2019) developed a simulation game to research decision-making in cybersecurity capability development. They focused primarily on the potential delays after capability development decisions and the uncertainties predicting cyber incidents. The study aimed to decide how to allocate resources to the prevention, detection, and response phases of cybersecurity. Their game is based on a system dynamics simulation model, including information systems, cybersecurity capabilities, and cyber incidents. Their study indicates that preventive capabilities can reduce cyber incident risks, but they can never entirely eliminate them. Investing only in prevention means lacking detection and response capabilities and, therefore, lacking the detection and recovery of actualized cyber incidents. (Jalali, Siegel & Madnick, 2019.)

In addition to the academic research, several organizations, many times close to governmental agencies, have introduced different cybersecurity-related models. Holzer and Merrit (2015) introduced a methodology to identify the best ways to analyze risks and enhance cyber resilience. They compared four different existing risk management models. They recommended that risk managers should use the tools developed for their field. They should translate the findings into the risk model that is used in organizational strategic planning. This procedure enables integrating information security risk management to organizational risk management and ensures top leadership's attention. (Holzer & Merrit, 2015.)

Bodeau and Graubart (2017) introduced the Cyber Prep -model, a threat-oriented approach allowing to assess threat assumptions and to develop a preparedness strategy. It is focused on advanced threats, but it is also applicable to conventional cyber threats. Cyber Prep can be used standalone or to complement and extend other frameworks and threat models. The model identifies the relationship between the attacker and defender and uses multiple dimensions to characterize them. Dimensions can include goals, scope, timeframe and capabilities. (Bodeau & Graubart, 2017.)

Goel, Kumar and Haddow (2020) claim that several risk assessment frameworks rely on exhaustive data about the organization and are better suited for tactical risk management. Furthermore, existing frameworks lack prioritization, and they do not strategically support senior leadership with mission and business objectives. They introduced an enterprise-level methodological approach to develop a strategy that prioritizes resources, implements, standardizes and monitors (PRISM) an organization's cybersecurity risk. PRISM is a qualitative model that should provide value to executives. (Goel, Kumar & Haddow, 2020.)

Park and Ruighaver (2008) formed a concept of information security strategy in organizations, developed a classification framework for them, and identified important factors influencing their effective implementation. They identified the dimensions of time, space and decision-making in information security strategies. (Park & Ruighaver, 2008.)

From the strategic point of view, traditional information security risk assessment is relatively narrow and technical. On the other hand, literature addressing strategic cybersecurity usually does not include technology but merely describes the phenomenon. This type of description is especially typical in cybersecurity strategies that should be based on strategic analysis. The research between these distinct areas is limited, mainly including the papers of different research institutions, usually close to government organizations. This is also the identified research gap for this master's thesis.

However, the literature includes some elements that require further research and can support this study. Proactive cybersecurity is effective, especially if uncertainties regarding the threats can be managed. Strategic cybersecurity must have a broader than technological approach, but the technology is part of cybersecurity. Furthermore, the use of experts and existing models are appropriate, and different types of game models, event trees and scenarios can be utilized. In a strategic context, the approach is likely more qualitative than quantitative. Possibly different trees and scenarios do not significantly increase the reliability of the analysis, but they support creating a common understanding of the phenomenon with the management.

1.6 Structure

This master's thesis is structured as follows. The research methods are presented in chapter 2. Chapter 3 includes the theory supporting the research. Chapter 4 is the main chapter, introducing the model for strategic cybersecurity analysis. Chapter 5 is reserved for the conclusions, and chapter 6 for the discussion.

2 RESEARCH METHODS

2.1 Research background and objectives

The research objective of this thesis is to determine what strategic analysis of cybersecurity means. Furthermore, the research assesses the means to anticipate future cyber events. The aim is to shift the advantage from the cyber attacker to the defender by increasing the defender's future cybersecurity capability and resilience. This shift can be achieved with the strategic cybersecurity analysis model introduced in this thesis. This novel analysis model can be used in the evaluative and estimative analysis of cybersecurity.

The exploratory nature and the construct of a novel model impacted the research design. The key elements in the research design were cybersecurity entities, their significant characteristics and anticipated relations (see Singleton and Straits, 2005). The research objectives were unambiguous enough to support operationalizing the research questions and to execute the research (see Saunders, Lewis & Thornhill, 2012).

Exploratory research aims to find new perspectives, discover new phenomena or examine insufficiently comprehended phenomena (Hirsjärvi, Remes & Sajavaara, 2009). It can be used to clarify a problem where its exact nature is not explicit (Saunders et al., 2012). As phenomena, information security and cybersecurity are well comprehended and researched. However, due to the legacy of information security, the approach typically emphasizes the technical side of cybersecurity. Cyber threats are addressed through own system vulnerabilities, and the focus is on reactive security. The strategic dimension of cybersecurity is still ambiguous, but its impact is increasing. Cybersecurity is already part of, for example, international politics, international law, hybrid threats and even military operations. This research aims to find new perspectives on cybersecurity, increase the understanding of its strategic impact and enable a proactive approach to the topic.

The objective of this chapter is to provide an open and transparent view to the research. The reliability and validity of this type of qualitative exploratory research is a challenge, especially when constructing a novel model for estimative analysis. The reliability and validity of the model can be confirmed with empirical evidence from its operational use. Unfortunately, this type of testing, where the assessments are compared to future real-life cyber events, requires considerable time.

2.2 Foundation of the research

2.2.1 Research philosophy

Denzin and Lincoln (2005) argue that qualitative research is closely related to an interpretive philosophy. The researchers need to comprehend the subjective meanings of a phenomenon (Saunders et al., 2012). The world can be interpreted in multiple ways, and there may be several realities (Saunders et al., 2012). Grenon and Smith (2004) argue that different views of reality can be equally true. The view depends on the entities, domains, perspectives or level of granularity. Ontology provides theories describing the world utilizing some logical language (Grenon & Smith, 2004).

The focus of ontology is on the nature of reality and how the world operates (Saunders et al., 2012). This research aims to describe and interpret cybersecurity using ontology. Furthermore, the approach is pragmatic. With pragmatism, the introduced model for strategic cybersecurity analysis is relevant, and the research findings have practical consequences. Pragmatism enables using multiple research methods allowing credible, well-founded, reliable and relevant results (Saunders et al., 2012). Ontology provides the tools to comprehend the phenomenon of cybersecurity. Pragmatism ensures that the model for cybersecurity analysis has practical implications.

2.2.2 Research approach

In many cases, qualitative research starts with an inductive approach. The objective is to use emergent research to develop a richer theoretical perspective than in the literature. However, Yin (2009) argues that some qualitative research strategies can start with a deductive approach, to test existing theoretical perspectives. In practice, much qualitative research uses an abductive approach, combining inductive and deductive approach. (Saunders et al., 2012.)

The research approach of this study is abductive. The research begins with a deductive approach, utilizing theories of ontology and threat ontology. The relevant strategic cybersecurity literature is limited. Therefore, the theories provide ample base to collect and analyze data, identify the participants, meanings, patterns and relationships of cybersecurity (see Saunders et al., 2012). The construction of the model is based on collected and analyzed data, shifting the phase more towards an inductive approach.

The research faced typical challenges of an inductive and abductive approach. Continuous data collection and simultaneous analysis required more time than anticipated. Furthermore, the ideas, results and conclusions emerged gradually, requiring several modifications in the research process and the cybersecurity analysis model. (see Saunders et al., 2012.)

2.2.3 Research methodology

This research is based on qualitative research methodology. Qualitative research has the perception that reality is not fixed, agreed upon, or measurable. Reality can be interpreted differently, and the interpretations can change over time (Merriam, 2002). Merriam (2002) reminds that qualitative research is appropriate when the objective is to understand a phenomenon or describe a process (Merriam, 2002). Furthermore, qualitative research examines the participants' meanings and relationships (Saunders et al., 2012). Different data collection techniques and analytical procedures can be used to develop a conceptual framework (Saunders et al., 2012). The objective of this research is to construct a model that interprets real-world cybersecurity. The aim is to increase understanding of cybersecurity as a phenomenon by describing the environment, the participants, their relations and activities using a strategic analysis model.

Tuomi and Sarajärvi emphasize the importance of theory also in qualitative research. A theory can support the decisions on research methods. It can ensure reliability and support the wholeness of the study (Tuomi & Sarajärvi, 2018). This research is based on theories of ontology and threat ontology. Data collection was an interactive process where the data was compared to the theories during the process (see Saunders et al., 2012). As the objective is to understand the phenomenon of cybersecurity, the researcher could process information immediately, check the accuracy of interpretations and explore unusual or unanticipated responses (see Merriam, 2002). In qualitative research, it is acceptable that the researcher is the primary instrument for data collection and analysis (Saunders et al., 2012). The research is based on the expertise of the researcher in cybersecurity, intelligence and military operations.

2.3 Research strategy

2.3.1 Constructive research process

Research strategy describes how the research questions are answered. Denzin and Lincoln (2005) argue that it is the methodological link between the research philosophy and subsequent choice of methods to collect and analyze data. Qualitative research can be associated with a variety of strategies having specific emphasis, scope and procedures. (Saunders et al., 2012.)

The research strategy of this thesis is based on constructive research. The objective is to create an innovative construction for cybersecurity analysis. The construction is aimed to solve problems of reality and contribute to the theory of the discipline. Constructions are invented and developed, not discovered. Lukka (2003) claims that constructive research is appropriate when the reality is constructed from basic elements like objects, time-space slices or logical relations. It focuses on real-world problems, produces an innovative construction, and implements and tests it. Constructive research is linked to prior theoretical knowledge, and it can reflect the empirical findings back to theory. Typically, the objective of the novel constructions is to improve forecasting and also control the events of reality. (Lukka, 2003.)

Constructive research supports the construction of a strategic cybersecurity analysis model. The innovative model aims to increase the capability to anticipate future cybersecurity events and threats. Improved cyber threat prediction advocates more efficient and timely cybersecurity capability design and development. The constructed model describes reality, including cyber threat source, target system, cyberspace, time-space they are located and their relations. It can also contribute to the theories of cybersecurity.

The constructive research includes several steps starting from identifying the practical problem, ending with the theoretical contribution (Lukka, 2003). This sub-chapter describes the implementation of constructive research in this study.

2.3.2 Identifying the problem and co-operation

The first step in constructive research is to identify a practical problem with the potential for theoretical contribution (Lukka, 2003). The research problem of this thesis has bothered the researcher for several years. Discussions with the chief executive officer (CEO) of a Finnish cybersecurity company revealed that the problem is relevant and has practical implications. This research aims to provide a solution to the problem but not excluding any theoretical contribution.

The research process followed a typical qualitative research process. The first problem statement was general, and it eventually developed toward a more specific research question (Merriam, 2002). The first problem focused on the defender's position in cyberspace. The idea was to challenge the assumption that a defender can only react to cyberattacks. The logical objective was to find ways to increase the defender's capability and to gain an advantage. The research problem was refined to more detailed research questions covering the actors and environment and how to analyze them. At this point, the focus was on cyber threat and the target system. However, the significant role of cyberspace was promptly identified.

The second step of constructive research includes the examination for long-term research co-operation with the target organization. The idea is to ensure both the researcher's and the target organization's commitment (Lukka, 2003). The researcher and the company had identified the same kind of research problem. Both parties identified the importance of the topic and were committed to the research without any official agreement. Furthermore, co-operation between the researcher and the company may continue after this research.

2.3.3 Obtaining understanding

The third step of the constructive research process is obtaining a deep understanding of the topic area, both practically and theoretically. This phase is aimed to reveal the problems of the research project, allow conceptualizing the problem and identify existing theory. (Lukka, 2003.)

The researcher has developed a deep understanding of threat analysis, targeting, environmental analysis and cybersecurity even before starting the study. The practical understanding was based on the researcher's previous expertise and the requirements of the cybersecurity company. However, the theoretical understanding was insufficient at this point. The construction of a strategic cybersecurity model required an increased understanding of a theory that could describe a phenomenon in a dynamic reality and environment (see Bittner, 2019a).

Eventually, the appropriate theoretical basis was identified for the research. A dynamic spatial ontology was capable of describing the spatial and temporal entities, their parts and interdependences in spatio-temporal locations (see Grenon & Smith, 2004). Furthermore, the threat ontology identified the relationships between the threat, target and the environment. It also included the components of a threat; intention, capability and opportunity (Little & Rogova, 2006). These theories were not cybersecurity specific, but they provided ample tools to analyze the elements of cybersecurity. Later in the research was also identified a need to model the interaction of a threat and a target system in cyberspace.

The theories of ontology supported data collection and analysis. The purposeful sampling of data covered the threat, the target and the environment (see Merriam, 2002). Data collection started from information security literature. However, the samples regarding information security provided only limited data, mainly highly technical, detailed or focused on responsive risk management. Furthermore, the theories of the discipline did not support strategic level analysis. Data collection was expanded to other disciplines that included a more relevant strategic approach. These disciplines include, for example, strategy, intelligence and military studies.

Most qualitative research methods are based on content analysis, at least as a loose theoretical framework (Tuomi & Sarajärvi, 2018). The analysis of this research was based on theory-related content analysis, namely, template analysis. A template is a list of categories representing the themes revealed from the collected data. Template analysis resembles the grounded theory method, but it is more inductive and flexible. It allows developing categories and attaching them to units of data. Coded and analyzed data were used to identify and explore themes, patterns and relationships. Furthermore, template analysis allowed presenting codes and categories hierarchically. (see Saunders et al., 2012.)

The first phase of the analysis included identifying the main categories to comprehend the collected data. The main categories at this point were a cyber threat, a target system, their activity, cyberspace and interaction. The collected data was attached to appropriate categories. Eventually, the category of activity was merged into the cyber threat and target system categories. The analysis identified internal aspects, the relations between the data and categories, enabling the subdivision of the categories hierarchically. Furthermore, the external relations between different categories were also identified, revealing the need for interaction analysis between the threat, target and cyberspace. Template analysis enabled the categorization of cybersecurity, supported the analysis and allowed arranging data into categories and providing the emergent structure of the cybersecurity analysis model. Furthermore, the process assured descriptive and hierarchical categories that are important in a qualitative study. (see Saunders et al., 2012.)

Qualitative research quality depends on the interaction between data collection and data analysis (Saunders et al., 2012). In this research, data were analyzed already during the collection, which allowed constant adjustments to the collection (see Merriam, 2002). At first, the approach was deductive. The analysis was not based on the theories, but the theories revealed new ideas during data collection and analysis. Furthermore, they provided main categories dividing the phenomenon into different classes, subcategories and parts. This upper-level categorization allowed the coding of different variables identified in the literature. Without the theories, collecting data, analyzing data, and understanding cybersecurity entities would have been difficult or even impossible.

The theory-related approach allowed relatively unrestricted references, from traditional information system literature to intelligence and military literature. The broad use of references was identified as a requirement when examining strategic level analysis.

2.3.4 Solution construction

The fourth step of the constructive research process is to innovate a solution idea and develop a problem-solving construction (Lukka, 2003). Lukka (2003) claims that this phase is creative, heuristic, and no designated methodology is available. However, an iterative process between the researcher and the organization is recommended (Lukka, 2003). Bhattacherjee (2012) claims that, typically, constructed models aim to represent a phenomenon, and they can be descriptive, predictive, or normative (Bhattacherjee, 2012). The model constructed in this research aims at predictive representation of cybersecurity.

In the research process, data collection, analysis and the construction of the model were closely intermingled. The analysis guided the data collection but also the construction of the model. Furthermore, data collection and analysis continued during solution construction, making the whole process interactive. The approach of this phase was mostly inductive, allowing recognition of essential themes, patterns and relationships (see Saunders et al., 2012). The two phases of constructive research, obtaining understanding and solution construction, were executed partly simultaneously.

Template analysis allowed utilizing existing schemas, data dictionaries and standards. The upper-level categories were subdivided using relevant existing models familiar from information security and intelligence analysis. They provided the categories for entities, relationships, properties, attributes, and activities (see Obrst, Chase & Markeloff, 2012). Utilizing existing models in categorization ensured the identification of all relevant parts of strategic cybersecurity and increased the reliability and validity of the research. The templates served as an analytical device to construct the conceptual framework and the final analysis model. Different templates also helped identify key themes and emergent issues that arose through data collection, analysis, and construction of the model (Saunders et al., 2012). They were tested continuously against subsequent data (see Merriam, 2002). Some of the codes were modified. The modifications were done after assessing their implications to the rest of the model. The construction process included the insertion of new codes, deleting and merging codes, and altering their hierarchy level. (Saunders et al., 2012.)

The construction process resembled the construction of an ontology. The first step included identifying the main actors in cybersecurity based on ontology and threat ontology theories. In a traditional threat assessment, the operating environment is part of the capability and opportunity. However, it was soon apparent that in cybersecurity, the environment has an even more noticeable impact. Therefore, cyberspace was determined as a category. The objective of the construction was to keep spatial entities, their processes and cyberspace separate in the first steps and combine them only in the last step of the analysis model. The objective of the next step was to identify and determine spatial subcategories from relevant literature. This phase provided the categories of the cyber threat and target system actors. It also identified the internal relations of spatial entities, their attributes and spatial regions. The third phase of the construction focused on the actors' activity, the processes they participate in. The classification of the activities was based on information security and military literature. This step covered the external relations of spatial entities (actors) to their temporal entities (processes) and spatio-temporal regions. During this step, the previously separate category of activity was merged into threat and target categories. This merge simplified the model and moved the activity category closer to its actors. The next step of the construction included the classification and analysis of cyberspace. The last step of the construction focused on the interaction between the threat, target system and cyberspace. This step combined all the categories of the previous steps. It is based on scenario trees with retrospective futurology. (see Little & Rogova, 2009; see Alkire, Lingel, & Hanser, 2018.)

2.3.5 Implementation and testing the solution

The fifth phase of constructive research includes implementing and testing the solution (Lukka, 2003). This phase includes the most significant divergence of this research to a typical constructive research process. The time allocated to this research did not support implementing and testing the model in a real-life environment. However, the strategic cybersecurity analysis model was presented to the experts of a Finnish cybersecurity company, and their feedback was taken into account in the model. Furthermore, the feedback was highly positive and supportive, to the point that the model will be eventually implemented into their artificial intelligence-based analysis system. The implementation and testing of the model will take place after this research is concluded as a master's thesis. For the same reasons, the sixth step of the constructive research process, assessing the applicability of the solution, is executed later. The operationalizing of the model is conducted in a separate process. (see Lukka, 2003.)

2.3.6 Theoretical contribution

The last phase of constructive research is to identify the theoretical contribution. Lukka (2003) emphasizes that practical problems may emerge in areas that are not covered in previous research, and constructive, empirical work may generate new theoretical inputs. Theoretical conclusions are not necessarily related to the success of the constructed model. (Lukka, 2003.)

The objective of this research was to examine strategic cybersecurity analysis and present a model for the analysis. The model can be understood in this context as the first step towards a theory. The literature identifies several ontologies developed to describe cybersecurity, but typically the approach is detailed and technical, supporting mostly traditional information security. The strategic cybersecurity analysis model could provide a basis for developing a foundational cybersecurity ontology, describing the phenomenon from a strategic point. The ontology could provide a base for lower-level ontologies and help integrate strategic cybersecurity analysis into other disciplines. Furthermore, strategic cybersecurity ontology could support the development of artificial intelligence-based predictive cybersecurity tools and procedures.

2.4 References

The primary sources of the research included information security, risk management, ontology, intelligence, and military planning and wargaming. Literature review constituted the basis for the research, focusing the research to the right direction (see Hirsjärvi, Remes & Sajavaara, 2009).

Extensive literature was necessary for the research for several different reasons. First, it was utilized to recognize previous research related to information security, threat assessment, cyber threat and target system interaction analysis. This first objective enabled understanding the context where the cybersecurity analysis model should be used. Second, relevant literature provided the theoretical basis on how to describe a phenomenon of cybersecurity. Particularly important was identifying a theory that enabled to describe a dynamic phenomenon with low probability but high consequences by nature. Third, relevant literature was utilized to understand how the phenomenon can be categorized and subdivided into parts to identify the relationships between the parts, their characteristics and processes. Furthermore, relevant literature provided data on how to categorize and analyze the operational environment, cyberspace. Lastly, the literature also provided appropriate categories, models and tools to analyze the interaction of the cyber threat and the target system in cyberspace.

The content analysis focusing on templates was a rational choice. Modelling cybersecurity required identifying different categories and subcategories to code the data from the references. It also increased the understanding of the relations inside and between the categories.

2.5 Reliability and validity of the research

Human involvement in qualitative research can create some shortcomings and biases that impact the study. Merriam (2002) claims that shortcomings and biases are unnecessary to eliminate, but they should be identified and monitored to understand their impact (Merriam, 2002). Reliability indicates consistency or the extent to which a measure does not contain random error (Singleton & Straits, 2005). Validity refers to the extent to which a measure adequately represents the construct that it is supposed to measure (Bhattacherjee, 2012).

Hirsjärvi, Remes and Sajavaara (2009) claim that challenges related to reliability or validity can be solved with increasing methods, theory or reference triangulation (Hirsjärvi et al., 2009). This research is based on theories of ontology, enabling a reliable and valid description of a complex phenomenon. Furthermore, a dynamic spatial ontology ensured that the relevant parts and their relations are included in the model. On the other hand, the threat ontology ensured that the valid components of intention, capability and opportunity are included in the research. Furthermore, threat ontology supported the identification of the upper-level categories of threat, target and environment. These theories provided a reliable and valid basis for the upper-level categories and their measurements.

Furthermore, the reference material was triangulated constantly during the data collection and analysis. The data was collected from different disciplines to ensure a multi-angled approach to strategic analysis. Data was frequently compared to the theories and the categories in existing strategic capability models. Also, inter-coder reliability was utilized. The constructed model was presented to five experts in a cybersecurity company that participated in the research initiation. Based on their statements, the results of this research can be considered reliable. The cybersecurity company will install this model to its artificial intelligence-based cybersecurity analysis tool. The empirical evidence of the use is available after this research. According to Singleton and Straits (2005), inter-coder reliability assurance is appropriate in exploratory studies. A small sample of persons can be used to gain information if the measure is clearly understood and interpreted similarly by respondents (Singleton & Straits, 2005).

Validity assessment was more problematic than reliability assessment. In general, systematic errors affecting validity are more challenging to detect than random errors. Validity can be assessed by evaluating an operational definition, comparing the operational definition and a specific criterion, or determining if the operational definition of a given construct correlates with other constructs. (Singleton & Straits, 2005.)

Content validity determines if the definitions represent the domain of a concept (Singleton & Straits, 2005). It requires a detailed description of the construct. The content validity of the constructed model was examined when it was presented to the cybersecurity experts. Bhattacherjee (2012) claims that an expert panel can examine the content validity of constructs (Bhattacherjee, 2012). On the other hand, Singleton and Straits (2005) argue that content validity is not reliable as a validity assessment (Singleton & Straits, 2005).

In addition to content validity, also construct validation was utilized. Data collection and analysis provided accumulated research evidence. The collected data supported the definitions of the model. Data was frequently compared to the theories and existing models of categorization. The categorization models utilized in this research are in continuous use in strategic studies, intelligence, military and information security research when describing strategic capabilities. Using existing models ensured that all the relevant and valid subcategories were identified and measurable. (see Singleton & Straits, 2005.)

Lastly, recognizing the challenges related to the reliability and validity of this type of qualitative research, the researcher has tried to describe the research methods and the research process as detailed as possible. This chapter aims to provide ample transparency regarding the research process, how the data was collected and analyzed, and how the model was constructed. Rich descriptions should persuade the reader of the trustworthiness of the findings (Merriam, 2002). Singleton and Straits (2005) state that all forms of validation are subjective. Eventually, the scientific community will determine if the research is reliable and valid (Singleton & Straits, 2005). In this type of research, where the objective is to construct a model for evaluative and estimative analysis, measuring reliability and validity constitutes a challenge. This challenge was identified already at the beginning of the research. Eventually, the reliability and validity of the cybersecurity analysis model will determine the reliability and validity of this research.

2.6 Reflection of the research methods

Constructing a model for an evaluative and estimative analysis of cybersecurity is a challenge. The research objectives were clear, supporting the design and execution of the research. Exploratory research provided ample freedom for increased understanding of cybersecurity. Quantitative measurement of strategic cybersecurity, especially covering future events, is challenging. Therefore, a qualitative research methodology was a clear choice. However, qualitative research needs to provide a rich description to increase the quality of the results.

Reliability and validity constituted significant challenges. In some cases, strategic cybersecurity may be a vague concept, depending on the situation, approach, and granularity level. This introduced model may provide a reliable and valid tool for analysis in some situations but be almost redundant in other cases. However, several research decisions aimed to increase the reliability and validity. The research started with a deductive approach, leaning on the different theories of ontology. Later, when constructing the cybersecurity analysis model, various existing models for categorizing strategic actors and their parts and environment were used. They ensure that the model covers all relevant cybersecurity parts.

Furthermore, the theory-related content analysis using templates was appropriate for this research. The grounded theory would have also been appropriate, but the number of categories would likely have been larger. Also, reducing the number of categories would have been solely the responsibility of the researcher. In the worst case, this might have caused inappropriate and redundant categories. The templates in existing models provided a reliable and valid framework for the analysis and construction.

The constructive research process provided a supportive framework for the research. The objective of this research correlates with the objectives of a typical constructive research. It aims to construct an innovative model to solve real-life problems and contribute to the theory of discipline. The research problem identification, the practical requirements, and the co-operation took place almost as in the typical constructive research process. Obtaining understanding and solution construction phases were in practice not as separate as expected. Simultaneous data collection and analysis, typical for qualitative research, resulted in almost intermingled phases. However, this simultaneousness did not cause any particular challenges. On the contrary, the close interaction of data collection, analysis and model construction was essential for the results.

The primary deficiency of this research is related to time. First of all, the inductive phase of the research required more time than planned. Simultaneous data collection, analysis and construction of the model was time-consuming. The ideas, results and conclusions emerged gradually, requiring several modifications in the research process and the cybersecurity analysis model. Furthermore, also constructive research strategy was time-consuming. As a result, the allotted time for the research did not enable implementing and testing the model in practice. However, the feedback from the cybersecurity experts indicated that the cybersecurity analysis model is reliable and valid. The researcher was satisfied to hear that the cybersecurity company will implement the model in their analysis system. Unfortunately, the empirical evidence of the implementation will be available only after this research. The extent of how well this research and the presented model assess cybersecurity will be determined after its operational use. The assessments produced with this strategic cybersecurity analysis model, compared to real-life cyber events, will eventually prove the efficiency of this model.

3 THEORETICAL BACKGROUND

3.1 Ontology

Strategic analysis of cybersecurity aims to provide information and knowledge for decision-making, support cybersecurity development, and the use of resources and capabilities. With strategic analysis, an organization should gain an advantage over the adversary and anticipate events in the domain. Approximately the same objective is identified by, e.g., Little and Rogova (2006). Although their focus is on threat assessment, they emphasize that the assessment always includes interactions between the source of the threat, the environment and own vulnerabilities. Also, actions taken against the assessed threat are included. (Little & Rogova, 2006; Steinberg, 2005.)

Various threat items constitute a complex structure that is difficult to capture. Eventually, the tools that normally apply to a conventional domain may not be adequate when analyzing an unconventional threat or phenomenon. Traditional threat assessment might recognize only simple binary relations between the participants, neglecting the complex networks of relations. (Little & Rogova, 2006) Little and Rogova (2006) claim that the complexity of threat requires an analysis based on ontology. An ontology allows categorizing the various types of complex objects, their properties, events, processes, relations and situations (Steinberg, 2005; Little & Rogova, 2006). Their focus is on a conventional threat, but all the identified challenges also apply to cyberspace. The strategic analysis of cybersecurity requires tools that can model the complex environment, the participants and the different relationships connecting them. In this research, ontologies are utilized as a framework for the analysis of cybersecurity.

Ontology is a branch of metaphysics regarding the nature and relations of different kinds of being. It is a theory about the nature of being and the things that have existence (Merriam-Webster Dictionary, 2020). As Grenon and Smith (2004) emphasize, ontology describes the entities existing in the world, the types or categories they belong to and the relations that connect them (Grenon & Smith, 2004). Ontology is based on the theory of mereotopology. Mereotopology combines the logic of parts and part-relations (mereology) with the logic of spatial extensions and connectedness (topology) (Smith, 1996; Little & Rogova, 2009). Mereotopology provides a formal structure for exploring relations that exist between different spatial and temporal items. These items can be either unitarily connected or dispersed over space and time (Grenon & Smith, 2004; Little & Rogova, 2006). Understanding the relations of items and their attributes, differentiating wholes from aggregate items and understanding the external and internal relations over time can be accomplished with a mereotopological approach (Little & Rogova, 2009).

Examination of a complex phenomenon requires generalizing and modelling reality. Grenon and Smith (2004) remind that reality can be represented in several different ways, and every representation can be independent but equally legitimate (Grenon & Smith, 2004). Similarly, reality can be examined in different domains, from different perspectives, or at a different granularity level (Grenon & Smith, 2004). Describing reality requires reducing and generalizing the results of observations. Eventually, each description is an abstraction of a real-world perception (Iwaniak, Łukowicz, Strzelecki & Kaczmarek, 2013). Theories of ontology create a formalized logical language about the world (Grenon & Smith, 2004). Little and Rogova (2009) point out that ontology provides tools for understanding, organizing, modelling, and communicating complex states of items and their relations, creating an understanding of the environment. An ontology can cover both concrete and abstract items, exploiting logic in analytical reasoning systems (Little & Rogova, 2009; Grenon & Smith, 2004). Ontology also enables building logical systems capable of classifying objects by their behaviour over time (Iwaniak et al., 2013). It can also distinguish the entities from the processes they participate in. Bittner (2019) emphasizes the importance of this feature, especially when describing dynamic reality (Bittner, 2019a).

Obrst, Chase and Markeloff (2012) divide ontologies into three main categories, upper, mid-level and domain ontologies. The appropriate category is defined mostly by the level of abstraction. The upper ontologies are at the highest level. They are also called fundamental, top-level or high-level ontologies. (Obrst, Chase & Markeloff, 2012) Upper ontologies also include formal ontologies (Iwaniak et al., 2013). A formal ontology addresses categories and relations that appear in all domains and are typically applicable from any perspective (Grenon & Smith, 2004). Formal ontologies allow an application- and domain-independent description of reality (Iwaniak et al., 2013). However, they are related to other ontologies, providing a common knowledge for lower-level domain-specific ontologies (Obrst et al., 2012). Herre, Hellert, Burek, Hoehndorf, Loebe and Michalek (2006) consider upper ontologies as foundational ontologies. They argue that every domain-specific or generic ontology must be based on an upper ontology that performs as a framework and reference (Herre, Hellert, Burek, Hoehndorf, Loebe & Michalek, 2006).

Mid-level ontologies are less abstract than upper ontologies. They make assertions covering multiple domain ontologies. They also provide more concrete representations of abstract concepts. However, there is no clear distinction between the upper and mid-level ontologies. Mid-level ontologies may include the ontologies representing commonly-used concepts, like time and location. Domain ontologies, on the other hand, define concepts particular to the domain of interest. They represent the concepts and relationships from a domain-specific perspective. Domain ontologies may rely on mid-level and upper ontologies. (Obrst et al., 2012) Grenon and Smith (2004) emphasize that the number and the content of ontologies are not limited. There can be as many ontologies as there are subject matters or domains. The domains in ontologies can include space, time and different types of physical domains. (Grenon & Smith, 2004)

Basic Formal Ontology (BFO) is an upper ontology about the basic structures of reality (Grenon & Smith, 2004; Little, Rogova & Boury-Brisset, 2008). Grenon and Smith (2004) state that it provides a formal language that can manage several ontological items required in a higher-level fusion process. These items can be objects, their properties or attributes, spaces, times, and different types of simple and complex relations between them. (Grenon & Smith, 2004; Little & Rogova, 2006) Bittner and Smith (2003) introduced a formal ontological theory, that was capable of describing the spatial and temporal parts of reality; SNAP-ontology describing the spatial part and the SPAN-ontology the temporal part (Bittner & Smith, 2003; Grenon & Smith, 2004; Little & Rogova, 2006). Consequently, Basic Formal Ontology covers three-dimensional (spatial) and four-dimensional (temporal or spatiotemporal) entities. It enables describing complex and dynamic reality by separating participants and their attributes from the processes they are executing (Little & Rogova, 2009). This feature is the one Bittner (2019a) identifies as a requirement when describing dynamic reality (Bittner, 2019a). For example, another upper ontology, General Formal Ontology (GFO), addresses participants, attributes and processes all as objects (Herre et al., 2006).

Based on Basic Formal Ontology, Little and Rogova (2006) presented the Threat Ontology intended for the threat assessment (Little & Rogova, 2006). They claim that threat items, the objects of analysis, form a complex structure that is difficult to capture. The Threat Ontology examines the formal dependence relations between the threat components of intent, capability and opportunity. However, the threat does not exist without the target, so the ontology includes also target vulnerabilities and environment. (Little & Rogova, 2006) The Threat Ontology attempts to provide a deep philosophical understanding of threats, their features, parts and relations (Little et al., 2008).

The work of Little and Rogova is based on the study of Steinberg (2005), who presented a concept for threat analysis. The goal of the concept was to establish a systematic approach for predicting, detecting and characterizing threat activity. The objective also included the automatization of some of the functions. The concept was based on advances in theories regarding situation, ontology and estimation. (Steinberg, 2005) Most of the other threat-related ontologies are domain or subject matter specific. Thomsen and Smith (2018) introduced a prototype of an ontology-driven information system. The objective was to support information-intensive tasks like planning a military mission or executing a threat assessment in operations. Their idea was to combine natural language and sensor data to discover new situations and thematic roles. They introduced a portion of reality (POR) representation, where space, time, object, attribute and the process are combined. In their model, the sensor could collect the information included in POR-representation and translate it to BFO-language. (Thomsen & Smith, 2018.)

In cybersecurity, the perspectives of ontologies are more system than strategic or phenomenon oriented. Ulicny, Moskal, Kokar, Abe and Smith (2014) argue that in most cases, cybersecurity ontologies are focused on technology, or they are otherwise technology-oriented. Typically, ontologies are applied to intrusion detection, situational awareness and software development, for example, modelling network monitoring or classifying malicious activities. Furthermore, a comprehensive ontology for cybersecurity is nonexistent. (Ulicny, Moskal, Kokar, Abe & Smith, 2014) Obrst, Chase and Markeloff (2012) remind that several foundational ontologies can be utilized when establishing cyber ontologies. Besides the Basic Formal Ontology, it is possible to exploit General Formal Ontology (GFO), the Descriptive Ontology for Linguistic and Cognitive Engineering (DOLCE), Object-Centered High-Level REference ontology (OCHRE), Suggested Upper Merged Ontology (SUMO), Unified Foundational Ontology (UFO) and Cyc/OpenCyc. (Obrst et al., 2012; Jansen, 2018)

Obrst, Chase and Markeloff (2012) presented a cyber ontology based on an initial malware ontology. Their ontology represents several categories of concepts. The concepts can be arranged, based on abstraction, from general to domain-specific. They also presented separate ontologies that span multiple concept categories. They argue that cyber ontology should cover persons, time, geospatial events and situations, network operations and other cyber resources. Modelling persons should include an ontological description of persons, their social roles and relationships, and their relationships to things. They suggest that cyber ontology may require geospatial concepts to describe the physical locations of people or infrastructure. (Obrst et al., 2012.)

Ulicny, Moskal, Kokar, Abe and Smith (2014) presented an ontology for cyber operations. It can be used to determine the threat actor, the target and the objective to determine potential courses of action and future impacts. The ontology is based on existing cybersecurity-related standards and markup languages. They propose that a cyber situational awareness engine needs to characterize the situation, either normal or abnormal. In this context, an abnormal situation meaning being under attack or in an otherwise undesirable condition. (Ulicny et al., 2014) Oltramari, Cranor, Walls and McDaniel (2014) proposed an ontology for improving cyber defenders' situational awareness. The objective was to support cyber defenders to make optimal operational decisions in every state of the cyber environment. They point out that concepts suitable for representing security in the physical world cannot be directly transferred to the cyber environment. (Oltramari, Cranor, Walls & McDaniel, 2014)

Syed, Padia, Finin, Mathews and Joshi (2016) presented the Unified Cybersecurity Ontology (UCO) that was intended to support information integration and cyber situational awareness in cybersecurity systems. The objective of the UCO is to provide a common understanding of cybersecurity and unify commonly used cybersecurity standards (Syed, Padia, Finin, Mathews & Joshi, 2016). Interestingly, they recognize the need to develop temporal representation and reasoning in future studies. They conclude that cybersecurity data and information can have a temporal component. They also claim a need to model uncertainty and extract cybersecurity information from unstructured data. (Syed et al., 2016) Wang, Chao, Lo and Wang (2017) demonstrated the use of ontologies in threat analysis and defensive mobile security methods. They identified the attack profiles of possible threats, determined the attack results, observed the effects of countermeasures and evaluated the defence costs and skills required. (Wang, Chao, Lo & Wang, 2017.)

Ontologies provide means for systematic and consistent recordings of facts about entities having different properties at different times. They provide facts about different relations taking place on times or processes occurring at certain time intervals. A dynamic phenomenon requires an ontology that can distinguish different types of changes. Bittner (2019) emphasizes that an ontology must be suitable for recognizing possible logical changes and processes in different combinations. Similarly, an ontology should recognize metaphysically and physically possible changes. For example, instantaneous changes are logically and metaphysically possible for immaterial entities but physically impossible for material entities. (Bittner, 2019a; Bittner, 2019b.)

3.2 Ontology entities and relations

3.2.1 Spatial entities

Grenon and Smith (2004) claim that an ontology describes the entities existing in the world, their categories and relations. Entities have different features, depending on if they are spatial or temporal. The main difference is that the spatial entities have a continuous existence and the temporal entities emerge at a limited time. (Grenon & Smith, 2004) In other words, spatial entities can be objects or actors, and temporal entities typically their processes or activities.

Bittner and Smith (2003) presented ontologies covering the spatial and temporal parts. The SNAP-ontology describes the spatial entities that have a continuous existence and the capability to endure. They are typically called continuants or endurants. (Bittner & Smith, 2003; Grenon & Smith, 2004) Spatial entities exist at a given time, in a given domain, and at a certain granularity level. Typically, they have existed already in the past and will continue existing in the future; they are not instantaneous. When snapshots of the times when they exist are captured and combined, enduring entities have existence over time. (Grenon & Smith, 2004.)

Spatial entities keep their identity even if they are changing, having different parts or different qualities at different times (Bittner, 2019a). Fundamentally, their parts and relations exist in their entirety at any particular time (Little & Rogova, 2009). Spatial entities have three-dimensional bodies and spatial regions. The SNAP-ontology describes where spatial entities are located, their qualities, powers, functions, roles and other features, and how they exist from one moment to the next. (Grenon & Smith, 2004.)

Spatial entities are divided into three main categories (figure 1). These categories are substantial entities, dependent entities and spatial regions. (Grenon & Smith, 2004, p. 141.)

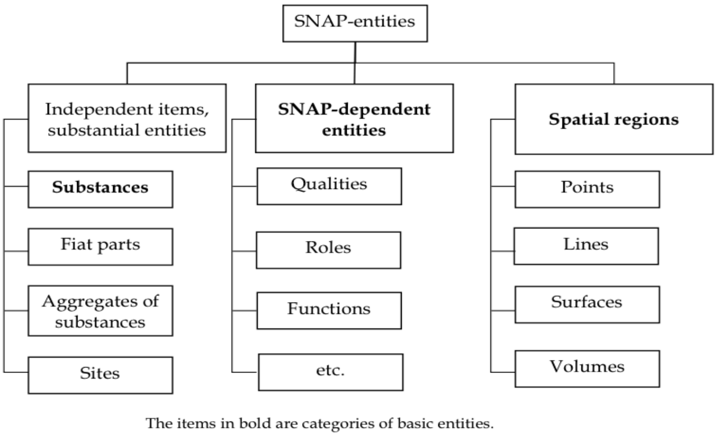

FIGURE 1 The main formal categories of SNAP entities.

Substantial entities include fiat parts, boundaries, aggregates, and sites. Maximally connected substantial entities are called substances. They are independent entities because their existence does not depend on other entities. Substances keep their identity over time and through the changes. They are self-connected wholes having boundaries and a location in space. Substances have sites that are located in spatial regions. Typically, sites are compounds of surroundings. They can be physically bounded or boundary-free. (Grenon & Smith, 2004.)

Dependent entities include various attributes, features, qualities, roles, states and functions. They are called dependent entities because their existence depends on substantial entities, and they cannot exist by themselves. An attribute can depend on one substantial entity only or multiple substances at the same time. (Grenon & Smith, 2004.)

Substantial entities have a location in spatial regions (Little & Rogova, 2009). Spatial regions are SNAP-entities on their own, and they are called endurants. Like substantial entities, also spatial regions have relations. Relations can include connectedness, a separation between other spatial regions, fiat boundaries, dimensionality, and other related notions. (Grenon & Smith, 2004) Both physical and subjective boundaries are possible (Little & Rogova, 2009).

The states and changes of spatial entities can be qualitative, substantial or locational (spatial). Qualitative changes are transformations that change the quality of an entity. A significant change can profoundly affect the nature of the entity, but it will keep the identity. Substantial change, typically, means the termination of the object in some way. Spatial change does not necessarily mean moving in the physical sense. It can also mean changes to the boundaries. (Iwaniak et al., 2013; Grenon & Smith, 2004.)

3.2.2 Temporal entities

The temporal part is described with the SPAN-ontology. The temporal entities are called occurrents or perdurants. Typically, they are different types of processes or activities. (Bittner & Smith, 2003) Temporal entities emerge in a limited time; they do not have a continuous existence like spatial entities. An occurrent can be, for example, a process, an event, an activity or a change. They open up at a particular time and therefore are restricted by time. When an occurrent emerges in a specific time window, it is associated with a corresponding temporal portion. (Grenon & Smith, 2004) Occurrents evolve, and they never exist in full at a given moment in time (Bittner, 2019a).

Grenon and Smith (2004) divide temporal entities into three main categories; processual entities, temporal regions and spatiotemporal regions (figure 2). (Grenon & Smith, 2004, p. 142.)

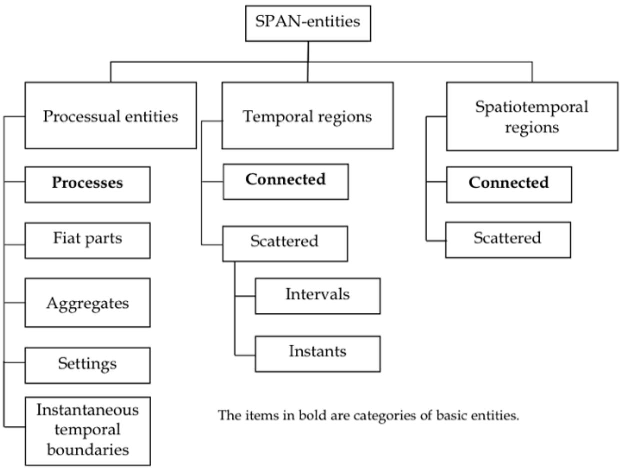

FIGURE 2 Taxonomy of SPAN entities.

Processual entities include processes, fiat parts, aggregates and boundaries, and they can have various levels of complex structures. They depend on spatial entities and cannot exist by themselves. Spatial entities are the participants of the processes. (Grenon & Smith, 2004) Due to this dependence, describing a process requires also describing the participating spatial entities (Bittner & Smith, 2003).

The processual entities are located in temporal and spatiotemporal regions. Temporal regions can be instantaneous or extended, connected or disconnected. Their boundaries are zero-dimensional instants of time. Every processual entity has a temporal location and a relation with the region of time. The relation transpires in the instantaneous temporal part, temporal slice, where that processual entity is located. The temporal location of each temporal entity is unique. Processual entities do not change their locations in time, like substantial entities may change their locations in space. (Grenon & Smith, 2004.)

Grenon and Smith (2004) state that the maximal spatiotemporal region is spacetime, and all spatiotemporal regions exist alongside in the spatiotemporal universe. A spatiotemporal location includes a relation between a temporal entity and its location in the region of spacetime. Furthermore, spatiotemporal regions are also entities on their own. They are independent of any processual entities that may be located at or within them. (Grenon & Smith, 2004) Grenon and Smith (2004) remind that spatiotemporal regions have specific four-dimensional shapes.

They can be, for example, shapes of army manoeuvres or storm movements. Processual entities can have several spatiotemporal relations between them. On the other hand, when two entities occupy the same spatiotemporal region, or the regions share a part, they have co-incidental relations or locational overlap. (Grenon & Smith, 2004) In the temporal SPAN-ontology, boundaries are always subjective because time is a continuum (Little & Rogova, 2009).

Processual entities have only a limited number of precise joints between them. Typically, processes merge and make larger process-wholes. Therefore, the temporal and spatiotemporal domain is continuously under change. The boundaries of the processes are beginnings and endings. Grenon and Smith (2004) remind that processual entities do not have temporal or spatiotemporal gaps. For example, a process cannot occur at two distinct times without occurring at every time interval between them. With the same logic, a process cannot occupy two topologically separated spatiotemporal regions without also occupying the spatiotemporal region between them. Possible discontinuities mean that the occurrent is not a single process but an aggregate of processes. Sometimes the determination can depend on the level of the granularity. (Grenon & Smith, 2004.)

As mentioned before, some occurrents can be instantaneous. Grenon and Smith (2004) call these instantaneous occurrents events. Events can be the boundaries (beginning and ending) of a process or transitions within a process (Grenon & Smith, 2004). Thomsen and Smith (2018) explain that a process is an occurrent, where every consecutive moment's substance is the same. Therefore, a process is a repetition of the same activity. On the other hand, an event has heterogeneous subsequent temporal parts, and the consecutive moments of the process are different. An event is, in fact, a discontinuity in the process. (Thomsen & Smith, 2018) Similarly, Jarrar and Ceusters (2017) claim that all processes are durative and no process occurs instantly in zero-time. They argue that the instantaneous processes are, in fact, the peak moments of the longer processes. They conclude that the peak moments are critical parts of the processes. If the process is terminated before the peak moment, the result of the process changes. (Jarrar & Ceusters, 2017) Obrst, Chase and Markeloff (2012) emphasize that events are entities that describe the occurrences of actions and changes in the real world. Situations represent the history of action occurrences. Events and situations are dynamic and therefore challenging to model. (Obrst et al., 2012.)

3.2.3 Internal and external relations of entities

Describing dynamic reality requires that spatial and temporal entities are examined separately. Separation enables keeping the spatial parts of an entity separated from the temporal parts of the activities (Little & Rogova, 2009). However, there is a close relationship between spatial and temporal entities that crosses the SNAP-SPAN-ontology divide in real life (Grenon & Smith, 2004). Combining these two ontologies is a challenge, mostly because spatial and temporal entities exist in time in different ways (Bittner & Smith, 2003). However, the ontologies can be integrated with transontology (Grenon & Smith, 2004).

Internal relations exist within the respective SNAP- and SPAN-ontologies, for example, between a substance, its attributes, and spatial region. Each object has a unique identity, even if it composed of various parts. Wholes are the sums of all parts, including their independent parts (substances) and dependent parts (attributes). Anything can be dismantled into spatial or temporal parts, but the result differs in different ontologies. In spatial SNAP-ontology can exist both physical and subjective boundaries. In temporal SPAN-ontology, boundaries are always subjective. (Little & Rogova, 2009.)

External relations include the relations between spatial and temporal entities, and they have several different variations. Bittner and Smith (2003) recognize three different types of relationships. They are dependence, participation and realization. In a dependence-type relationship, a process is dependent on the substance. Participation refers to a situation where substances participate in a process. In realization, the roles, functions and plans are actualized in the process. (Bittner & Smith, 2003.)

Substances and their attributes can affect the processes, processes can affect substances and attributes, or they can have a mutual dependence on each other. Little and Rogova (2009) suggest several different types of relations. In perpetration, the substance has an active role in starting, continuing or terminating the process. The substance can also influence the process by facilitating or hindering it. The substance can also have only indirect or passive influence. When the attributes have similar relations with the process, they can be discovered by their temporal initiations, persistence or termination. Little and Rogova (2009) emphasize that attribute detection can be an important factor when identifying the difference between a potential and a viable threat. Changes in attributes can be an indicator that certain activities or changes in the threat are taking place. (Little & Rogova, 2009.)

When the temporal entities (processes) affect spatial entities (substances and their attributes), the relationship is called involvement. The effects of involvement can vary. In creation, the process brings out the existence of substance. In sustainment, the process prolongs the existence of the substance. In degradation, the process affects the existence of the substance negatively. In destruction, the process destroys the existence of the substance. Demarcation can establish a spatial boundary, and blurring can blur it. The process affecting only the attributes is called affection. As in the case of substance, affection also includes creation, continuation, degradation and destruction. (Little & Rogova, 2009.)

The various types of relations described above enable an understanding of complex relationships between the entities. They can include relations between independent physical items and their dependent parts, the attributes. The relations also include the spatial regions where the substances are located, presented as coordinates or addresses. Furthermore, they can include processes and the temporal regions (times) when the process takes place. All these entities can be reviewed at different levels of granularity and from multiple perspectives. (Little & Rogova, 2009.)

Little and Rogova (2009) argue that internal and external spatial and temporal relations must be examined independently. Independent examination enables managing situations at a different level of granularity. Accordingly, this allows for supporting different levels of decision-makers and gives flexibility and scalability to analysis processes. (Little & Rogova, 2009.)

3.3 Threat, target and cyberspace

3.3.1 Threat

The role and the impact of a threat in cybersecurity are prominent. Without a threat, cybersecurity remains unchallenged and secured. A threat, a target and cyberspace constitute a complex phenomenon. Before discussing cyber threats, it is necessary to examine threats in general.

A threat cannot exist by itself. Vandepeer (2011) emphasizes that a threat must refer to something. Understanding the threat requires also understanding the threatened target (Vandepeer, 2011). Bayne (2002) describes threat as anything that can modify, destruct or interrupt service. Threats can be divided into human and non-human elements (Bayne, 2002). Schechter (2004) reminds that the concept of a threat does not always refer to an adversary. It can also mean a chain of events caused by the threat source (Schechter, 2004). Typically, a threat is understood to include three components; an intention, a capability and an opportunity. All these components are foundationally related to each other. (Little, Rogova & Boury-Brisset, 2008) Threats can be categorized as either potential or viable. The difference is the state of readiness. Potential threats are missing at least one of the essential components and their corresponding relations. A potential threat is not yet actualized, but it might become a viable threat. A viable threat contains all three components. (Little et al., 2008.)

Intentions, capabilities, and opportunities have a formal relation of foundational dependence; one component's existence is a requirement for the existence of another component or components (Little & Rogova, 2006). If one of the components is changed or removed, the threat is changed or destroyed. The existence of a threat depends on the existence and relationships between these components. (Little et al., 2008) In an analysis, examining these components is essential. Steinberg (2005) emphasizes that adversary's capability, opportunity and intent to execute actions are the indicators of threatening situations (Steinberg, 2005).

Intentions are plans or goals to be accomplished, and they can be inferred from different means related to the objectives. Intentions are based on individuals' or groups' decisions (Little & Rogova, 2006; Steinberg, 2005). Furthermore, they are the psychological component of the threat, impacted by capabilities and opportunities. Capabilities can be objects, their attributes or behaviours. These available capabilities enable intentions when opportunities emerge. (Little & Rogova, 2006) Steinberg (2005) states that the threat source's capability depends on designing, developing, and deploying or delivering the threat activity's resources. Therefore, the analysis aims to search for appropriate indicators (Steinberg, 2005). The threat components are equally valid in both conventional and unconventional threats, but they may differ in different domains (Little & Rogova, 2006).

Opportunities are spatiotemporal states like observing the target, knowing the adversary's intentions or identifying the adversary's vulnerabilities. Opportunities allow actualizing intentions and deploying capabilities. (Little & Rogova, 2006) However, opportunities include some constraints. The threat source must have the opportunity to execute an attack against particular targets. Therefore, the accessibility and vulnerability of the target set some constraints. Some constraints may be based on the threat source's own assessment of opportunities and expected outcomes. (Steinberg, 2005.)

Typically, a threat consists of different types of items or parts. However, the parts themselves do not create a threat. The question is if the parts constitute an aggregate or a whole. An aggregate is just a group of independent items. On the other hand, a whole includes items with dependent relations. Identifying the difference is essential. Aggregates and wholes may include the same items, but only in the whole they are connected and can create a viable threat. Furthermore, the wholes include relations that cannot be comprehensively explained just by adding up the parts. Parts are tied together through dependence creating a whole. (Little et al., 2008.)

A complex whole is sometimes difficult to capture into a categorical structure. A threat source contains parts and part-relations, which present a distinct ontological structure. (Little & Rogova, 2006) In an integral whole, a single part itself can be essential for the existence of the whole. On the other hand, the existence of a non-essential part is only conditional. A viable threat is an integral whole that includes all essential parts and interdependent components; intention, capability and opportunity. Each of these components can be considered a center of gravity. Disrupting any of them will change the threat's essence. On the other hand, enhancing one component can enhance other components or the whole threat. (Little et al., 2008.)

Little, Rogova and Boury-Brisset (2008) emphasize that the threat parts often extend over spatial regions or temporal periods, existing as dispersed wholes. Even if the threat seems to be spatially, temporally or causally dispersed, it may contain parts connected with some unifying feature. Even if dispersed wholes may appear to exist as aggregates of items, they may include strong ontological relations. A typical feature of wholes is that they can maintain identity over time, even if they gain or lose members. Therefore, a whole will survive as long as it does not lose the essential parts. Aggregates, on the other hand, cannot maintain their identity if they gain or lose members. At any moment, they are just a summation of their members at that time and place. (Little et al., 2008) In unitary wholes, the parts are spatiotemporally contiguous and unified, which likely requires less processing to recognize them (Little & Rogova, 2006). However, in many cases, the data and information required in the analysis are widespread in space and time (Steinberg, 2005). If the foundational dependence can be identified, relevant threat elements can be recognized, even if they are dispersed (Little & Rogova, 2006).

Potential threats are not in a state of being. They do not have existent spatial items, but they are in the state of becoming a threat. Parts of the threat items are constantly unfolding and are not yet actualized at a given place or time. (Little & Rogova, 2006) They have only temporal items because their existence is instantiated only temporally, not physically (Little et al., 2008). A viable threat contains all of its spatial and temporal entities and respective relations at a given place and time (Little & Rogova, 2006).

Little and Rogova (2006) argue that the essence of threat analysis is to understand the elements needed to be present for a threat to change from potential to a viable one. Analysis requires understanding the distinctions between various formal configurations of integrated wholes. For threat assessment is essential to understand the potentiality or actuality of a threat condition. That provides an increased understanding of how the threat components, as integrated wholes, exist and change over time. Since potential threats do not exist in their entirety, appropriate mitigation can prevent them from developing into a viable threat. The actions can deny adversary's opportunities, change their intentions or restrict their capabilities. Disrupting any of the components means disrupting the threat as a whole. (Little & Rogova, 2006.)

The strategic analysis of cybersecurity is not a traditional threat assessment, but the overall objective is the same. The analysis emphasizes the ability to collect data, information and knowledge for decision making, which allows predictive actions and an advantage over the adversary. A strategic analysis of cybersecurity must identify adversary's capability design, development and deployment, and the impact on their capabilities, intentions, and opportunities. These results support the design and development of own cybersecurity capabilities to mitigate or disrupt adversary's actions.

3.3.2 Information and communication technologies – the target

The target of a cyber threat is the computing environment (information system), even if the eventual objective exists in a physical environment. Raggad (2010) determines the computing environment consisting of people, activities, data, technology and network. The information in the computing environment is for the users, and the protection of the information requires the protection of the computing environment. Information security is typically related to confidentiality, integrity and availability of information. (Raggad, 2010.)

An information system includes complex relations between different actors. People using the system are dependent on other people, activities, technology, data and networks. They are the users and administrators of the system. Activities can include executing and following different policies, procedures, standards and guidelines. An information system depends on processes that define how interactions between the different elements of an information system are managed. Data forms the conceptual resource, and it can be divided into noise, data, information and knowledge. Raggad (2010) limits the technology to include the hardware and software tools used in the computing environment. On the other hand, the network element includes all physical resources, including the network infrastructure, buildings and environment. Vulnerabilities in the information system can compromise confidentiality, integrity and availability. (Raggad, 2010.)

Little and Rogova (2006) emphasize that modelling complex situational items, like vulnerabilities, constitute a challenge. They point out that vulnerability states have complex ontological part-structure, where several different relations exist between intentions, capabilities and opportunities. Furthermore, the basic ontological structure of vulnerability contains several types of integrated wholes that can include the threat, defenders and non-combatants. All of these can include their embedded relations of intentions, capabilities and opportunities as parts. (Little & Rogova, 2006.)

Little and Rogova's (2006) threat insights can be extended to an information system, the target of a cyber threat. The target system exists as an integrated whole, and it includes the same components of intentions, capabilities and opportunities (see Little & Rogova, 2006). In an information system, intentions are the plans, goals and actions to protect the system. They include the will to invest in security controls and express these goals outside the organization. Intentions are the psychological element, also when protecting an information system. Intentions to protect an information system are affected by the capabilities and opportunities. The capability to protect includes different security controls, composed of the actors, their attributes and behaviours, the spatial and temporal entities. Effective security controls can be seen as a whole, not an aggregate of unattached parts. (see Little et al., 2008.)

Capabilities are the enablers of the intentions. However, in own information system, capabilities do not directly open or exploit opportunities. The objective is to prevent adversary's activities. Protecting an information system means preventing opportunities from the adversary to attack. If an opportunity emerges, it usually means that the intentions and capabilities to protect the information system are compromised. The appropriate step is to close the adversary's opportunity. As in the case of a threat, information system security can also be categorized either potential or viable. When system security is potential, an information system has vulnerabilities. It is missing entirely or partly the plans to secure the system, the intention, or the capability to operate the security controls. The deficiencies in the security elements mean an opportunity for the adversary to exploit the system. If intentions and capabilities are valid, the system security is viable, and the adversary does not have an opportunity to attack. The objective is that an information system should not include any vulnerabilities that can challenge the information confidentiality, integrity or availability. That is also a question of perspective and granularity.

As in the case of a threat, also information system includes relations of foundational dependence between intentions, capabilities and opportunities. Changing or removing one component means changed or destroyed cybersecurity. On the other hand, if intentions or capabilities are enhanced, the probability of attack opportunities decreases. From the ontological perspective, an information system includes different entities and numerous relations. People, technology, data and networks, are spatial entities having different types of attributes and exist in their entirety at any given moment (see Grenon & Smith, 2004). On the other hand, most information system activities, either related to the administration, protection or use, are temporal entities. These processes have a beginning and ending, as well as the peak moment. Other parts of the computing system are participants of these activities.

3.3.3 Cyberspace

Cyberspace is the operational environment where a cyber threat source and a target system reside, operate and interact. Ormrod and Turnbull (2016) define cyberspace as an evolving, loosely bounded and interconnected information environment utilizing communication methods (Ormrod & Turnbull, 2016). Information technology literature identifies several models to categorize cyberspace. Typically, it is understood to comprise a physical layer, logical layer and informational or social layer, with some variations depending on the respective model.

According to the Joint Publication of Cyber Operations (2018), cyberspace includes the interrelated layers of physical network, logical network, and cyber-persona. The physical network includes the devices and infrastructure that provide storage, transport, and information processing within cyberspace. Physical network layer components require physical security measures. The logical network layer consists of the elements that are abstracted from the physical network. They can be individual links and nodes and various distributed elements, including data, applications, and network processes. The logical location is not necessarily related to the geographical location, and a global network can be considered a single network only in the logical sense. Logical elements can be reached only using cyberspace capabilities. The cyber-persona layer is created by abstracting data from the logical network to develop a digital identity representation in cyberspace. Cyber-personas may refer to an actual person or other entity. One individual may create and maintain multiple cyber-personas, and a single cyber-persona can have multiple users. (JP 3-12., 2018.)

Collier, Linkov and Lambert (2013) divide cyberspace into four domains. The physical domain includes hardware, software and networks as a cyberinfrastructure. The information domain covers monitoring, information storage and visualization. Information is analyzed, sensed and used for decision-making in the cognitive domain. The social domain includes social, ethical and other considerations of cyberspace. (Collier, Linkov & Lambert, 2003.)

Fourkas (2004) approaches cyberspace from a spatial perspective. The technical layer includes the technological infrastructure of cyberspace. The geographical layer covers the topology of networks based on the location of the nodes and hubs. The third layer is the social layer that includes the people and organizations using the information and communication networks. People, space and time are essential characteristics when examining the basic features of the spatial conception of cyberspace. (Fourkas, 2004.)

Zimet and Skoudis (2009) divide cyberspace into four domains: systems domain, content and application domain, people and social domain and governance domain. The systems domain is the infrastructure that carries, stores and manipulates information. Interestingly, they emphasize the importance of the support infrastructure, like the electrical power grid or supervisory control and data acquisition systems (SCADA). They claim that the system domain includes a dependency loop; the communications infrastructure depends on the power grid that is controlled with a SCADA system that relies on the communications infrastructure. The content and application domain operates on top of the systems domain, providing usable applications. The people and social domain enable creating communities in cyberspace, with beneficial or malicious objectives. (Zimet & Skoudis, 2009.)

O'Neil (2009) divides cyberspace also into four different levels. The base-level includes the physical elements of communication equipment. The second level, called the hard net, includes the infrastructures based on the elements carrying electromagnetic signals. This level includes different types of telecommunication networks. The third level is logical, including the services of physical signals to carry logical messages. This level includes telephone, radios and television services, internet, private IP-based networks and SCADA-networks. The fourth level is called cyber, including the intellectual content, data, commands, knowledge, ideas and mental models. (O'Neil, 2009.)

The stability of the layers varies. Changes in the physical layer require time. On the other hand, the changes can happen rapidly in the logical and social layers, complicating own analysis and actions. (JP 3-12., 2018) The role of software in cyberspace is increasing, and future conflicts are likely to rely more on software. Software enables obtaining an advantage in speed and the capacity to gather large quantities of data, lowering the detection threshold and identifying adversary vulnerabilities. Accordingly, the role of hardware is decreasing. Furthermore, the data becomes further abstracted from information through big data and analytics. (Ormrod & Turnbull, 2016.)

Ulicny, Moskal, Kokar, Abe and Smith (2014) point out that cyber domain is a dynamic environment. It can change its state independently, regardless of intentional human or computer actions. Typically, actors aim to modify the domain in order to accomplish some predetermined objectives. Objectives can include gaining an advantage in the domain or avoiding some undesired states. (Ulicny et al., 2014). The first one is typical for the threat, the latter one for the target information system.

The layered approach provides a technical view of cyberspace. However, for strategic analysis, a different approach is required. The Joint Publication of Cyberspace Operations (2018) determines cyberspace as a global domain within the information environment. It includes interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12, 2018.)

Ormrod and Turnbull (2016) argue that cyberspace is not a domain. They claim that cyber domain concepts create boundaries that do not represent the complexity of cyberspace. The domain view also insufficiently describes the interaction between different actors. Cyberspace should be referred to as an environment. (Ormrod & Turnbull, 2016) Similarly, Crowther (2017) suggests that cyberspace should be considered equal to air, land and sea (Crowther, 2017) It must be considered at all levels of warfare; strategic, operational and tactical. Cyberspace is an environment that stores, transports, interprets and mediates information across physical and virtual domains. Cyberspace interacts with communication, information, cognitive and social elements. (Ormrod & Turnbull, 2016.)

Rattray (2009) claims that cyberspace includes systems and infrastructures governed by physics laws and computer code logic. Global communications can be created across cyberspace, almost instantaneously. Data can move long distances quickly, many times unrestricted by physical barriers or political boundaries. Controlling essential aspects of the environment increases the actors' power. Inability to obtain access or keep control can limit the political, diplomatic, economic, military and informational aspects of power. (Rattray, 2009)

Rattray (2009) identified four common features that apply to cyberspace based on the environmental theories of power. These features include technological advances, speed and scope of operations, control of key features and national mobilization. The technological advances refer to new types of strategic vulnerabilities and the increasing role of nonstate actors. The speed and scope are related to fast and global operations and command and control automation. The control of key features includes rapid changes in the environment that are based on human control. The national mobilization means having a cadre of professionals cooperating with the private sector. Essential assets in cyberspace include physical infrastructures that enable global communications. These assets include undersea fiber optics, communications satellites and major interconnection points of global networks. Some of these assets may constitute chokepoints. Control or disruption of cyber chokepoints can have a significant impact on global communications. (Rattray, 2009.)

Characteristics of cyberspace may support the offence if critical networks are vulnerable to exploitation, manipulation and disruption. Advantages can be gained by focusing on niche objectives, utilizing anonymous access and acting rapidly. Attackers' stealthy deployment and the attribution challenges mean that damage limitation using preemptive or retaliatory strikes is irrelevant. The speed and freedom of movement create challenges and advantages, but also weaknesses. The interactions in cyberspace are based on human-made hardware and software. Therefore, the geography of cyberspace is more inconstant than in other environments. Parts of cyberspace can be easily activated or deactivated, created or moved. However, cyberspace cannot be modified infinitely. Physical laws, attributes of code and the people and organizations impact the level of the change. Governments, corporations and individuals can control the established interconnections, but cyberspace cannot be controlled to the same degree as land, sea and air. (Rattray, 2009.)

Geers (2001) argue that the dynamic nature of the cyber domain offers benefits to both an attacker and a defender. An attacker may have an increased number of targets and ways to engage them, but a defender can increase the redundancy and survivability of its networks (Geers, 2011). Sigholm and Bang (2013) remind that identifying an attack, its type, the consequences, and the threat source are more challenging in cyberspace than in a traditional environment (Sigholm & Bang, 2013). Other significant differences, compared to the traditional domains, are the relativity of the threat and target and the concept of distance. Geers (2011) claims that in cyberspace, any actor can gain an advantage. Nation-states may have a superior capability, but yet small countries and hackers can exploit their vulnerabilities. Furthermore, the spatial distance between adversaries can be irrelevant in cyber conflict, and in cyberspace almost anything is available. However, limited cyberspace terrain causes some constraints. Different types of reconfigurations, updates, and human decisions can change cyberspace without warning. Furthermore, the final objectives may exist in the real world. Therefore, the results in the physical domain may emerge after a while. (Geers, 2011.)

Chang and Granger (2012) claim that examining cyberwarfare requires understanding the cyber domain, even if the characteristics challenge it. Defining the cyber environment is essential. The objective is to understand the functions and behaviour of the environment and identify their implications. The main features of the cyber domain include convergence, the human element, speed, and asymmetry. (Chang & Granger, 2012) Tikk-Ringas (2015) argues that as a domain, cyberspace includes deliberate, strategically and politically designed, employed and exploited features. The physical, virtual and cognitive layers of cyberspace include strategic contextualization, with political, normative, military and industrial ambitions. (Tikk-Ringas, 2015.)

Oltramari, Cranor, Walls and McDaniel (2014) remind that cyberspace presents a unique challenge to situation awareness. After all, it is a combination of human and machine elements interacting in global networks (Oltramari et al., 2014). Ulicny, Moskal, Kokar, Abe and Smith (2014) emphasize the importance of cyberspace. Effective cybersecurity requires information collection from the environment. The decisions should be made based on collected information and knowledge, and appropriate actions should follow the decisions. Furthermore, there is a need to collect feedback from the environment in response to the actions and update knowledge to improve future decisions. (Ulicny et al., 2014) They focused on system-level cybersecurity, but their findings also apply to the strategic level.

3.3.4 Interaction

Little and Rogova (2006) suggest that the three components of the threat and the target have different roles in the operational environment. Intent and capability are, in most cases, relations that effect inside the threat source and the target system. These components are related internally, and they typically do not overlap directly to another entity's side. The third element, opportunity, has a different role. It includes a set of interactions, which allow confrontation of the threat source and the target system in the environment (figure 3). (Little & Rogova, 2006, p. 6.)

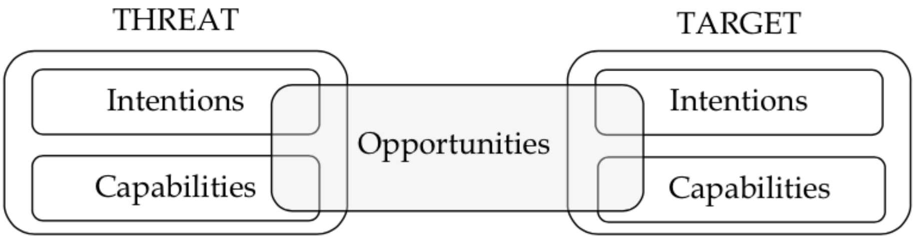

FIGURE 3 Relational structures of threat and target.

Opportunities enable the activation of the intentions and capabilities in a shared environment. They include intentional activities like collecting information of an adversary, gaining an advantageous position, performing deception actions or executing spatial manoeuvres. Opportunities also include passive environmental factors, such as weather, cover, non-combatants and terrain that affect both entities' conditions. (Little & Rogova, 2006) These traditional environmental factors have analogies in cyberspace, and they are covered in more detailed later in this thesis.

Little and Rogova (2006) focus on traditional threat and target in a traditional domain. Nevertheless, most of their observations apply also in cyberspace. The intentions and capabilities are the features of a cyber threat source and a target system. A cyber threat source's opportunity can be actualized in cyberspace, resulting as a confrontation with a target information system.

Modelling a threat requires understanding the intentions of the threat source. On a strategic level, intentions can be diplomatic, economic, military or information, or a combination of these. The capabilities can be modelled based on the actors and their physical and non-physical attributes and properties (Little & Rogova, 2006). Similarly, the same requirements apply to the target. Modelling own system as a target requires an in-depth understanding of own development intentions (objectives) and capabilities (actors, attributes and processes). Modelling the environment requires covering spatial, temporal, and spatiotemporal regions, including the entities located in them. In a conventional domain, the spatial distance between friendly and enemy forces needs to be considered. In most cases, this does not apply to cyberspace, where physical distance is not usually a factor. However, the requirement to identify scattered spatial and temporal regions related to own and adversary's processes is even more significant in cyberspace than in a conventional domain. (see Little & Rogova, 2006.)

In the interaction, the cyberthreat and the target system affect each other. Understanding the phenomenon requires identifying different threat behaviours against the target and the kinds of effect the target may have on the threat (Little & Rogova, 2006). One of the critical questions is how the interaction between athreat and a target system in cyberspace can be modelled and analyzed. Information security literature offers several possibilities, but the studies are mostly domain-specific, and in many cases, the approach is technical or otherwise detailed. The threat is a hacker, and the target is an information system or only part of it. Schechter (2004) has a slightly broader view on the interaction. He claims that with threat scenarios, it is possible to explore the causes of information system security failures and the reasons they occur. The examination should start with a simple primary threat, then creating individual threat scenarios and expanding them into multiple scenarios. The scenarios can be presented as event trees or Directed Acyclic Graph (DAG), including the security controls mitigating the threat. Schechter argues that scenarios can establish a common understanding of the events. (Schechter, 2004.)

Alkire, Lingel and Hanser (2018) introduced a command and control (C2) resilience tabletop exercise model. It is designed to compare alternative C2 concepts in a given scenario. The model does not focus on a traditional information system but a military command and control system. The unique feature of this model is retrospective futurology. The scenarios are examined in the past tense. The mission in the scenario has already occurred before the examination of the situation. The objective of the model is to examine and identify essential qualities, risks and resilience of the C2-system in different scenarios. The qualities are assumed to have failures, and the participants assess their consequences and ways to increase system resilience. (Alkire, Lingel & Hanser, 2018) Retrospective futurology does not focus on the probability of an event. Therefore, it is an appropriate approach when the phenomenon includes low probability and high consequence events, typical in cybersecurity.

3.4 Data, information, knowledge and wisdom

The strategic analysis of cybersecurity is a process where the collected cybersecurity data is refined to information and knowledge, and eventually to the decision-makers' wisdom. Ulicny, Moskal, Kokar, Abe and Smith (2014) emphasize that cybersecurity requires information about the environment and decisions based on knowledge (Ulicny et al., 2014). The transformation from data to wisdom is typically presented with the data–information–knowledge–wisdom (DIKW) hierarchy. It is commonly used to contextualize different information levels and describe lower-level data transformation to a higher-level entity. The hierarchy is based on the assumption that data is utilized to create information, information to create knowledge, and knowledge to create wisdom (figure 4). (Rowley, 2006, p. 164.)

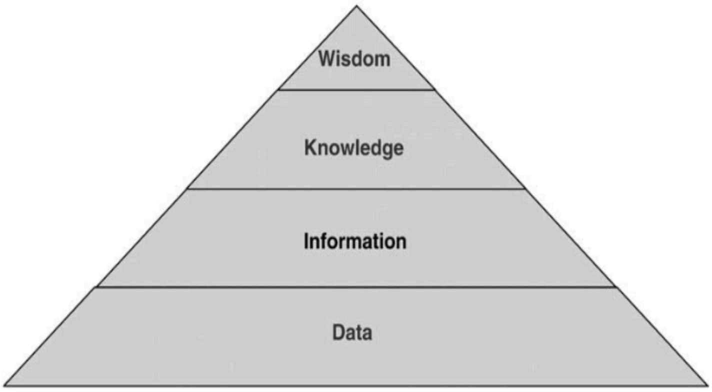

FIGURE 4 The DIKW-hierarchy.

Ackoff (1989) defines data as symbols that represent properties of objects, events and their environment. It is the product of observation. The difference between data and information is functional, not structural. (Rowley, 2006) Liew claims that data are recorded symbols and signal readings. Symbols can be words, numbers, diagrams, and images. Signals include a sensor or sensory readings. The primary purpose of data is to record activities or situations to capture an accurate picture or real event. Eventually, all data is historical, except if it used for illustration purposes. (Liew, 2007.)

Rowley (2006) studied 16 different textbooks regarding DIKW-hierarchy. She summarizes that data has no meaning or value because it does not have any context or interpretation. It is facts or observations that are unorganized and unprocessed and do not express any specific meaning. Data items are an elementary and recorded description of things, events, activities and transactions. Rowley points out that the different definitions of data include, in most cases, what data is not, instead of what it is. For example, data lacks meaning or value; data is unorganized and unprocessed. However, data lays the foundation for defining information. (Rowley, 2006) Liew (2007) states that data management includes the capture, storage, structure, compilation, retrieval, and analysis of records. It is the reconstruction of recent or historical events that serve as inputs for decision-making (Liew, 2007).

Ackoff (1989) explains that information is contained in descriptions. Information systems generate, store, retrieve and process data. Information is inferred from data. (Rowley, 2006) Liew (2007) determines that information contains a relevant meaning, implication, or input for decision or action. It may come from current or historical sources. The purpose of the information is to support decision making, problem-solving or identifying an opportunity. (Liew, 2007) According to Rowley (2006), information is defined in terms of data because it is usually seen as organized or structured data. Processing data to information gives data relevance for a particular purpose or context. It makes it meaningful, valuable, useful and relevant. The process phases are classification, rearranging/sorting, aggregating, performing calculations, and selection. (Rowley, 2006) Information management, in this context, includes reconstructing a picture of historical events, collecting current or recent intelligence and projecting possible future events. It also includes the analysis for decision making. (Liew, 2007)

Knowledge is know-how. It enables transforming information into instructions. Knowledge can be acquired from another actor or extracted from experience**.** (Rowley, 2006) Liew (2007) claims that the purpose of knowledge is to create or increase value for the organization and stakeholders (Liew, 2007). Typically, knowledge is defined based on the information. Some scholars argue that the process converts information into knowledge; others explain that it adds ingredients to information. Knowledge can be understood as a mix of information, understanding, capability, experience, skills and values. It is actionable information and information combined with understanding and capability. (Rowley, 2006) Liew (2007) argues that managing knowledge includes managing human, relationship, social, and structural capitals. It also can include managing the source and the flow of knowledge in knowledge creation, sharing, and application. All of these are intended to create and sustain organizational value and competitive advantage. (Liew, 2007)

Wisdom is the ability to increase effectiveness and add value with judgement. The ethical and aesthetic values are unique and personal, and natural to the actor. Defining wisdom is more complicated than defining other levels of the DIKW-hierarchy. Wisdom is closely related to human intuition, understanding, interpretation and actions. (Rowley, 2006.)

There are several other hierarchy presentations, but most of them recognize the key elements: data, information, knowledge, and wisdom. Some models may have some additional levels like understanding, intelligence or enlightenment. Nevertheless, the higher elements in the hierarchy are typically explained using the lower elements in a transformation process. The challenge, in real life, is to understand and explain how data is transformed into information, information transformed into knowledge, and knowledge transformed into wisdom. There is more data than information, more information than knowledge and more knowledge than wisdom. With this reasoning, wisdom can be obtained only after the processing of data, information and knowledge. (Rowley, 2006.)

Nevertheless, the process starts with data (Rowley, 2006). Liew (2007) reminds that data and information have two sources, activities and situations. Both of these generate data that can be captured or lost. When data are captured, activities and situations generate information that has relevant meaning. A situation is a context that affects decisions. Once data and information are captured and stored, they can be processed into information through compilation and analysis. Liew criticizes the definitions because most of them share a common anomaly. They are defined as related to each other. He accepts these definitions if the objective is to describe the inter-relationships. Nevertheless, the typical definitions are circular. (Liew, 2007.)

The process to develop data into information, knowledge and wisdom is built-in in the information fusion process. The purpose of information fusion is to exploit prior knowledge and the information collected from different sources. Information is used to assess the states of an environment and the threats within. Higher-level fusion integrates different data types that can include objects of interest and their attributes, the relationships between them, their behaviour, subject-matter expertise and domain knowledge. The result of a higher-level fusion is a coherent understanding of current and predicted situations. (Little & Rogova, 2009.)

Syed, Padia, Finin, Mathews and Joshi (2016) emphasize that data and information are scattered as isolated pieces in cybersecurity. Data and information are generated by different tools, sensors and systems, using different standards and formats and published by different sources. Cybersecurity data can be available in structured, semi-structured or unstructured forms within or outside of the organization. Unifying scattered information can support in-depth investigations and help transition from a reactive approach to a more proactive and, eventually, a predictive approach. (Syed et al., 2016.)

3.5 Conclusions of the theory

Ontologies aim to describe reality, making it understandable and manageable. They enable structuring the various elements, their attributes and relationships in and with an environment. The dynamic spatial ontology supports excellently describing a dynamic phenomenon, like cybersecurity. Together with the threat ontology, it enables identifying the spatial and temporal entities of cybersecurity, their relations and the operational environment. Furthermore, the threat ontology enables identifying the components of intention, capability and opportunity, providing the baseline for the interaction examination of the threat and the target system. However, even when the different ontology theories identify the internal and external relations of the spatial and temporal entities, they do not fully support the interaction analysis between the threat and the target system. Therefore, interaction analysis must be based on another type of modelling. Most of the interaction models in information security are too detailed and technology-oriented for the strategic analysis. Therefore, models supporting strategic interaction analysis and strategic scenarios are required.

Ontologies can enhance the process and results of the analysis. An ontology, covering the essential parts, relations and activities of the entities, constitutes a solid base to start the analysis process. Careful and thorough modelling of the phenomenon, using an ontology, allows understanding all the participating essential items, their actions and the results of the actions. Furthermore, understanding the phenomenon enables the identification of already collected and stored data. It identifies the data that is yet missing and must be collected before analysis. This requirement covers all the entities, the threat, the target system and cyberspace.

It is essential to understand the objectives of the analysis. It should provide reliable and valid knowledge to decision-makers to enable timely and proactive decisions regarding cybersecurity development and operations. The analysis requires resources for data collection and analysis to refine the collected data into information, knowledge and eventually to the wisdom of the decision-maker.

Relevant cybersecurity literature includes several studies where a domain-specific ontology is used in domain-specific cybersecurity research. Due to their domain-specificity, they are relatively detailed and, therefore, not employable in strategic cybersecurity. On the other hand, foundational ontologies are domain-independent and exploitable also in strategic analysis of cybersecurity. The ontologies used in this research support describing the elements and strategic cybersecurity environment for an analysis model. However, these ontologies do not exclude the need for foundational cybersecurity ontology. Foundational upper ontologies of cybersecurity could enhance the design of domain-specific cyber ontology and the integration of cybersecurity to other disciplines and threat landscapes.

Based on the threat ontology, the strategic cybersecurity analysis model should include the entities of a cyber threat, a target information system and cyberspace. A dynamic spatial ontology indicates that the model should identify the spatial and temporal elements of these entities. Furthermore, the threat ontology requires modelling an interaction between a cyber threat source and a target system, identifying the components of intention, capability and opportunity. Based on the utilized theories, these are the main elements of the strategic cybersecurity analysis model.

4 STRATEGIC CYBERSECURITY ANALYSIS

4.1 Background of the analysis model

4.1.1 Classification of the entities

Anything that includes parts has a structure that relates these parts to each other. One of the first steps of analysis is to determine an appropriate structure for the analytical problem to identify the parts and collect information. (Heuer, 1999) The strategic cybersecurity analysis includes the following components: the cyber threat source, the target system, their activities, the environment, and the interaction between all of these components. These components are divided into detailed parts in order to enable the analysis. Furthermore, the analysis considers the traditional components of a threat: intention, capability and opportunity (see Steinberg, 2005).

First of all, the analysis aims to identify all the parts that make the spatial entities, including the internal relations between the parts. Secondly, the analysis aims to identify the temporal entities, including the external relations between the temporal and spatial entities, the processes and their participants. Furthermore, the analysis aims to identify the spatial entities of cyberspace and the temporal entities intended to modify it. The spatial entities, temporal entities and the environment are kept separate at the beginning of the analysis. This separation enables the analysis of one entity without the interference of the other entities. If the entities are analyzed together, a change in any of them will cause a need to reanalyze all of them. All the entities are combined in the last phase of the analysis.

Identification of the parts requires their classification. A classification with detailed subcategories provides several advantages. It allows identifying the related entities of the phenomenon and ensures that all the significant elements and parts are noticed. Furthermore, a classification helps to identify the sources where the information regarding the entities may be found. It also supports structuring the collected data and information, providing a taxonomy and a partonomy regarding the phenomenon. An example of taxonomy and partonomy, modified to cybersecurity, is presented in figure 5 (figure 5). (see Jansen, 2018, p. 193.)

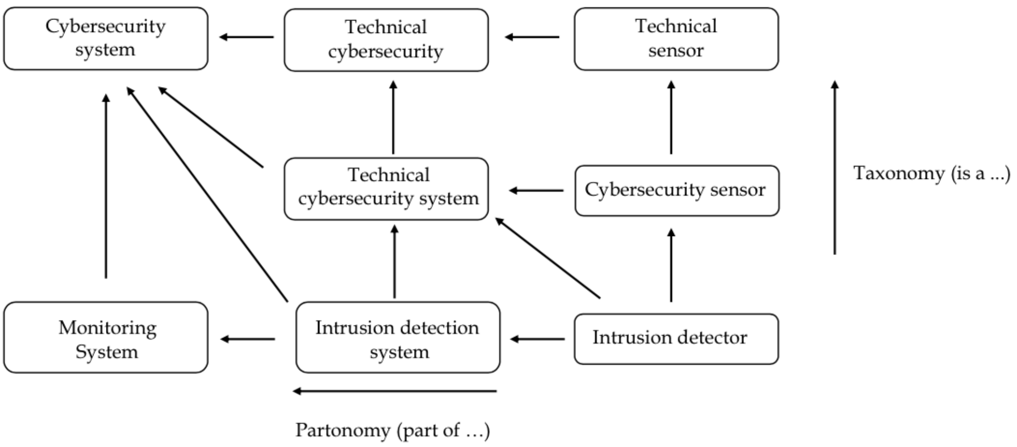

FIGURE 5 An example of taxonomy and partonomy.

For the classification of the components, several options are available. The preferred model depends on the objective, approach, and details required in the analysis. The phenomenon can be classified on a strategic level, for example, based on DIMEFIL-, PMESII- or DOTMLPF -models.

The typical method to describe any nation is the PMESII-model, broadly identifying political, military, economic, social, infrastructure, and information elements. It can be used in complex analysis or just as an outline (McDonnell, 2009). On the other hand, national power instruments are typically described using the DIME-model, covering diplomatic, informational, military, and economic assets. In some cases, it is extended to DIMEFIL-model, also introducing financial, intelligence, and legal instruments. Both models represent national means. (McDonnell, 2009) The PMESII–model can describe adversary, friendly, allied or neutral systems, regardless of whether they are nation-states, different groups or organizations (McDonnell, 2009). Typically, the adversary matches its DIMEFIL-instruments against our PMESII-elements and vice versa (McDonnell, 2009). However, several other models are also available for classification. For example, Lehto and Limnéll (2016) assessed the cybersecurity capability of Finland using categories of PMESII, DOTMLPF-II, Global Cybersecurity Index (GCI), EU cybersecurity dashboard and Microsoft security intelligence report (Lehto & Limnéll, 2016).

DIMEFIL and PMESII consider mostly national level elements. When the analysis of strategic cybersecurity focuses on a national level, these models may provide appropriate classification tools. On the other hand, if the analysis requires more concrete and measurable elements, a version of DOTMLPF can provide an appropriate model. The model stands for doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOD Dictionary, 2020). The basic model can be supplemented with, for example, interoperability and information, into DOTMLPF-II -model (Lehto & Limnéll, 2016) or with policy, extending it to DOTMLPF-P -model (DOD Dictionary, 2020).

The classes of DOTMLPF-II and -P hold the following definitions. A doctrine (D) is a fundamental government policy or a military principle (Merriam-Webster, 2020). A doctrine defines how the conflicts are fought (Lehto & Limnéll, 2016). Organization (O) discloses how the entity is organized to fight, and training (T) how the organization is improving its capabilities and preparing to operate. Materiel (M) includes the necessary equipment and systems required to operate and fill capability gaps. Leadership and education (L) describe how the leaders are educated and what is their professional development. Personnel (P) exposes the availability of qualified personnel. Facilities (F) are different types of properties and installations that support the forces. Interoperability (I) is the ability of the forces to operate efficiently. Information (I) includes the demands of the data, information and knowledge needed in the capabilities and processes. (Lehto & Limnéll, 2016) Policy (P) is a high-level overall plan embracing the general goals and acceptable procedures, especially of a governmental body (Merriam-Webster, 2020).

The DOTMLPF-II and -P -classifications enable a thorough understanding of the components in the analysis, the threat source, the target system, their activity, cyberspace and interaction. Furthermore, they also help identify the variables behind intention, capability and opportunity (see Steinberg, 2005). An intention is a psychological element of the threat and, respectively, of the own cybersecurity. Information declaring the intention can be discovered from different policy, strategy and doctrine documents or an organization's leadership. Presumably, the actual intentions are not always declared openly. Therefore, they can be assessed based on the activities of the organization. Intention includes both spatial and temporal entities.

The spatial elements of capability include materiel, personnel, organization and facilities. The temporal elements of the capability include training and interoperability. Furthermore, any process aimed to develop or use the elements of the capability is a temporal entity. Information can be utilized to promote or conceal capability.

The third element, the opportunity, is based on the intention and the capability. It is also closely related to the information. From the adversary's perspective, the objective is to keep the achieved or unfolded opportunity concealed from the defender until the opportunity is exploited. From the defender's point, the objective is to conceal the vulnerability that may provide an opportunity for the adversary. The concealment should be retained until the opportunity window is closed from the adversary utilizing own cybersecurity measures. However, there is always a possibility to exploit the existence or non-existence of the opportunity in information influencing. In cybersecurity, an opportunity is also closely related to the attributes and modifications of cyberspace.

Classification provides a tool for defining a taxonomy and a partonomy of the phenomenon. The strategic cybersecurity analysis can utilize models that are already available or create a new one if required. On the other hand, partonomy and taxonomy support identifying the parts and their relations of the cyber threat source and the target system. For the analysis, it essential to identify if the entity is unitary or dispersed. Especially in the dispersed entity, it is essential to identify if the parts are connected as an aggregate or a whole. Classification allows defining the key characteristics, the properties for measuring, and the scale and the unit type. Classification and related measurements support the analysis, but they also enable the documentation of the analysis process and increase the reliability and replicability of the analysis.

4.1.2 Measurement of categories

The quality, reliability and usability of the strategic cybersecurity analysis can be increased by measuring the determined categories, subcategories and individual parts. Singleton (2005) defines measurement as a process that assigns numbers or labels to units of analysis. The objective is to represent the conceptual properties (Singleton, 2005). As relevant literature indicates, quantitative measurement in risk management provides reliability, but includes challenges collecting relevant data for the analysis. On the other hand, qualitative analysis is considered questionable, because it relies on expertise. However, a rich description of the phenomenon can provide a common understanding. Vandepeer (2011) argues that a risk management process includes more depth and rigour than an intelligence threat assessment based on an analyst's personal experience. Furthermore, intelligence analysis often lacks transparency and replicability (Vandepeer, 2011). Intelligence discipline has identified this deficiency. Analysis literature has introduced several methods to increase transparency and replicability (see Hibbs Pherson & Pherson, 2017).

Measurement requires the identification of the essential characteristics and the selection of the attributes that reflect the phenomenon. Furthermore, measurement in cybersecurity requires an appropriate way to combine the attributes. The unit of measurement, the scale type and the instrument used in the measurement require thorough consideration. The instrument should produce an appropriate unit in an appropriate scale type, and the results should be able to combine. A structural model for cybersecurity measurement is presented in figure 6 (figure 6). (Pfleeger, 2009, p. 40.)

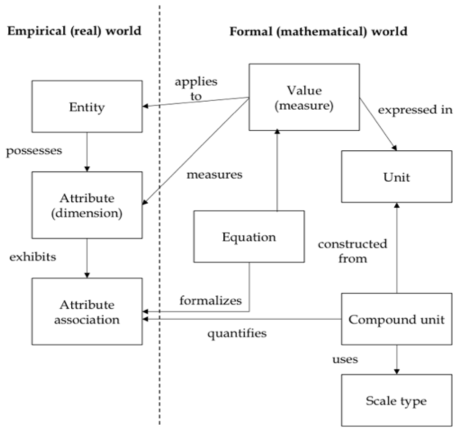

FIGURE 6 Structural model for cybersecurity measurement.

Valuable metrics are clear and unambiguous, and support information collection and decision-making and decrease subjective interpretation. Both quantitative and qualitative measurements are appropriate. Qualitative scales help measure abstract factors, like intention or threat. In some models, abstract factors are presented quantitatively, but the measurement is based on predetermined qualitative criteria. (Mateski, Trevino, Veitch, Michalski, Harris, Maruoka & Frye, 2012) The method for measurement and the metrics used in the cybersecurity analysis depends on the objective, perspective and granularity of the analysis.

Measurement should cover all the classes and sub-classes of the analysis, including the spatial and temporal entities and the components of intention, capability and opportunity. Strategic cybersecurity is such a complex phenomenon that purely quantitative measurement is likely unattainable. Quantitative measurement needs to be supported by a rich and comparable qualitative measurement. Measurement provides several advantages. It increases the understanding of the different entities and their actions; it supports comparing the threat and target system's spatial and temporal entities. It also supports the documentation and presentation of the analysis results. Furthermore, measurement enables monitoring the development of the threat, target system and cyberspace, providing an appropriate incentive for a new analysis.

4.1.3 Identifying future capabilities

The strategic analysis focuses on future capabilities and environment. Current capabilities might provide a baseline for the analysis. However, the objective is to identify the development of the adversary's capabilities and cyberspace so early and reliably that it enables the development of own cybersecurity accordingly. The capability can be analyzed with three different approaches; capability design, development and deployment (Steinberg, 2005).

Capability design is related to concepts, theories and technologies, setting the base for capability development. Capability design is based on the objectives presented in different strategy and doctrine documents. Several concepts can precede official doctrines, including extant capabilities later incorporated into plans and practices. New concepts and doctrines may also require new types of activities, requiring new ways to operate, new capabilities, personnel, and infrastructure. Training can also be used to test new concepts. (CJCSI, 2016) Furthermore, the capability design is closely related to intentions and objectives. They determine what kind of capabilities are required in the future. For the strategic analysis, monitoring adversary's capability design is essential to understand the future development, and eventually, gaining an advantage. (see Steinberg, 2005.)

The second element is capability development, including the adversary's activity aimed to increase its performance. When using DOTMLPF-II- model, the development applies to all the elements. Furthermore, in cybersecurity, capability development applies also to cyberspace. Intentional modifications to cyberspace can increase the capability of the adversary, either permanently or temporarily. Furthermore, changes to cyberspace might also create opportunities for adversary operations. Nevertheless, any change in the capability design results in a change in the capability development of spatial and temporal entities and the environment. (see Steinberg, 2005.)

The third element is the ability to deploy and deliver the designed and developed capability (Steinberg, 2005). This element is addressed in more detailed in the last phase of this analysis process.

4.1.4 The activity analysis

The analysis of the capability development considers mainly spatial entities, but it also includes the temporal entities, the processes. As a reminder, temporal entities are the different activities the spatial entities, like a threat source and a target system, are executing (see Grenon & Smith, 2004). Analyzing a process requires also the analysis of the participating spatial entities (Bittner & Smith, 2003). Temporal entities include the activities of the threat source and target system and the interaction between them.

Typically, an activity includes the beginning and the ending, the endurance and the changes and the peak moment. For the analysis, the particularly interesting objects are these discontinuities. They indicate a change, a new phase in the process. The peak moment of a process usually defines the outcome of the activity. These instantaneous moments enable the determination of the level of the change, duration and telicity of the process. For example, identifying the peak moment is essential when determining applicable countermeasures executed before the peak moment. If the process is terminated before the peak moment, the result of the process may change. (see Jarrar & Ceusters, 2017.)

The activity analysis covers the external relations between spatial and temporal entities, the relationship between processes and the participating entities. Although a process depends on a participating spatial entity, the relationship is typically bilateral. The spatial entity can affect the process, but the process can also affect the spatial entity. The impact can be active, passive or indirect. Changes in attributes can be an indicator that certain changes are taking place. (Little & Rogova, 2009.)

Jarrar and Ceusters (2017) argue that processes are more challenging to classify than spatial entities. They propose a distinction between the temporal parts and the occurrent parts of processes. Moreover, they divide a process into three levels: change, duration and telicity. An action is telic if it has a goal; otherwise, it is atelic. The example of temporal classification modified to cybersecurity is presented in figure 7 (figure 7). (see Jarrar & Ceusters, 2017, p. 2.)

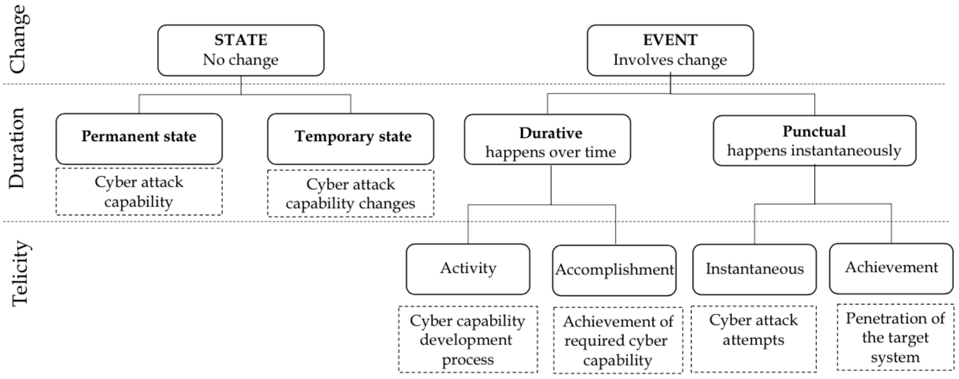

FIGURE 7 Example of a temporal classification in cyberspace.

The analysis of a process requires identifying the process, the participating spatial entities and their role. Furthermore, the analysis requires the identification of different types of discontinuities inside the process. These can be the beginning and ending of the process, the changes that occur during the process and the peak moments of the process. These identified elements enable structuring the process, identifying and monitoring the changes, assessing the results, and identifying the moments when own countermeasures are most efficient.

4.2 General description of the analysis model

The strategic cybersecurity analysis starts with the analysis of the spatial elements of the cyber threat source. The analysis includes assessing the adversary's future objectives and intentions and future capabilities to achieve these objectives. The capability analysis may require analyzing the adversary's current capabilities to set the baseline for future capability assessment. When the objectives and available spatial capabilities are analyzed, the analysis focuses on the temporal entities, the processes the identified adversaries can execute.

The second phase of the analysis focuses on the target system. In this context, the target system comprises of own information and communication technology systems (ICTs) and cybersecurity controls. The analysis includes the assessment of current ICTs and cybersecurity controls and also the objectives to develop them. In addition to the spatial entities, also temporal entities are addressed; the processes ICTs and cybersecurity controls are capable of executing. However, the identified future development of own ICTs and cybersecurity controls set only a baseline for actual future cybersecurity design and development. Eventually, the final results of this strategic cybersecurity analysis determine the defender's cybersecurity development requirements. As in the case of the threat source, also here, the analysis of the spatial and temporal entities is executed separately.

The third phase of the analysis covers the environment, cyberspace. If required, the analysis can focus first on the current cyberspace. Nevertheless, the main objective is to identify the future operational area and the main characteristics of cyberspace. The impact of the environment is assessed from both the adversary and own point of view. Also, in this case, the analysis is preliminary. The results of this strategic cybersecurity analysis indicate the required actions to cyberspace in order to increase a defender's advantage and decrease adversary's opportunities. The impact of cyberspace on capabilities and operations is more significant than a traditional environment. Therefore, cyberspace requires special attention in the analysis.

The last phase of the analysis focuses on the interaction between the threat and target system in cyberspace. This phase assesses the adversary's future capabilities and operations against the defender's capabilities to secure ICTs. The objective of this phase is to confirm the adversary's objectives, capabilities and operations. It also provides knowledge for own cybersecurity capability design, development and cyberspace modifications. This knowledge aims to increase own advantages while minimizing adversary opportunities. Achieved results support future cybersecurity development plans.

The upper-level structure of the strategic cybersecurity analysis model is presented in figure 8 (figure 8).

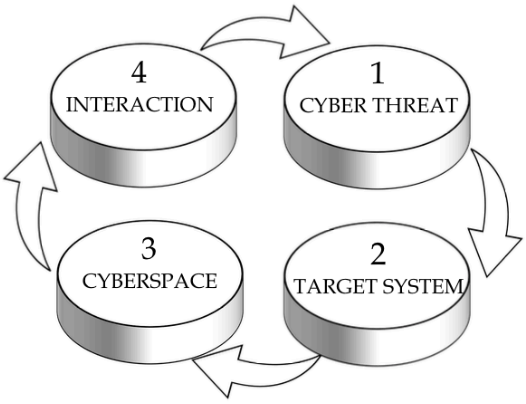

FIGURE 8 The upper-level structure of the cybersecurity analysis model

4.3 The first phase – cyber threat

4.3.1 The intention of a threat

The objective of the first phase is to identify the threat sources, their intentions, parts, qualities, spatial locations and activities. This first phase of the analysis covers, first of all, the spatial entities and the internal relations connecting their parts. Furthermore, the analysis focuses also on the external relations connecting the spatial entities to the temporal entities. The structure of the first phase is presented in figure 9 (figure 9).

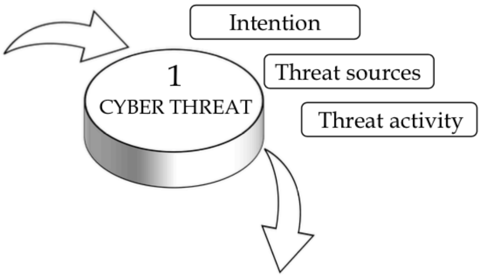

FIGURE 9 Analysis of a cyber threat

Although the focus is on the threat sources, the first step concerns the own ICTs, the target system. This preliminary step aims to examine the factors that make own ICTs a possible target, identify the valuable assets in the system, or identify the value of the ICTs themselves for possible threat actors. Assessing the target system's valuable assets enables identifying possible threat sources and their intentions (see JP 2-01.3, 2014). At this point, detailed analysis is not required. The objective of this step is just to identify the possible threat sources.

As a target system, own ICTs have a specific value for the threat source. This value can be assessed by examining the declared or otherwise disclosed adversary's objectives and intentions. The focus should be broader than just cybersecurity. Furthermore, the actions in cyberspace may not be the final objective, and they may cause consequences also in the physical or information domain (Ormrod & Turnbull, 2016). The intentions can be resolved from different documents, declarations of the adversary leadership, or the adversary's activities. These activities can be related to research and development, training, operations or capability development. If the probable threat source is a nation-state, probably much information, classified or unclassified, regarding the intentions are available. Also, the activities of a large organization are difficult to conceal. On the other hand, if the threat source is an individual or a small group, the intentions are likely expressed more unofficial manner, if expressed at all beforehand. These unofficial declarations can be different types of announcements or messages in social media or another appropriate medium. The actions of the small actors may be difficult to identify.

Mateski, Trevino, Veitch, Michalski, Harris, Maruoka and Frye (2012) divide threat attributes into commitment and resource attributes. Commitment attributes describe the willingness of a threat source, the intention. It can be divided into three sub-classes: intensity, stealth and time. These classes can be utilized when assessing the level of intention. Intensity describes the determination to pursue the objectives and the risk levels a threat source is willing to take. (Mateski et al., 2012) Intensity can be assessed based on how much resources an adversary is willing to allocate for the objective. Furthermore, the frequency of the activity or the consequences an adversary can tolerate can indicate intensity.

Stealth describes an adversary's ability and will to maintain a certain secrecy level when pursuing the objectives. A higher level of stealth allows a threat source to hide, causing difficulties for the defender on intelligence collection and threat identification and eventually challenges in threat mitigation. (Mateski et al., 2012) Assessing the level of an adversary's stealth is a challenge. Nevertheless, if an adversary's actions to maintain the stealth are identified, there might be a way to assess how much resources the adversary allocates for that task. Likely, the more resources are used for stealth, the more prominent is the intention and the objectives.

Time is a temporal resource a threat source uses when achieving the objective. The more time an adversary is willing and able to commit, the more potential a threat source has for devastating impacts (Mateski et al., 2012). Time is an essential factor, especially in strategic analysis. Likely, the more time the adversary is willing to use, the stronger is the intention, and the more important are the objectives. The analysis should also take note of some historical time aspects of the intention for a perspective.

The information has a role in either promoting or concealing the intention. Information can be incomplete or intentionally incorrect, presenting the intensity, stealth and time in the way that supports the adversary. An adversary can execute influence operations to disseminate propaganda to pursue a competitive advantage over the defender (Waltzman, 2017). The information environment includes both technical and psychosocial dimensions, where the influence operations fall into the psychosocial dimension. The adversary tailors the information influence based on the target organization's history and culture. (Waltzman, 2017) The objectives can include deceiving the defender, discrediting its decision-makers, and disorienting and demoralizing public and armed forces (Rugge, 2018). Miskimmon, O'Loughlin and Roselle (2013) claim that the states strive to construct credible narratives about issues, identities and the nature of the international system. A strategic narrative is a deliberate choice. (Hellman & Wagnsson, 2017) Identifying a threat source's intention requires a more comprehensive approach than just cybersecurity.

Intensity, stealth and time are not imminent elements of the intention. However, they provide classification and general metrics for assessing the importance of the intention and how prominent risk an adversary is willing to take to achieve the objectives. They also support the analysis by prioritizing an adversary's possible actions to fulfil the intention. The greater the incentive is to attack, the more likely the attack is than other options the adversary might have (Schechter, 2004).

The role of the information might be more extensive than just cybersecurity, as cybersecurity can be only one element in the strategic influence. Therefore, the information regarding the intention should be examined in a larger context than cybersecurity. The intentions regarding cybersecurity might be embedded in the strategic level of information operations and narratives.

4.3.2 Threat sources

Several possible cyber threat sources are likely discarded in the previous step due to a missing or irrelevant intention for malicious action against the target system. Nevertheless, it is essential not to limit too much of the possible threat sources. In some cases, a cyber threat source itself may have no relevance regarding the target system, but a third party can use it for malicious activities.

Depending on the target system, potential threat sources can be individual hackers or disgruntled insiders that execute their agendas with cyberattacks. They can be criminals, aiming to have financial or other personal benefits. A threat source can also be terrorists or other malicious groups in order to advance their cause. It is also possible that commercial organizations constitute a threat source when executing industrial espionage or disrupting competitors to gain a relative advantage. Inherently, nation-states can be a threat source, using cyberspace to achieve diplomatic, information, military, or economic advantages. (Hundley & Anderson, 1995.)

The classification and accuracy depend on the context. Threat sources may be divided into nation-state or non-state threats, non-state threats into groups or individuals, or intentional or accidental threats (JP 3-12, 2018). Eventually, threat sources should be classified into appropriate categories, depending on the objectives of the analysis.

After the general level classification, the identified and probable cyber threat sources require more detailed analysis. The objective is to identify and assess the threat sources of the future. In some cases, this might require analyzing current threat sources to identify the baseline for future analysis. From the ontology point of view, a cyber threat source is a spatial entity that consists of independent substantial entities, dependent qualities, and locations in spatial regions. The analysis starts with identifying spatial entities having a continuous existence and keeping their identity even if they change. (Grenon & Smith, 2004; Bittner, 2019a.)

If a cyber threat source is classified according to DOTMLPF-II -P, the substantial entities of the capability are materiel, personnel, organization, facilities, training and information. Training is, in fact, a temporal entity, a process, but in this context, it can be utilized to describe the level of the skills of a threat source. A classification guides where to find relevant information regarding the categories of the substantial entities. Also, here information is closely related to capability, either promoting or concealing it. It does not directly affect the capability, but it can affect how the defender sees the threat source capability.

Cyber threat sources are composed of different parts that can create either an aggregate or a whole. Aggregates and wholes may have the same items, but only in the whole, the parts are foundationally connected (Little et al., 2008). From the capability and readiness point of view, this difference is significant. Only a whole can constitute a viable threat. A cyber threat source that is an aggregate constitutes only a possible threat and requires some development to become viable. Strategic analysis should identify if the relations of the parts have a foundational dependence, even when the parts are dispersed. Furthermore, the analysis should identify the required development towards a viable cyber threat and the time required.

Wholes can be complex by nature, consisting of items that can be difficult to categorize, especially in cybersecurity (see Little & Rogova, 2006). The analysis aims to find the parts and capture the foundational dependences that connect the parts inside the whole. Identification of the connections allows recognizing the threat source parts, even if they are dispersed over space and time. The analysis also helps to understand the internal structure, relations, roles and the importance of the threat source parts. The connections are probably not always directly observed, but they can be inferred from the states of entities, their context and other connections (Steinberg, 2005).

When a threat source is a unitary whole, as an individual hacker, the parts are probably easy to recognize. However, in cyberspace, most of the threat sources are likely dispersed over the network, physically, logically and socially (see Steinberg, 2005). Therefore, a threat source can be a physical entity, a logical entity, a cyber-persona, or a combination of all these (JP 3-12., 2018).

All the parts of a whole are not equally important. A single part of a threat source can be essential for the existence of the threat. On the other hand, the existence of a non-essential part can be only conditional (Little et al., 2008). These essential parts may constitute the center of gravity of a cyber threat source (see JP 2-01.3, 2014). Furthermore, capabilities and parts of a cyber threat source that do not meet the adversary's assessed doctrine requirements can be considered vulnerabilities. Similarly, capabilities that meet or exceed the doctrine requirements can be considered strengths. (see JP 2-01.3, 2014.)

After the different parts and their connections in categories are identified, the analysis focuses on the dependent entities; the qualities of the substantial entities (see Grenon & Smith, 2004). The objective is to identify and evaluate the capabilities and the possible limitations of the adversary (see JP 2-01.3, 2014). Together with the substantial entities and their interdependences, the attributes expose the capability of a cyber threat source (see Little & Rogova, 2009). Cyber threat source attributes can include different features, qualities, roles, states and functions, that determine the capability. Qualities can also include composition, disposition, strength, training status, effectiveness, personalities and other miscellaneous attributes (see JP 2-01.3, 2014).

Changes in the attributes can be indicators of a significant change in the status of a threat (Little & Rogova, 2009). Substantial parts, attributes and locations of cyber threat sources can change periodically. However, as long as the threat source maintains its identity, it constitutes the same threat source. Locational change can mean physical or logical move or changes to boundaries. Qualitative changes can modify the qualities of a threat source. A substantial change typically means the termination of the object. (Iwaniak et al., 2013; Grenon & Smith, 2004.)

Lehto and Limnéll (2016) argue that available doctrines reveal some details about the capabilities. Nevertheless, resource allocation to cyber capabilities might constitute the clearest indicator of capability (Lehto & Limnéll, 2016). Mateski, Trevino, Veitch, Michalski, Harris, Maruoka and Frye (2012) argue that the higher capability a threat source possesses, the easier, with fewer resources and less time, it can achieve determined objectives. Furthermore, a significant capability enables achieving also challenging objectives. (Mateski et al., 2012.)

Measuring the cyber threat source's capability can be executed quantitatively, including the number of personnel, materiel or the different resources available. On the other hand, the capability can be compared, quantitatively or qualitatively, to the capabilities required in the adversary's assessed future doctrine or strategic objectives. The comparison can also be made against the defensive capabilities of the target system.

4.3.3 The threat source activity

After the adversary's objectives and the spatial entities are identified, the analysis focuses on identifying an adversary's possible activities, the temporal entities. Due to mutual dependence, the analysis of temporal entities also includes spatial entities. The role and activity of a spatial entity determine how easy it is to identify the related temporal entities. The more active role a spatial entity has in a process, the likely the process is identified. For example, if a spatial entity engages a process, the process is identifiable through the spatial entity. On the other hand, if a spatial entity's role is passive, identifying the process can be challenging. On the other hand, an identified process may reveal previously concealed spatial entities. Furthermore, an adversary's intentions, objectives and the end states can reveal what kind of processes and capabilities are required to achieve these objectives. The identified objectives and processes support the identification of spatial entities, even if they have not been identified in the earlier phases of the analysis. A process can bring out the spatial entity's existence, prolong the existence, degrade or even destroy the spatial entity (see Little & Rogova, 2009).

An assessed adversary's design and development of the capabilities provide the basis for analyzing an adversary's activities. An activity analysis focuses on the deployment and delivery of cyber capabilities; how an adversary executes cyber operations in the future (see Steinberg, 2005). This step is close to a traditional assessment of an adversary's courses of action. It is based on the intentions, capabilities and opportunities available for an adversary. The analysis aims to identify the types of operations cyber threat sources are capable of executing. Furthermore, the analysis reveals how the components of the threat source participate or support cyber operations. If the adversary is assumed to have several different activity options, the analysis should identify their probabilities. (see JP 2-01.3, 2014.)

The reliability of the adversary's activity assessment is challenging. However, there are ways to decrease the margin of error. The previous steps have already revealed some boundaries that limit an adversary's activity. First of all, the activities are based on the assessed intentions of the adversary. The intentions can reveal likely objectives, desired end states, and the activities they require. (see JP 2-01.3, 2014) Secondly, the type of activity depends on the capabilities required to achieve the objectives and are available for the adversary at a determined timeframe. Identification of the capabilities enables assessing the courses of action the adversary is capable of executing. Thirdly, activities are also limited by the opportunities that determine the timing of the activity.

The assessment regarding the adversary's courses of action should meet specific criteria. The assessed actions should support the adversary's likely objectives. Furthermore, the adversary should have sufficient time, space and resources to execute the activity, maintaining risks on an acceptable level. The assessed courses of actions should be consistent with the adversary's modus operandi, but at the same time, analysis needs to identify deception. (JP 2-01.3, 2014) An adversary's training can indicate some elements of the possible courses of action. All these factors and limitations of the adversary's activity should be considered in the activity analysis. A thorough understanding of the doctrine and the threat source's mindset is required to assess the actions reliably (JP 2-01.3, 2014). This understanding of the modus operandi can be based on the doctrine, tactics, psychology, and the adversary's historical patterns (Lemay, Knight & Fernandez, 2014).

The activity analysis focuses on the deployment and delivery of the adversary's future cyber capabilities. Nevertheless, there should be feedback to the analysis of the adversary's capability design and development. For example, comparing the adversary's objectives, available capabilities, and activities may reveal the adversary's capability gaps. These capability gaps can be actual, indicating that the threat is not yet viable, or the capability is adequate only to limited objectives. On the other hand, some of the capability gaps can be capabilities that the defender has not yet identified. Nevertheless, assessed and identified capability gaps require additional information collection to assess the development of the threat or identify the concealed capabilities.

The analysis of a cyber threat should be followed by active information collection and monitoring of the threat. Monitoring allows the identification of new elements of threat sources. Furthermore, it supports identifying significant changes in capabilities and intentions. Measurement of the collected information supports identifying the changes and contributes to the quality control of the analysis by allowing improvements in reliability and validity. Monitoring can also provide an incentive to update the current strategic analysis.

4.4 The second phase - the target system

4.4.1 Own information and communication technology systems

The second phase of the strategic analysis regards the own information and communication technology systems (ICTs) and the cybersecurity controls defending them. This phase has three objectives and, therefore, three different parts. The first objective is to continue the analysis of own ICTs as a target for the adversary. The second part of this phase focuses on the designed cybersecurity controls, and the third part the activities of the cybersecurity controls. The structure of the second phase is presented in figure 10 (figure10).

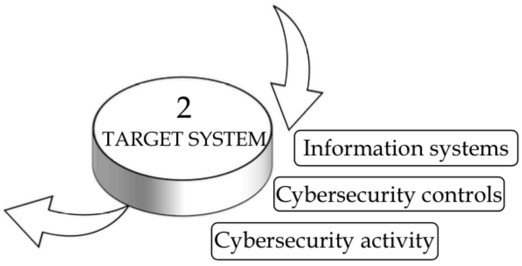

FIGURE 10 Analysis of a target system

The own ICTs are examined from the point of view of an adversary. The objective is to understand what kind of target own ICTs constitute and how they are exposed to an adversary. An adversary's targeting process likely includes the phases of detection, location, identification and classification. The strategic analysis should follow the same process. An adversary's objective is to identify, describe and evaluate the composition and different parts of the target to determine the functions, capabilities and vulnerabilities of the system. (see Joint Targeting, 2017.)

The strategic analysis should be detailed enough to understand how the parts of designed ICTs are exposed to an adversary. The classification of ICTs supports the identification of different parts, and it can be based on different models. If the model presented by Raggad (2010) is used, the targets in the ICTs are people, activities, data, technology and network (Raggad, 2010). These categories can be divided into subcategories until the essential parts and their relations in every category are identified. This division provides an understanding of how these parts create the target and the kinds of interdependences they include, even when the ICTs are dispersed physically, logically and socially. In this phase, the main focus is on substantial entities of people, data, technology and network. The temporal entity of activities can be considered if it increases understanding of the spatial entities and own ICTs as a target. The objectives to develop ICTs can be identified from different organizational strategies, doctrines, resource allocations and roadmaps. Ideally, ICTs and the related cybersecurity controls are developed in coordination.

The analysis of own ICTs can utilize some penetration testing elements, where the objective is to identify and report security vulnerabilities (see Alisherov & Sattarova, 2009). For the strategic analysis, there is no need to execute an actual penetration test unless a reliable knowledge of the structure, accessibility and vulnerabilities of current ICTs is incomplete. Nevertheless, understanding future ICTs requires an understanding of current information systems. The strategic analysis can utilize white-box penetration testing procedures, where the network configuration is known, or grey box testing, if only partial network knowledge is available (see Zenko, 2015). Typically, a white box test is a simulation of a well-prepared attacker with broad access to the system (Alisherov & Sattarova, 2009). This type of setting presents the worst-case scenario for the ICTs as a target. Depending on the situation, the threat can be assumed to be invisible or visible for the target, if that is significant for the exposition of the ICTs. Nevertheless, the analysts must have complete expertise on the target system and its usage and the future structure and operations of the ICTs. (see Ami & Hasan, 2012.)

4.4.2 Identification of cybersecurity controls

This step aims to identify own cybersecurity controls, the parts they are created from, and their relations in the designed security configuration. Assessing future security controls requires also surveying the current situation as the baseline for the analysis. The main focus of this step is the spatial entities of the cybersecurity controls.

The tasks of cybersecurity controls include protecting the information assets, ensuring business continuity, and minimizing the consequences of information security incidents. The tasks are achieved by implementing the appropriate set of controls to reduce risks to an acceptable level. They can be chosen based on a risk management process, and managed using information security management, including policies, processes, procedures, organizational structures, software and hardware. (ISO, 2018.)

Cybersecurity controls and countermeasures can vary considerably. Some controls are designed to limit physical access to an area allowing access to the IT infrastructure. On the other hand, some countermeasures are designed to block access and protect privacy over an organization's networks. Furthermore, some countermeasures are designed to enable recovery after a successful malicious intrusion. (Paul Rees, Deane, Rakes, & Baker, 2011)

Raggad (2010) divides security controls into managerial, operational and technical controls (Raggad, 2010). On the other hand, ISO and NIST introduce more detailed lists of security controls. ISO (2018) has 14 different control sets covering, for example, security policies, human resource security, physical security, asset management, access control, operations security and business incident and continuity management (ISO, 2018). The control sets defined by NIST (2020) are relatively similar to ISO, covering, for example, access control, awareness and training, configuration management, identification and authentication, incident response, physical and environmental protection, personnel security and supply chain (NIST, 2020).

Regardless of the model used to classify future security controls, the main focus in this phase is on the spatial entities. They can include, for example, software, hardware, and various technical and physical controls. The temporal entities, e.g. the actual development, operations and use of the cybersecurity controls, are covered in the next step of this analysis process. However, if the analysis in this step requires, also temporal cybersecurity controls can be addressed. The spatial and temporal security controls should be kept separate for the time being. Future cybersecurity capabilities can include new types of cybersecurity controls, new qualities for current controls, new parts for current controls or new types of relationships between current controls and their parts. Cybersecurity development objectives can be found from different strategy and policy documents, doctrines, roadmaps and cybersecurity investment plans. Nevertheless, assessing the actual future investments and capability developments can be difficult.

After the identification and classification of future spatial security controls are completed, the analysis focuses on identifying the parts and their interdependences in each spatial cybersecurity control. The objective is to identify the essential elements and also the possible vulnerabilities of the controls. The analysis likely reveals security controls, where the parts create a whole, referring to an operationally viable cybersecurity control. On the other hand, if the parts create an aggregate, the analysis should indicate the need for further cybersecurity capability development. After identifying the spatial entities of the security controls, it is possible to assess their dependent entities, the attributes, different features, qualities, roles, states and functions.

The analysis of own cybersecurity controls can utilize the different information security standards, like ISO or NIST, when identifying spatial and temporal security controls. Also, using DOTMLPF-II -P model is possible, depending on the required level of the analysis. Nevertheless, the use of information security standards is encouraged.

The identification of the cybersecurity capabilities provides only a baseline for future capability design and development. Eventually, the final results of this strategic cybersecurity analysis will provide a comprehensive understanding and requirements for future cybersecurity design, development and investments.

4.4.3 Cybersecurity control activity

The National Institute of Standards and Technology (NIST) cybersecurity framework (2018) includes five cybersecurity core functions: identification, protection, detection, response, and recovery (NIST, 2018). The literature also recognizes some simplified models, including prevention, detection, and response/recovery (Jalali, Siegel & Madnick, 2019).

Identification includes the means to identify malicious activity. Protection refers to the preparation and implementation of the safeguards of the system. Detection covers the development and implementation of the activities to discover the occurrence of cyber events. Detection can be achieved through monitoring and surveillance mechanisms or technologies. Response covers the development and implementation of the activities to respond to a detected cyber event, aiming to contain the impact of a cyberattack. Recovery refers to developing and implementing the activities or processes that restore the compromised or degraded services to their regular operation. (Kolini & Janczewski, 2015.)

These core functions can be understood as temporal entities where the defender's spatial cybersecurity controls participate. The analysis aims to identify the different processes and sub-processes of these core functions. Every core function is divided into more detailed process parts. For example, the core function of identification includes several different processes and related spatial entities tasked to identify a cyber threat. The spatial entities and the processes have a bilateral interaction. A spatial security control, or its attributes, can start, continue or terminate any cybersecurity core function, or just to facilitate it. On the other hand, the core function process can bring out, prolong, degrade or destruct the existence of the related spatial cybersecurity control or its attributes. (see Little & Rogova, 2009.)

Cyberspace protection requires control of all direct connections between own ICTs and the public parts of cyberspace. Control means monitoring, detecting, and preventing the entrance of malicious network traffic and unauthorized exfiltration of information through these connections (JP 3-12, 2018). Kolini and Janczewski (2015) divide cyber defense activities into passive defense and active defense. Passive defense includes all the measures and controls that can be used passively to protect, detect, respond and recover from the cyber threat. Passive defence supports achieving the resistance and resilience of the defender's system against cyberattacks. On the other hand, active defence refers to the active capability to minimize the impact of the cyberattacks, using offensive capabilities to discover, destruct, disrupt, degrade or nullify incoming cyber threats. In this context, discovery refers to the capability to collect valuable information about the threat source. Destruction means damaging the threat source's system and causing a malfunction. Disruption refers to a type of denial of service, where the resources of a threat source are exhausted, consumed or unavailable for the use. Degradation of service occurs when users are experiencing a lowered quality of service. Nullification refers to the ability of an entity to nullify the cyberattack. (Kolini & Janczewski, 2015) The objective of the strategic analysis is to examine the actions of passive defence. However, if international law, national legislation or other jurisdiction allows, the analysis can also cover the active defence (see Formin, 2020).

This analysis phase can also indicate some preliminary information of the attack probabilities for the last phase of this analysis, the interaction. The probability of a cyberattack is increased if the own ICTs has a high value, exploitable vulnerabilities, easy access or inadequate cybersecurity controls. These factors make attack either attractive or enable low-risk attacks (see Mateski et al., 2012). On the other hand, any factor creating a disincentive to attack correlates negatively to the attack frequency (Schechter, 2004). Disincentives may include the low value of the ICTs, challenging access and adequate security controls.

The analysis of security controls should indicate the requirements for future capability design and development. Capability can be increased by developing the spatial entities, their attributes and the processes they participate in. The viable processes should be supported, defective processes modified, and missing processes created. However, these requirements for cybersecurity development can be considered only preliminary. For example, at this point, there is no understanding of how own cybersecurity controls operate against cyber threats or how they wear out in the process. This type of knowledge is especially significant if the processes decrease the efficiency and the resilience of own cybersecurity. The last phase of this strategic cybersecurity analysis will specify the development requirements regarding the interaction between cyber threat and own cybersecurity controls.

4.5 The third phase – cyberspace

4.5.1 Classification of cyberspace

The substantial entities, including their attributes and other qualities, have a location in spatial regions (Little & Rogova, 2009). These locations are spatial entities on their own, and other spatial entities, like cyber threat sources or own ICTs, are located in them. As a spatial region, cyberspace is endurant. It has relations of connectedness and separation between spatial regions, fiat boundaries and dimensionality. (see Grenon & Smith, 2004.)

Reliable and valid analysis requires understanding the threat and the target system. In cybersecurity, equally important is to understand the conditions where these two entities operate and interact. In a traditional threat component triangle, opportunity depends on the intention and capability, the will and means to operate. In cybersecurity, cyberspace itself is a factor that impacts the capability and provides or prevents opportunities. A traditional operational environment consists of the conditions, circumstances, and influences that affect the use of capabilities (JP 3-12., 2018). The impact of cyberspace is more significant than a traditional environment. The structure of the third phase of the analysis is presented in figure 11 (figure 11).

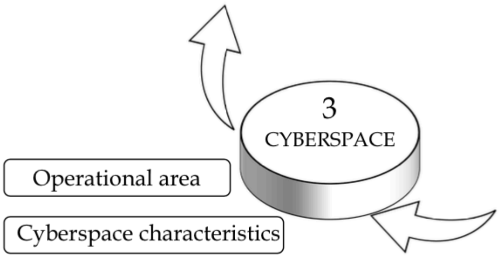

FIGURE 11 Analysis of cyberspace

Cyberspace is a complex operational environment, and it can be divided into several different dimensions, depending on the objectives of the analysis. As mentioned before, it can be divided into a physical layer, a logical layer and a social layer. The physical layer includes the infrastructure, all the connected and supporting devices of the physical network that store, transport and process the information. The elements have a geographical location. The logical layer includes all the elements that are abstracted from the physical network, based on programming, like data, applications and network processes. The logical layer elements reside in physical equipment, but the location is logical, not geographical. The logical elements can be reached only with cyberspace capabilities, not physical capabilities. The third layer is the social layer. It can be examined from the perspective of a threat when the focus is on the cyber-personas operating the social layer. When the focus is on the information included in these cyber-personas' traffic, the social layer resembles more an environment where these cyber-personas operate. (JP 2-01.3, 2014.)

In addition to the layer-based perspectives, cyberspace can be divided into red, blue and grey cyberspaces. Red cyberspace is a portion of cyberspace owned or controlled by an adversary or where an adversary has a presence. Controlling a part of cyberspace means more the capability to execute operations there than the actual control. Blue cyberspace refers to protected areas by friendly entities, a state, a company, or other own organizations. Grey cyberspace covers mainly the rest of the networks, involving entities that are neither adversary nor own. (JP 3-12., 2018.)

Another possible classification of cyberspace is related to connectivity. Even when cyberspace is increasingly interconnected, some elements may be intentionally isolated or subdivided into enclaves using access controls, encryption, unique protocols, or physical separation. The first three include the physical connection, but the access is limited in the logical layer. The last one also provides physical isolation. These isolated or subdivided parts can be used as an attack supporting environment, even if the defender cannot usually see them. (see JP 3-12., 2018.)

4.5.2 Analysis of the operational environment

Analyzing the operational environment starts with identifying the operational area and determining the significant characteristics of the environment. The impact of an operational environment is assessed on both adversary and friendly capabilities. (JP 2-01.3, 2014.)

In many cases, the analysis of cyberspace is compared to the analysis of a traditional environment. Lemay, Knight and Fernandez (2014) introduced an Intelligence Preparation of the Cyber Environment (IPCE), based on the Joint Intelligence Preparation of the Operational Environment (JIPOE) -process. The objective of the JIPOE is to increase military planners' understanding of the environment, and IPCE has a similar objective. They modified the traditional JIPOE triangle of weather-enemy–terrain into traffic-adversary-network for cyberspace. (Lemay, Knight & Fernandez, 2014.)

In a traditional analysis of the operational environment, the first step is to determine its significant characteristics, namely weather and terrain. Lemay, Knight and Fernandez (2014) claim that the equivalent to the terrain is the network in cyberspace. The network can either support or obstruct mobility. With the same logic, cyberspace equivalent to the weather is traffic. The data traffic mainly originates from neutral sources, causing a noise not controlled by the adversary or the defender. The environmental impact assessment includes identifying mobility corridors that can be used as a means of approach. In cyberspace, these corridors are potential attack vectors and command and control channels. Both offensive and defensive technologies are affected by network characteristics. The third and fourth steps of the IPCE-process consist of evaluating the adversary and determining the adversary courses of action. (Lemay et al., 2014) In this strategic cybersecurity analysis, these elements are covered already in the previous phases.

The key terrain analysis, also in cyberspace, reveals the locations that by holding provides an advantage over the adversary (see JP 3-12., 2018). However, in cyberspace, an adversary and a friendly entity can occupy the same terrain, even without knowing the other's presence. The traditional environmental aspects of terrain include obstacles, avenues of approach, cover and concealment, observation and fields of fire, and key terrain (JP 3-12., 2018). In cyberspace, obstacles may include firewalls, port blocks and, at a strategic level, complex systems of cybersecurity controls. Avenues of approach can be connected nodes, links, and all the connections that enable reaching target systems. Cover and concealment may refer to hidden addresses, password-protected access or any means to hide resources and decrease the system's exposition to an adversary. In cyberspace, observation and fields of fire can refer to locations that allow network traffic monitoring, intercepting, recording or even active cyber operations. Key terrains in cyberspace can be different access points, key waypoints for observing incoming threats, or cyberspace terrain related to critical assets. (see JP 3-12., 2018.)

Rattray (2009) claims that some features of the traditional domains are valid also in cyberspace. As in land power theories, also in cyberspace, there is a need for determined essential resources and focal points for transit. Sea power theories emphasize the need to control the environment, enabling global manoeuvre and technological change, valid also in cyberspace. Airpower theories emphasize the significance of offence-defence interaction, the impact of a new type of power, and international cooperation when securing a new domain. Space power has a clear linkage to cyberspace, carrying information globally, relying on networks using space systems and orbital locations creating cyberspace chokepoints. (Rattray, 2009.)

Winterfeld (2001) suggests that the significant characteristics of the cyber environment include the classification of the network, baseline activity in the network, information, architecture, operating systems and connectivity. The process should also identify the network limits, evaluate the existing databases, and identify intelligence gaps. (Winterfeld, 2001) Winterfeld's approach is valid when analyzing a limited network, but the perspective is likely too narrow in the strategic context.

The traditional terrain analysis supports the determination of which own courses of action can best exploit the terrain and how it affects the adversary's available courses of action (JP 2-01.3, 2014). In cyberspace, the assessment regarding the adversary is similar. However, from a friendly perspective, the focus is on terrain that can support cyber defence by obstructing adversary's opportunities and supporting own cybersecurity controls. If active cyber defence is allowed, the objectives of the cyberspace analysis are closer to traditional terrain analysis.

Some cyberspace analysis models follow the traditional environment analyses too closely, partly ignoring the exceptional nature of cyberspace. Typically, the environmental impact is assessed as a part of the capabilities and actions of the adversary. Any changes in the environment affect the capability of the adversary. However, the changes in a traditional environment are usually slow and do not immediately impact the capabilities. In cyberspace, changes can occur quickly and have an imminent impact on the threat and target system capabilities and opportunities. The modifications can be either coincidental or deliberate. To avoid the constant re-analysis of the threat and the target, the environmental analysis of cyberspace and the actors should be kept separate in the first phases of the analysis. However, the significance of cyberspace must be noticed at all times.

4.5.3 Analysis of cyberspace

The strategic analysis of cyberspace includes two main steps, determining the operational area and identifying its significant characteristics. The strategic analysis baseline is current cyberspace, but the focus must be on the designed future developments of cyberspace. The objective is to understand how the development of cyberspace affects the capabilities and opportunities of both the adversary and the target system. The analysis should also reveal what kind of advantages a defender may gain by actively modifying cyberspace.

The analysis should take into consideration the physical, logical and social layers of cyberspace. The identified modifications in the physical layer may provide insights into how and why an adversary is developing its networks. On the other hand, the analysis should reveal requirements for own development in a physical layer. From the strategic analysis perspective, the logical layer and social layer constitute a challenge. They are constantly changing by nature, and the changes are effortless to execute. The analysis of the physical layer may be emphasized when assessing the design and development of cyberspace. The other two layers may be more significant when assessing the deployment and operations in cyberspace. The layers may require separate analysis, but eventually, the results of cyberspace analysis should be combined.

Identification of the operational area can be executed by dividing cyberspace into blue, grey and red areas. In blue cyberspace, the defender can execute appropriate changes to the environment. On the other hand, in red cyberspace, the defender has only limited possibilities to operate. In grey cyberspace, the defender, the adversary and the third parties can operate, possibly facing some limitations. From the defender's point of view, different areas have different roles. The defender must protect and modify blue cyberspace, collect information from red cyberspace, and actively modify grey cyberspace to own advantage.

When the operational areas are determined, the analysis focuses on the significant characteristics of cyberspace, using appropriate models. The analysis should identify the key terrains for both the adversary and the defender. Most likely, blue and red cyberspaces include several key terrains for the defender and the adversary. Nevertheless, the most interesting key terrains may locate in grey cyberspace. For the defender, the key terrain analysis provides knowledge of what terrains the defender should control at any time are, and what are the required actions to gain possibly missing key terrains or prevent the adversary from gaining them.

Next, the analysis covers mobility corridors and obstacles. From the defender's perspective, the objective is to identify the mobility corridors that allow the adversary to reach blue cyberspace or provide opportunities or advantages in grey cyberspace. The analysis should reveal the mobility corridors that need to be blocked with obstacles to degrade adversary's opportunities. It also reveals the corridors that are not dangerous and can be covered, for example, with monitoring. On the other hand, the analysis should identify the mobility corridors, which enable appropriate freedom of actions for the defender, for gaining and maintaining the advantage.

Cover and concealment, on a strategic level, may refer to the parts of cyberspace that the adversary is concealing for gaining an advantage. Most likely, most of these concealed parts are in the red cyberspace and partly in grey cyberspace. From the defender point of view, the analysis sets requirements for intelligence collection of the adversary modifications in cyberspace. Furthermore, the analysis might reveal the parts of blue cyberspace that the defender needs to conceal from the adversary.

In the strategic analysis, the observation and field of fire can refer to the locations and mobility corridors that require traffic monitoring and intercepting and areas where active cybersecurity operations are possible. The analysis sets requirements for the defender's intelligence collection. First of all, identifying the areas where modifications are required to increase own advantages and decrease adversary's opportunities. Also, to provide information for cyberspace modifications for active cyber operations. On the other hand, the analysis should reveal the areas where the adversary can monitor, intercept and impact the defender.

The analysis should provide an in-depth understanding of cyberspace and its effects on adversary's and defender's capabilities and opportunities in a determined timeframe. It should reveal the actions that the defender must execute in cyberspace to ensure the capability to defend ICTs, preferably keeping an advantage all the time. It also reveals the actions that the defender must take to decrease the adversary's capabilities and opportunities, preferably to the level that prevents the adversary's malicious actions. Cyberspace is not a traditional operational environment. In cyberspace, a defender can gain an advantage by continually modifying the environment to support cybersecurity.

4.6 The fourth phase – interaction

4.6.1 Methods for assessing an interaction

The last phase of the analysis combines all the previous phases. This phase focuses on the interaction between the cyber threat and the target system in cyberspace, and it has two main objectives. First, it verifies the objectives, intentions, capabilities and the possible opportunities of the adversary. Second, it verifies the capabilities and operations of the defender's cybersecurity controls and identifies possible capability gaps. The identified capability gaps provide input for own cybersecurity capability design and development. This phase also provides some metrics that enable monitoring both the adversary and own cybersecurity capability development. The structure of the fourth phase is presented in figure 12 (figure 12).

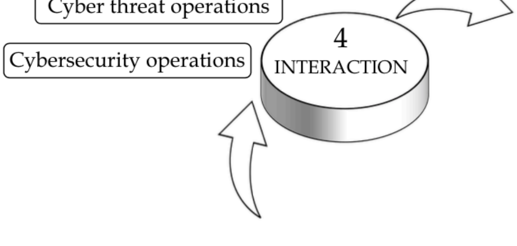

FIGURE 12 Interaction analysis

Information security literature provides several different methods for assessing the interaction. However, most of them apply only in a limited environment, with limited threat and target system. Strategic cybersecurity analysis requires a broader approach than most of these models can provide.

Typically, cyber threats to ICTs are chains of events of several different threat sources, their parts and actions. Chains of events can be examined with scenarios, including the threat sources, the target system, the environment, and the activity they execute. Scenarios can be presented as a text, picture or a tree, supported by a descriptive text. The trees are usually called threat trees, event trees or attack trees. (Schechter, 2004) The adversary's objective can be presented as the top node of the tree. Subordinate nodes present the logical actions an adversary might execute to achieve that goal. Each unique path through the tree represents an attack scenario. (Mateski et al., 2012) Furthermore, the defender's actions can be inserted into the respective nodes, enabling the assessment of the interaction. Presenting scenarios with trees allow describing attacks deductively. Furthermore, they provide a method for characterizing both attacks and attackers and generate data for analysis and development. Trees are also flexible enough to be used to model different types of attacks or threats. (Mateski et al., 2012) The scenarios can also be presented in a Directed Acyclic Graph (DAG) -diagram, where the branches can have several connections (Schechter, 2004).

However, Alkire, Lingel and Hanser (2018) argue that even if event trees describe how the threat acts when confronting security controls, they do not necessarily include actions following that confrontation. Furthermore, the analysis may focus on single interaction at a time, missing the larger context of the actions. Also, traditional event trees typically do not take into account the environmental impact. To avoid some of these deficiencies, they developed a war game method for command and control (C2) exercises for the U.S. Armed Forces. The presented model is not a traditional wargame. It is an adaptation of assumption-based planning, aiming to identify weaknesses in a strategic plan and provide inputs for the plan modifications. The presented model focuses on risk and resilience, and it uses retrospective futurology. The scenarios are addressed in the past tense, where all the individual events of the scenarios have already occurred. The objective is to examine and identify the essential qualities, related risks and resilience of the command and control systems in different scenarios. After the qualities of the system are identified, they are assumed to have failures. The participants assess the consequences and the probabilities of the failures and determine the actions required to increase the system resilience. There are two types of resilience actions, a shaping action to prevent the failure and a hedging action to restrict the failure results. The process produces a list of the risks and qualities, where the failures can occur, and where they can affect the operation. Furthermore, the participants attempt to find indicators that may predict these failures. (Alkire et al., 2018.)

The model of Alkire, Lingel and Hanser is close to a method Heuer (1999) calls thinking backwards. The method assumes that something unexpected has occurred, and the analyst aims to understand how it could have happened. The advantage of this method is that instead of assessing the possibilities of an event, it focuses on how the event took place. This type of approach enables a different perspective, preventing anchoring to the present situation. The approach is beneficial when assessing events with a low probability but serious consequences.

(Heuer, 1999) As noted, cybersecurity events typically are this type of events by nature.

The reliability of the different event tree analyses can be increased if the cyber threat and own cybersecurity are measured quantitatively or qualitatively. Measurement enables assessing cyberattack plausibility and the interaction results (see Mateski et al., 2012). However, Scoblic and Tetlock (2020) argue that scenarios are not supposed to be predictive but merely provocative to challenge assumptions and mental models. They suggest a combination of scenario planning and probabilistic forecasting that provides a range of possible futures to calculate possible outcomes. These different approaches can be linked by developing clusters of questions that indicate which assessed future is likely to emerge. (Scoblic & Tetlock, 2020) Regardless of the prediction or provocation level, different attack trees provide the organization a shared understanding of the situation (see Schecter, 2004).

The strategic cybersecurity analysis requires a broad approach to the threat, target and environment. Therefore, traditional theories used in information security may serve appropriately in a confined environment, but not at a strategic level. Scenarios, presented in different types of trees, allow the comparison of adversaries' actions to own cybersecurity. However, detailed capability comparison does not necessarily support strategic cybersecurity. The strategic analysis of cybersecurity requires a strategic approach to the phenomenon. A proposition for the strategic interaction model is presented in the following subchapters.

4.6.2 Probability of the actions

The adversary has the initiative to use its capability based on the opportunity it assumes to have. It decides when and how to execute the offensive actions. The adversary's activity has been assessed and prioritized in the previous phases, but reprioritization may be required in this last phase. This last phase attaches the opportunity more attentively to the analysis, especially based on the target system vulnerabilities and cyberspace. However, the opportunity available for the adversary is not constant. It can change depending on the adversary's intention and the capability, the target system vulnerabilities and the modifications in cyberspace. (see Steinberg, 2005.)

The significance of the intentions and objectives determine the risk level an adversary is willing to take. They also determine how severe consequences an adversary is willing to bear. On the other hand, the time and resources an adversary is willing to use for that particular objective also define the probability of the opportunity. (see Winterfeld, 2001) The probability of the adversary's actions can be considered high when the activity enables reaching the objectives, the operation is easy, the risk level is low, and the consequences for the adversary are appealing. On the other hand, if the operation is not relevant to the objectives, it is challenging to execute, it includes high risk, and the outcome is not appropriate, the probability of the adversary's actions can be considered low. (Mateski et al., 2012.)

The target system characteristics also affect the probability of the offense. The organization's value as a target, the information exposed of the target organization, and the target's security level affect the quantity or the frequency of offensive cyber events (Mateski et al., 2012). The more tempting is the incentive to attack, the more likely the attack is, and the higher is the attack frequency. Also, the rate of successful attacks affects the attack probability. When assessing the incentive to attack, it is essential to notice the other options available for the adversary (Schechter, 2004). Disincentives to prevent a cyberattack can include a high risk related to the attack and the risk of undesirable consequences to the adversary. These consequences can include a disclosure of the adversary's capabilities, damage to reputation, capture and incarceration, or even physical harm. (Schechter, 2004) Also, the resources required in the attack constitute a disincentive correlating negatively with attack frequency and security risk. The stronger the target system is, the higher is the expected cost of a successful attack (Schechter, 2004).

Analyzing every possible adversary's course of action requires time and resources and, therefore, may require a prioritization based on probabilities. However, it is essential to maintain the strategic focus. The probability of an adversary's cyber operation may not be related to cybersecurity but larger strategic objectives. On the other hand, cyberspace enables operations that may appear low probability but still have high consequences. Therefore, special attention is required when prioritizing the scenarios.

4.6.3 Interaction analysis

The cyber threat sources, own cybersecurity, the activities and the environment have been analyzed in the previous phases. The analysis has revealed the adversary's assessed intentions and capabilities, and preliminary opportunities and possible courses of actions. Furthermore, analysis has enabled an understanding of defender's ICTs as a target, the cybersecurity capabilities, the intentions to develop them and the preliminary actions they can execute. Also, the qualities, changes and possible modifications of cyberspace have been assessed.

This last step combines the results of the previous phases, assesses the reliability of the analysis, and identify requirements for own cybersecurity development. The main focus of this phase, and the whole analysis process, is to identify cyber threats, determine the effectiveness of cybersecurity controls, identify possible capability gaps, and determine future development requirements.

The interaction analysis starts with the adversary's capabilities and activity. The activity is presented as a scenario, including the courses of action of the adversary. First, the adversary's assessed objectives are installed at the top of the scenario, and the required and available capabilities for the objectives are examined. When the required capabilities are identified, the possible courses of action to reach the objectives are determined. The effects of cyberspace are taken into account, especially when they improve or decrease the adversary's capability. The next step is to install the defender's cybersecurity controls and their actions into the same scenario, using the same scale as for the adversary. The aim is to identify respective cybersecurity capabilities against every adversary action. The attributes of cyberspace are similar for both the adversary and the defender.

The analysis utilizes retrospective futurology or thinking backwards. At the top of the scenario are the adversary's objectives. The analysis starts from the situation where the adversary has reached these objectives through its courses of action. The analysis aims to find and identify those cybersecurity capabilities, processes and possible modifications of cyberspace that could have prevented the adversary from taking the last step of the scenario to the objective. After these cybersecurity controls are identified, they are installed into the scenario to defend the last step. Next, the analysis focuses on the adversary and assesses how the adversary may work around these new cybersecurity controls. If the adversary can again penetrate the new cybersecurity controls, yet another group of cybersecurity controls are identified and installed into the scenario. This process is continued until the analysis has identified those cybersecurity capabilities, activities and modifications to cyberspace that can prevent adversary's action. The installed cybersecurity controls may also include yet nonexistent controls, providing input for cybersecurity innovation, design and development.

Next, the analysis focuses on the previous step of the scenario. The analysis of this step includes a similar process, where the adversary's capabilities are compared to the defender's cybersecurity capabilities, new cybersecurity capabilities are installed and compared to the adversary's actions. This process is continued as long as that particular step is prevented from the adversary. A similar analysis is executed in every step of the scenario until the analysis has reached the first step of the adversary, the beginning of the scenario. Every step of the scenario and the analysis includes the adversary's capabilities, own cybersecurity capabilities and the qualities and modifications of cyberspace as part of the capability and opportunity.

The analysis should provide several conclusions regarding the adversary. First of all, it should provide a detailed list and description of the adversary's main courses of action, including several alternative operations. Furthermore, it should also reveal low probability, high consequence types of operations. It also provides a list of adversary's capability strengths and gaps. These can be utilized when monitoring an adversary's capability development, for example, identifying the change of a threat from possible to viable. Furthermore, adversary's capability gaps can be exploited in active cyber operations when allowed by the legislation.

For own cybersecurity development, this process provides several inputs. First of all, it provides a knowledge of those cybersecurity controls that could prevent the adversary's actions. From this list, it is possible to identify the controls that are operational, partly operational or missing. The last two categories provide input to modify the design and development of future cybersecurity capabilities. Second, this analysis provides knowledge, how modifications of cyberspace affect adversary's operations and the defender's cybersecurity. These observations provide requirements for cyberspace modifications preventing adversary's activities and opportunities and supporting own cybersecurity. Third, the scenarios can indicate the circumstances where the adversary's opportunity for hostile activity is available or when it is not a factor. Fourth, the scenarios provide also knowledge of the responsibilities of different cybersecurity capabilities and operations. The scenarios also encourage examining how cybersecurity activities can be managed, controlled and coordinated.

Retrospective futurology has several advantages. The focus is all the time on the adversary's actions, regardless of how probable they are. This approach allows identifying also low probability events. Backward examination of the scenarios also provides a comprehensive list of possible adversary's options and a similarly comprehensive list of required cybersecurity capabilities. With a constant comparison of the adversary's actions to own cybersecurity, effective security controls, both spatial and temporal, are identified. There are probably several identified cybersecurity controls that require design and development and some controls that are not available for various reasons. However, the scenarios provide knowledge on replacing unavailable cybersecurity controls with available ones or requirements to innovate new cybersecurity controls. Retrospective futurology supports the construct of layered and diverse cybersecurity system.

The value of the analysis depends on the documentation of the process. Proper documentation of the process, the results and the conclusions provide a possibility to assess the reliability and validity of the analysis. Documentation enables also returning to the analysis. If some of the factors are changed, there is no need to repeat the whole analysis process; only part of the analysis will suffice. Documentation also allows a presentation of the results and the description of the process to the decision-makers, increasing their reliability to the analysis results. The results should support decision-makers to rational choices understanding the consequences.

The resolution of the analysis depends on the available resources and time. The analysis presented here is mainly focusing on the protection phase of cybersecurity. However, the analysis can be used to examine how the adversary is identified and detected, how own cybersecurity is responding to the threat, or how own ICTs are recovering from the attack. The level of details and approach depends on the requirements for the analysis. The simplest version of the analysis can include a table-top comparison of the adversary's future capabilities to own future cybersecurity. When applicable, this type of comparison can be supplemented with scenarios involving simple interaction analysis. Both of these simplified options provide some information required in own cybersecurity development and cyberspace modifications. Even the simplest form of the analysis may increase shared understanding of cybersecurity in the organization.

4.7 Conclusions

An ontology differentiating spatial and temporal entities and identifying their spatial and spatio-temporal regions support cybersecurity analysis appropriately. Furthermore, an ontology addressing the threat, target and environment, and the components of intention, capability, and opportunity support modelling the elements of cybersecurity. Relying on these theories and using existing classification models assure the validity and reliability of the strategic cybersecurity analysis model. Measuring these classes, even when challenging, would increase the applicability of the model.

The effectivity of this model is based on two main characteristics; it is threat-based, and it aims to estimate future cybersecurity development. Threat based means that cyber threats initiate the analysis, not own system vulnerabilities. Unfortunately, the approach is resource-intensive. First of all, it requires the identification of several possible cyber threat sources. Furthermore, it requires effective information collection for the analysis and monitoring of the assessed developments. However, it enables identifying emerging threats, even before they induce vulnerabilities in own information systems.

The estimation of future development means that the focus is not on the adversary's current intentions and capabilities or the opportunities it is currently exploiting. All these components are, in fact, visible and, therefore, uninteresting from the strategic view. Current threats are mitigated reactively, with current cybersecurity capabilities. The objective of the strategic cybersecurity analysis is to identify future adversaries, their intentions and capabilities that are not yet visible and attempt to exploit the opportunities unfolding in the future. The objective is to describe adversaries' assessed cyber capability development and utilize this knowledge to design and develop own cybersecurity capabilities in advance. The objective should support proactive cybersecurity design and development and also identify the requirements for cyber resilience. After all, the eventual objective is to gain an advantage in cyberspace.

The components of intention, capability and opportunity are dependent on each other, but their significance may vary in cybersecurity. For the strategic analysis, especially at the beginning of the process, the most significant component is the adversary's intention. The objectives behind intention determine the types of cyber capabilities and operations an adversary is developing for the future. However, an adversary's intention is not always cyber-specific but can be part of more extensive strategic objectives. Therefore, the beginning of the analysis needs to have a larger than cybersecurity approach. Furthermore, in a traditional threat analysis, the intention and capability determine the opportunity. In cybersecurity, an adversary's opportunity is also defined by the target system's cybersecurity capabilities and cyberspace. As an operational environment, cyberspace is rapidly modifiable, having an imminent impact on opportunities.

The analysis is threat-based, but it does not decrease the importance to know own information systems and cybersecurity controls thoroughly. Understanding can include, for example, recognizing the primary assets and their values, the exposure of the system and the cybersecurity controls that protect the system. These requirements are relatively self-evident and straightforward enough. However, at the strategic level, knowing own information systems can be a challenge. Own systems, regardless if they belong to a government or a private organization or both, include various actors with different tasks and resources, some of them outsourced. Modelling the threat is essential, but equally important is to be able to model the own system.

The strategic analysis model can be utilized according to organizational needs. However, it is most effective when all four phases are utilized. Especially significant is the interaction phase that eventually provides an in-depth understanding of cyber threats, own cybersecurity, cyberspace and how all these elements impact each other. Furthermore, when identifying and determining the effective cybersecurity capabilities in the scenarios, they should not be restricted by current capabilities. Some of the adequate cybersecurity controls may be yet nonexistent, but they are equally essential to identify. Required novel cybersecurity capabilities can be innovated, they can be replaced with several existing capabilities or replaced with a new usage of available capabilities. Nevertheless, the analysis provides knowledge of the cybersecurity development requirements.

The analysis process reveals several different cyber threats capable of several different types of cyber operations. Some characteristics may indicate the probability of the operations. Traditionally, threat analysis is commenced from the most probable or dangerous scenario. However, in cybersecurity, the adversary's capabilities and cyberspace may undergo rapid modifications, changing the most probable scenario continuously. In some cases, the appropriate scenario to start the analysis could be the most dangerous one. The use of retrospective futurology supports this approach because it does not consider the probability of the scenario but focuses on the adversary's objectives and results.

The model of strategic cybersecurity analysis should provide knowledge and wisdom for strategic cybersecurity decision-making. The decisions at a strategic level are probably not based exclusively on quantitative data and information, especially regarding a complex phenomenon like cybersecurity. The information and knowledge supporting decision-making should also include rich and descriptive qualitative information. Sometimes a common understanding of the phenomenon may be more important than exact quantitative data, especially if the data is too limited to describe the elements of the phenomenon. The identification, classification and measurement of cybersecurity using the presented model will provide rich descriptions that should increase the knowledge and wisdom regarding cybersecurity design and development decisions.

5 CONCLUSIONS

The objective of this master's thesis was to determine what means strategic analysis of cybersecurity and how the analysis can be utilized in developing cybersecurity. The main research question was:

- What means strategic analysis of cybersecurity?

The main question was divided into the following sub-questions:

- What are the actors and their relations affecting security in cyberspace?
- How can the actors, their activities and cyberspace categorized and analyzed?
- What is included in the analysis process?
- What are the results of the analysis, and how they can be used?

The objective of this research was to introduce a practical model to support a strategic analysis of cybersecurity. Based on the model, strategic cybersecurity analysis includes four main categories; the cyber threat, the target system, cyberspace and interaction of all these entities. The structure of the analysis is presented in figure 13 (figure 13).

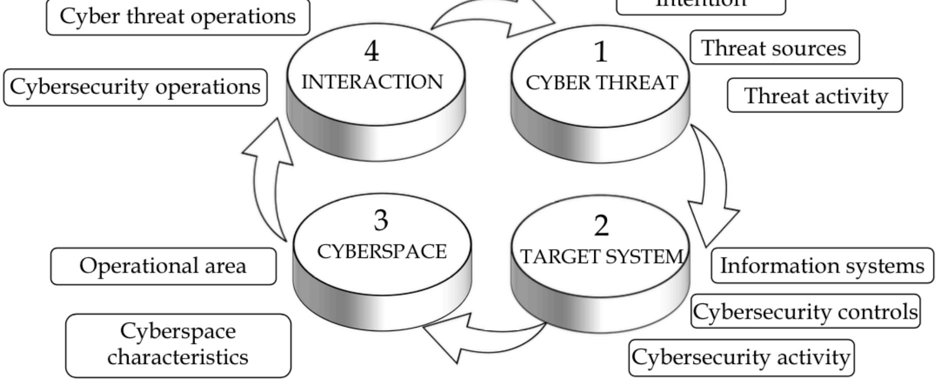

FIGURE 13 The structure of the strategic cybersecurity analysis model

Strategic analysis means focusing on future cybersecurity. The analysis is not about own information system vulnerabilities in current threats or threats in the imminent future. The objective is to provide reliable and valid information that decisions regarding own cybersecurity design, development and deployment can be made on time. Only proactive cybersecurity enables gaining an advantage over the adversary, making cyberattacks challenging to execute, requiring considerable resources. Furthermore, the defender's advantage should create a considerable risk for the adversary included in the attack or the after-attack consequences, providing only limited results.

Anticipating future cyber events is a challenge, and capability design and development always includes a risk. Preventing every cyberattack is likely not a viable objective. Therefore, cybersecurity should always include also appropriate resilience. However, this model can support the decisions regarding the resource allocations to different cybersecurity core functions. When the strategic analysis indicates that available cybersecurity controls are effective, the design and development resources can be allocated to identification, protection and detection. On the other hand, if effective cybersecurity controls are mainly or partly unachievable, the resources can be allocated more to response and even recovery functions.

Proactive cybersecurity requires considering all the essential elements that have an impact on cybersecurity. The key element is the threat. Without a cyberthreat, cybersecurity remains uncompromised. On the other hand, a threat constitutes a threat only when it has a target to interact in cyberspace. This rationalizing indicates that the strategic cybersecurity analysis must include a threat, a target, cyberspace, and interaction.

A cyber threat is the initiating factor in cybersecurity. Therefore, it is logical to start the analysis from a threat. All possible threats in cyberspace cannot be analyzed. There must be a process to narrow down the number of threats. However, unlikely in a typical information security risk management, a cyber threat is not determined based on own vulnerabilities but based on the value that the own information system might contain as a target. Furthermore, it is essential to understand that the strategic level information system may not be the eventual objective, but it is the passage to the adversary's final objectives. Therefore, the approach to the threat cannot be only technical; it needs to be strategic.

The same applies to the own information system. In some cases, only one information system may be the target. However, the target is likely a whole ecosystem or some essential part of it. The target system can be anything that has strategic importance to the adversary or the target organization. It might be a SCADA system controlling the national power grid, water distribution system or banking system. The analysis of own information systems cannot focus on just detailed security controls. Own ICTs must be familiar at a strategic level, identifying all the spatial and temporal elements that impact the operations and the security of the ICTs.

Furthermore, cyberspace should be analyzed as a strategic environment. The hourly or daily changes in cyberspace, either automatically or with human involvement, are not interesting from the strategic perspective. Strategic analysis requires that an adversary's plans to modify cyberspace can be anticipated and identified and assess the impact on the adversary's offensive capabilities. Furthermore, the strategic analysis should provide knowledge, how to modify and develop own cyberspace to decrease the adversary's capabilities and opportunities and increase own advantage. Decisions based on analyzed information may be related to technical plans, agreements on interoperability or even in legislation, if required.

Understanding the actors impacting cybersecurity requires the identification of how they interact with each other. Without the interaction part of the analysis, the result is merely a list of possible threats, targets, and cyberspace characteristics, without profound outcomes and in-depth understanding.

The analysis itself is a relatively straightforward process. The analysts need to identify future cyber threats, own information systems and cybersecurity controls development, and the changes taking place in future cyberspace. After identifying these, the main task is to divide the entities and their processes into as detailed parts as possible and identify their internal and external relations. Their characteristics and relations reveal the threat's status and what kind of development is required to change the threat from possible to viable. After the actors and cyberspace are divided into subcategories, they can be combined to the construct that supports analysis and decision-making. The main point is to identify the substance of the classes in a strategic timeframe.

In real life, the process is not straightforward. Probably the main challenge is data and information collection. There are almost unlimited data available for the analysis. The challenge is to find and identify the valid information required in the analysis. The strategic cybersecurity analysis model can help to identify the actors. Classification allows identifying the relevant cybersecurity entities and ensures that all the significant elements and parts are noticed. Furthermore, classification helps to identify the sources where the information regarding the entities may be found.

On the other hand, the challenge is finding the data and information not available for the analysis, for example, due to the adversary's concealment. The model supports structuring the collected data and information, providing a taxonomy and a partonomy regarding the phenomenon. Identifying any of the entities, characteristics, their processes, or spatio-temporal locations may reveal the other related but currently hidden entities. When the information collection cannot provide all the required and relevant information for the decision-making, the analysis process can refine the available data and information and increase the value to level of knowledge.

Reliable analysis of classes requires measurement. Measurement provides several advantages. It enables an in-depth and detailed understanding of the entities and their actions. Measurement allows comparison of the cyber threat to the target system. It supports the documentation of the analysis and the presentation of the results to the decision-makers. Furthermore, measurement provides the baseline for monitoring the development of cyber threats, target system, and cyberspace. Unfortunately, measuring the actors, their characteristics, and cyberspace may include significant challenges, especially when focusing on future development. Cybersecurity includes complex systems with vast numbers of participants that constitute a challenge to measure reliably. Available reliable quantitative data is limited. On the other hand, qualitative data does not support detailed measurements and comparisons. Therefore, qualitative definitions and the measurement of the classes should include rich descriptions. Detailed descriptions allow obtaining deep understanding, knowledge and wisdom of cybersecurity for the decision-making.

The strategic cybersecurity analysis model must be understood as an example of the analysis construct or process. After all, future cybersecurity decisions determine the required knowledge. The analysis can emphasize the different entities of the threat, target and cyberspace. On the other hand, it can emphasize the spatial entities and their characteristics, or their processes, the time or the physical or logical location. Furthermore, the granularity of the analysis may change depending on the decision requirements.

This model for strategic cybersecurity analysis provides no panacea for effective cybersecurity. However, it may help to construct and classify the phenomenon. The analysis process should reveal the most likely cyber threats, their intentions, capabilities, and available opportunities. Furthermore, the analysis should reveal what kind of value own ICTs present as a target, identify the cybersecurity controls and how they operate. The analysis should provide an understanding of cyberspace development and how to modify it to decrease the adversary's capabilities and opportunities and increase advantages. The last phase of the analysis, interaction, should provide a profound understanding of how the different elements collide in cyberspace. The definitive objective of this strategic cybersecurity analysis model is to provide valid and reliable knowledge that can be utilized when making appropriate decisions, on time and in advance, regarding future cybersecurity capabilities.

6 DISCUSSION

This research answers all the research questions. The researcher defined the substance of strategic cybersecurity analysis, identified the essential elements, their relations and impact, described the analysis process, and presented the utilization of the results. However, these results cannot fully define strategic cybersecurity analysis. The results indicate that gaining an advantage and systematically design and develop cybersecurity requires significant resources and time. Furthermore, the quality of the analysis does not depend on the capability to categorize all the essential elements. The quality is determined by the capacity to collect relevant information of these categories for the analysis. This model may support the collection, but it cannot replace it.

The analysis model is relatively detailed on the upper-level, but the flexibility increases in sub-categories. This solution aims to support the analysis in different environments, organizations, situations and level of granularity. The model presented here does not provide a fit-for-all solution. There is always a need for in-depth cybersecurity expertise. The reliability and validity of the model are ensured by using existing models in categorization. Nevertheless, at some point in the analysis, the objects are subdivided into such detailed parts that no existing categorizing model can support the analysis. Identifying the intricate parts, their characteristics, and relations require significant expertise, in addition to the capable information collection.

The researcher had two options to address the objectives of the research. The first one would have been philosophical, aiming to examine the phenomenon from different angles. That would have resulted in an increased understanding of strategic cybersecurity analysis, but mainly describing it without any practical relevance. On the other hand, the chosen approach aimed to understand the phenomenon and provide a practical tool to increase the knowledge and support the development of cybersecurity. The selection of the approach determined that the objective was not to define strategic cybersecurity analysis completely but merely to define how it can be done.

The topic and objectives of the research steered the research design. The objective was to construct a novel model that could be used in the evaluative and estimative analysis. It was clear that the research must be exploratory, based on qualitative research methodology. The challenges related to the reliability and validity of the research were identified already in the beginning. For reliability and validity reasons, an abductive approach was chosen. The beginning of the research relied on the different theories of ontology, using a deductive approach. The support of the theories ensured that the research included all the elements in a dynamic environment and the components of intention, capability and opportunity. The construction part of the research used a more inductive approach. This solution provided appropriate confidence to the researcher that the research addresses relevant factors of cybersecurity. As a research strategy, constructive research was an appropriate choice. It supported the construction of an innovative model aimed to solve practical problems. The main deficiency was that the research time did not allow the installation and testing of the model in a real-life environment. Therefore, any empirical evidence of the use of the model will be available after this research. This shortcoming was not assessed to be significant enough to extend the research and delay the researcher's graduation.

Content analysis using templates was a solid choice. Template analysis supported the classification of cybersecurity actors and the construction of the model. Data collection, analysis and the construction of the model were closely intermingled. The analysis guided the data collection and the construction of the model, making the whole process interactive. The researcher's most significant surprise was how time-consuming a constructive research strategy can be when using qualitative data combined with an abductive approach and content analysis.

Cybersecurity is based on the legacy of information security, where the emphasis is mainly on technical information systems. This research aims to broaden this approach. First of all, the analysis model is threat-based, starting from the cyber threat and regarding own ICTs as a target. Compared to traditional vulnerability-based analysis, this approach enables identification of the emerging threats. Furthermore, this research aims to regard cybersecurity as a strategic phenomenon. Cyber threats, target systems and cyberspace might be interesting entities by themselves, but they are more interesting as part of the larger strategic influencing. Hopefully, this model supports the analysis of cybersecurity itself and cybersecurity in a broader strategic context.

This research can be considered as a step towards increased understanding of cybersecurity in a strategic context. The results are not comprehensive enough to determine strategic cybersecurity analysis from every possible angle. For future research, every step of this model constitutes a viable topic. Furthermore, the strategic cybersecurity analysis has no value of its own. The value is determined by how well it can support cybersecurity decision-making. Examining this model as part of cybersecurity decision-making would provide detailed information about the feasibility of the model. Also, the capability to support the interoperability between different organizations would be interesting. Future research should focus on how well this model can support proactive cybersecurity decision-making and what requirements are set for other steps of the decision-making process.

REFERENCES

Ackoff, R. (1989). From Data to Wisdom. *Journal of Applied Systems Analysis, 16, (1989), 3–9.*

Alisherov, F. & Sattarova, F. (2009). Methodology for Penetration Testing. *International Journal of of Grid and Distributed Computing, Vol. 2, No. 2, June 2009, 43 – 50.*

Alkire, B., Lingel, S. & Hanser, L. (2018). A Wargame Method for Assessing Risk and Resilience of Military Command-and-Control Organizations. Santa Monica, CA: RAND Corporation.

Ami, P. & Hasan, A. (2012). Seven Phrase Penetration Testing Model. *International Journal of Computer Applications, Volume 59, No. 5, December 2012, 16 – 20.*

Andrews, K. (1997). The Concept of Corporate Strategy. In N. J. Foss (Ed.), *Resources, Firms and Strategies (50 – 59).* New York: Oxford University Press.

Baskerville, R. (1991). Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security. *European Journal of Information Systems 1(2), 121 - 130.*

Baskerville, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys, Vol 25, No. 4. December 1993, 375 – 414.*

Bayne, J. (2002). An Overview of Threat and Risk Assessment. *Sans Institute InfoSec Reading Room, 2002.*

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices (2nd ed.). *University of South Florida, 2012. Textbooks Collection, 3. Accessed 9.12.2021. http://scholarcommons.usf.edu/oa_textbooks/3.*

Bittner, T. (2019a). Formal Ontology of Space, Time, and Physical Entities in Classical Mechanics. *Applied Ontology 0 (2019) 1–0, 1 – 39.*

Bittner, T. (2019b). On the Computational Realization of Formal Ontologies: Formalizing an Ontology of Instantiation in Spacetime using Isabelle/HOL as a case study. *Applied Ontology, vol. 14, no. 3, 251-292.*

Bittner, T. & Smith, B. (2003). Formal Ontologies for Space and Time. *IFOMIS report, 2003.*

Bodeau, D. & Graubart, R. (2017). Cyber Prep 2.0. Motivating Organizational Cyber Strategies in Terms of Preparedness. *Mitre Corporation, 2017, Bedford MA.*

Cavusoglu, H., Raghunathan, S. & Yue, W. (2014). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems, 25:2, 281-304.*

Chairman of the Joint Chiefs of Staff (2016). Guidance for Developing and Implementing Joint Concepts. *CJCSI 3010.02E. 17 August 2016.*

Chang, W. & Granger, S. (2012). Warfare in the Cyber Domain. *Air and Space Power Journal, 2012.*

Collier, Z., Linkov, I. & Lambert, J. (2013). Four Domains of Cybersecurity: A Risk-based Systems Approach to Cyber Decisions. *Environment Systems & Decisions, (2013), 469–470.*

Crowther, G. (2017). The Cyber Domain. *The Cyber Defense Review. Vol. 2, No. 3. (Fall 2017), 63 – 78.*

De Gusmao, A., Silva, L., Silva, M., Poleto, T. & Costa, A. (2016). Information Security Risk Analysis Model Using Fuzzy Decision Theory. *International Journal of Information Management, 36, 25 –34.*

Denzin, N., & Lincoln, Y. (2005). Introduction: The Discipline and Practice of Qualitative Research. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage handbook of qualitative research (1 – 32).* Washington D.C: Sage Publications Ltd

Department of Commerce (2020). Security and Privacy Controls for Information Systems and Organizations. *NIST Special Publication 800-53 Revision 5, September, 2020.*

Department of Defence (2014). Joint Intelligence Preparation of the Operational Environment. *Joint Publication 2-01.3., 21 May 2014.*

Department of Defence (2017). Joint Targeting. *Joint Targeting School, Virginia. 1 March 2017.*

Department of Defence (2018). Cybespace Operations. *Joint Publication 3-12. 5 February 2018.*

Department of Defence (2020). DOD Dictionary of Military and Associated Terms. *June 2020.*

Feng, N. & Li, M. (2011). An Information Systems Security Risk Assessment Model Under Certain Environment. *Applied Soft Computing 11, 2011, 4332 – 4340.*

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. & Smeraldi, F. (2014). Game Theory Meets Information Security Management. In N. Cuppens-Boulahia et al. (Eds.). *SEC 2014, IFIP AICT 428, 2014. IFIP International Federation for Information Processing 2014, 15–29.*

Fourkas, V. (2004). What is 'Cyberspace'? *Aristotle University of Thessalonica, 2004.*

Geers, K. (2011). Strategic Cyber Security. *Publication of Nato Cooperative Cyber Defence Center of Exellence.* Tallinn: CCD COE Publication.

Goel, R., Kumar, A. & Haddow, J. (2020). PRISM: A Strategic Decision Framework for Cybersecurity Risk Assessment. *Information & Computer Security Vol. 28 No. 4, 2020, 591-625.*

Grenon, P. & Smith, B. (2004). SNAP and SPAN: Towards Dynamic Spatial Ontology. *Spatial Cognition and Computation, 4:1 (March 2004), 69 – 103.*

Hellman, M. & Wagnsson, C. (2017). How can European states respond to Russian information warfare? An analytical framework. *European Security, 2017, Vol 26, No. 2, 153-170.*

Herre, H., Hellert, B., Burek, P., Hoehndorf, R., Loebe, F. & Michalek, H. (2006). General Formal Ontology (GFO), Part I : Basic Principles. *University of Leipzig, No. 8, July 2006.*

Heuer, R. (1999). Psychology of Intelligence Analysis. (2018). Eastford: Martino Fine Books.

Hibbs Pherson, K. & Pherson, R. (2017). Critical Thinking for Strategic Intelligence (2nd ed.). *Kindle Edition.* Thousand Oaks: Sage Publications.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). Tutki ja kirjoita (22nd ed.). Porvoo: Kirjayhtymä Oy.

Holzer, C. & Merrit, J. (2015). Risk Assessment in Cyber Resiliency. *Progress Report, Purdue University, 13 May 2015.*

Hu, H., Liu, Y., Chen, C., Zhang, H. & Liu, Y. (2020). Optimal Decision Making Approach for Cyber Security Defense Using Evolutionary Game. *IEEE Transactions on Network and Service Management, Vol. 17, No. 3. September 2020, 1683 – 1700.*

Huang, D., Hu, Q. & Behara, R. (2008). An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-Averse Firm. *Int. J. Production Economics, 114, 793– 804.*

Hundley, R. & Anderson, R. (1995). Emerging Challenge: Security and Safety in Cyberspace. *IEEE Technology and Society, Winter 1995/1996, 19–28.*

International Organization for Standardization (2018). Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary. *International standard ISO/IEC 27000:2018(E).*

Iwaniak A., Łukowicz, J., Strzelecki, M. & Kaczmarek, I. (2013). Ontology Driven Analysis of Spatio-temporal Phenomena, Aimed at Spatial Planning and

Environmental Forecasting. *Conference Paper, Photogrammetry, Remote Sensing and Spatial Information Sciences, Vol. XL-7/W2, November 2013.*

Jalali, M., Siegel, M. & Madnick, S. (2019). Decision-making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment. *Journal of Strategic Information Systems 28. (2019), 66–82.*

Jansen, L. (2018). Categories: The Top-Level Ontology. *Applied Ontology, January 2008, 173 – 196.*

Jarrar, T. & Ceusters, W. (2017). Classifying Processes and Basic Formal Ontology. *Conference paper, International Conference on Biomedical Ontology (ICBO 2017).*

Karabacak, B. & Sogukpinar, I. (2005). ISRAM: Information Security Risk Analysis Method. *Computers & Security, 24, 147 – 159.*

Kolini, F. & Janczewski, L. (2015). Cyber Defense Capability Model: A Foundation Taxonomy. *International Conference on Information Resources Management. CONF-IRM 2015 Proceedings, 32.*

Kramer, F. (2009). Policy Recommendations for a Strategic Framework. In Kramer, F., Starr, S. & Wentz, L. (eds.). *Cyberpower and National Security (3 – 23). Center for Technology and National Security Policy, National Defence University.* Dulles, VA: Potomac Books.

Kwan J. & Johnson, E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly Vol. 38 No. 2, June 2014, 451 – 471.*

Lehto, M. & Limnell, J. (2016) Cyber Security Capability and Case Finland. *Proceedings of the 15th European Conference on Cyber Warfare and Security ECCWS2016, 7-8th July 2016, Bundeswehr University, Munich, Germany, 182-190.*

Lemay, A., Knight, S. & Fernandez, J. M. (2014). Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace. *Journal of Information Warfare, vol 13, No. 3 (2014), 46 – 56.*

Liew, A. (2007). Understanding Data, Information, Knowledge and their Inter-Relationships. *Journal of Knowledge Management Practice, Vol. 8, No. 2, June 2007.*

Little, E. & Rogova, G. (2006). An Ontological Analysis of Threat and Vulnerability. *IEEE 2006 9th International Conference on Information Fusion, 1–8.*

Little, E., Rogova, G. & Boury-Brisset, A.-C. (2008). Theoretical Foundations and Proposed Applications of Threat Ontology to Information Fusion. *Technical Report DRDC, Defence R&D Canada, Valcartier TR 2005-269, November 2008.*

Little, E. & Rogova, G. (2009). Designing Ontologies for Higher Level Fusion. *Information Fusion 10 (2009), 70 – 82.*

Lo, C. & Chen, W. (2012). A Hybrid Information Security Risk Assessment Procedure Considering Interdependences Between Controls. *Expert Systems with Applications, 39, 247–257.*

Lukka, K. (2003). The Constructive Research Approach. In Ojala L. & Hilmola, O-P. (eds.). *Case Study Research in Logistics (83 – 101). Turku School of Economics and Business Administration,* Turku: Grafia.

Mateski, M., Trevino, C., Veitch, C., Michalski, J., Harris, M., Maruoka, S. & Frye, J. (2012). Cyber Threat Metrics. *Sandia Report, SAND2012- 2427. Sandia National Laboratories, 2012.*

McDonnell, J. (2009). National Strategic Planning: Linking DIMEFIL/PMESII to a Theory of Victory. *Master's thesis. Joint Forces Staff College, National Defence University. April 2009.*

Merriam, S. (2002). Introduction to Qualitative Research. *Qualitative Research in Practise: Examples for Discussion and Analysis (3-17).* San Francisco, CA: Jossey-Bass.

Merriam-Webster Dictionary (2020). Definition of "analysis". Accessed 27.2.2020. *https://www.merriam-webster.com/dictionary/analysis.*

Merriam-Webster Dictionary (2020) Definition of "cybersecurity". Accessed 20.4.2020. *https://www.merriam-webster.com/dictionary/cybersecurity*.

Merriam-Webster Dictionary (2020) Definition of "doctrine". Accessed 23.3.2020. *https://www.merriam-webster.com/dictionary/doctrine.*

Merriam-Webster Dictionary (2020). Definition of "ontology". Accessed 23.3.2020. *https://www.merriam-webster.com/dictionary/ontology.*

Merriam-Webster Dictionary (2020). Definition of "policy". Accessed 27.2.2020. *https://www.merriam-webster.com/dictionary/policy.*

Merriam-Webster Dictionary (2020). Definition of "strategic". Accessed 27.2.2020. *https://www.merriam-webster.com/dictionary/strategic*.

Miskimmon, A., O'Loughlin, B. & Roselle, L. (2013). Strategic Narratives. Communication Power and The New Order. NewYork: Routledge, 2013.

Ministry of Foreign Affairs of Finland, (2020). International law and cyberspace. Finland's national positions. Accessed 30.10.2020. https://um.fi/documents.

National Institute of Standards and Technology (NIST) (2018). Framework for Improving Critical Infrastructure Cybersecurity. *Version 1.1, April 16, 2018.*

Obrst, L., Chase, P. & Markeloff, R. (2012). Developing an Ontology of the Cyber Security Domain. *STIDS, volume 966 of CEUR Workshop Proceedings, 49 - 56.*

Oltramari, A., Cranor, L., Walls, R. & McDaniel, P. (2014). Building an Ontology of Cyber Security. *The 9th International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS 2014), 54 – 61.*

O'Neil, W. (2009) Cyberspace and Insfrastructure. In Kramer, F., Starr, S. & Wentz, L. (eds.). *Cyberpower and National Security (113 – 146). Center for Technology and National Security Policy, National Defence University.* Dulles, VA: Potomac Books.

Ormrod, D. & Turnbull, B. (2016). The Cyber Conceptual Framework for Developing Military Doctrine. *Defence Studies, 16:3, 270 - 298.*

Park, S. & Ruighaver, T. (2008). Strategic Approach to Information Security in Organizations. *International Conference on Information Science and Security. Seoul, Korea, 10 – 11 January, 2008.* Los Alamitos, CA: IEEE Computer Society.

Paul Rees, L., Deane, J., Rakes, T. & Baker, W. (2011). Decision Support for Cybersecurity Risk Planning. *Decision Support Systems 51 (2011), 493 – 505.*

Pfleeger, S. (2009). Useful Cybersecurity Metrics. *IT Professional Magazine, Vol 11, Iss. 3, May/Jun 2009, 38 – 45.*

Raggad, B. (2010). Information Security Management. Concepts and Practice. Boka Raton, FL: Taylor & Francis Group.

Rattray, G. (2009). An Environmental Approach to Understanding Cyberpower. In Kramer, F., Starr, S. & Wentz, L. (eds.). *Cyberpower and National Security (253 – 274). Center for Technology and National Security Policy, National Defence University.* Dulles, VA: Potomac Books.

Rowley, J. (2006). The Wisdom Hierarchy: Representations of the DIKW Hierarchy. *Journal of Information Science, 33 (2) 2007, 163 – 180.*

Rugge, F. (2018). Mind Hacking: Information Warfare in the Cyber Age. *Istituto per gli Studi di Politica Intrnazionale. Analysis No. 319, January 2018.*

Saleh, M. & Alfantookh, A. (2011). A New Comprehensive Framework for Enterprise Information Security Risk Management. *Applied Computing and Informatics, 9, 107–118.*

Saunders, M., Lewis, P. & Thornhill, A. (2012). Research Methods for Business Students (6th ed.). *Pearson Education UK, England, 2012. E-book.*

Scoblic, P. & Tetlock, P. (2020). A Better Crystal Ball, The Right Way to Think About the Future. *Foreign Policy, November/December 2020.*

Security Committee, (2019). Finland's Cyber Security Strategy 2019. *Government Resolution 3.10.2019.*

Schechter, S. (2004). Computer Security Strength & Risk: A Quantitative Approach. *Thesis for the Degree of Doctor of Philosophy. Harvard University, Cambridge, Massachusetts, May 2004.*

Sigholm, J. & Bang, M. (2013). Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats. *Intelligence and Security Informatics Conference (EISIC), 2013 European, 166 - 171.*

Singleton, R. & Straits, B. (2005). Approaches to Social Research (4th ed.). New York: Oxford University Press, 2005.

Smith, B. (1996). Mereotopology: A Theory of Parts and Boundaries. *Data and Knowledge Engineering, 20 (1996), 287 – 303.*

Steinberg, A. (2005). Threat Assessment Technology Development. In Dey, A., Kokinov, B, Leake, D. & Turner, R (eds.). *Proceedings of Modeling and Using Context (490 – 500). 5th International and Interdisciplinary Conference.* Paris, France, July 2005.

Syed, Z., Padia, A., Finin, T., Mathews, L. & Joshi, A. (2016). UCO: A Unified Cybersecurity Ontology. *The Workshops of the Thirtieth AAAI Conference on Artificial Intelligence. Artificial Intelligence for Cyber Security: Technical Report WS-16-03, 195 – 202.*

Thomsen, E. & Smith, B. (2018). Ontology-based Fusion Sensor Data and Natural Language. *Applied Ontology 13 (4), 2018, 295 - 333.*

Tikk-Ringas, E. (2015). Evolution of the Cyber Domain: The Implications for National and Global Security. *IISS Strategic Dossier*. London: Routledge.

Tuomi, J. & Sarajärvi, A. (2018) Laadullinen tutkimus ja sisällönanalyysi (2nd ed.). Helsinki: Tammi.

Turvallisuuskomitea (2018). Kyberturvallisuuden sanasto. Helsinki: Sanastokeskus TSK ry.

Ulicny B., Moskal J., Kokar M., Abe K. & Smith J. (2014). Inference and Ontologies. In Kott, A., Wang, C. & Erbacher, R. (eds.). *Cyber Defense and Situational Awareness Advances in Information Security (167 – 200). Vol 62.* Springer.

Vandepeer, C. (2011). Intelligence Analysis and Threat Assessment: Towards a More Comprehensive Model of Threat. *Proceedings of the 4th Australian*

Security and Intelligence Conference (103 – 111), 5th -7th December. Perth: Edith Cowan University.

Waltzman, R. (2017). The Weaponization of Information. The Need for Cognitive Security. *Testimony in the Senate Armed Services Committee, Subcommittee on Cybersecurity, April 27, 2017.*

Wang, P., Chao, K.-M., Lo, C.-C. & Wang, Y.-S. (2017). Using Ontologies to Perform Threat Analysis and Develop Defensive Strategies for Mobile Security. *Information Technology and Management, 18, 1 – 25.*

Winterfeld, S. (2001). Use Offense to Inform Defense. Find Flaws Before the Bad Guys do. *GSEC Practical Requirements. SANS Institute, 2001.*

Yevseyeva, I., Basto-Fernandes, V., Emmerich, M. & van Moorse, A. (2015). Selecting optimal subset of security controls. *Procedia Computer Science, 64, (2015), 1035 – 1042.*

Yin, R. (2009). Case study research: Design and methods (4th ed.). Thousand Oaks, CA: Sage.

Zenko, M. (2015). Red Team. How to Succeed by thinking Like the Enemy. New York, NY: Basic Books, 2015.

Zimet, E. & Skoudis, E. (2009). A Graphical Introduction to the Structural Elements of Cyberspace. In Kramer, F., Starr, S. & Wentz, L. (eds.). *Cyberpower and National Security (91 – 112). Center for Technology and National Security Policy, National Defence University.* Dulles, VA: Potomac Books.