Juhani Matilainen

USING CYBER THREAT INTELLIGENCE AS A PART OF ORGANISATIONAL CYBERSECURITY

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2021

ABSTRACT

Matilainen, Juhani
Using Cyber Threat Intelligence as a part of organizational cybersecurity
Jyväskylä: University of Jyväskylä, 2020, 55 pp.
Information Systems Science, Master's Thesis
Supervisor: Lehto, Martti

Cyber Threat Intelligence (CTI) has gained public attention at the same time security breaches are publicised in the press. This thesis is conducted as qualitative study to research Cyber Threat Intelligence usage to harder organisations' cyber defence. Through content analysis, 14 documents were coded and analysed to form a preliminary framework for CTI usability in organisations.

This thesis is using known OODA loop as framework to clarify CTI usage in organizations. As qualitative study, one framework was created. For results, CTI can provide much needed addition for organisational cyber security. From strategic to tactical, CTI can enhance cyber defence is properly used.

Keywords: Cyber Threat Intelligence, Cybersecurity, Situational awareness, Intelligence analysis

TIIVISTELMÄ

Matilainen, Juhani
Using Cyber Threat Intelligence as a part of organizational cybersecurity
Jyväskylä: Jyväskylän yliopisto, 2020, 55 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Kyberuhkatiedustelu on hieman kiistanalainen aihe ammatillisissa ja akateemisissa piireissä. Koska osa-alue on vielä nuori, tutkimus toimivuuden osalta on vielä vähäistä. Julkisuudessa moni kyberhyökkäys on saanut huomiota. Tämä tutkimus selvittää kyberuhkatiedustelun käyttöä osana organisaatioiden kyberpuolustusta.

Tutkielma tehtiin laadullisena tutkimuksena, sisällön analyysin keinoin valitsemalla 14 dokumenttia. Näiden dokumenttien ja OODA silmukan pohjalta luotiin viitekehys kyberuhkatiedustelun käyttöön organisaatioissa. Johtopäätöksenä on todettu, että kyberuhkatiedustelu voi tarjota tarvittavaa tietoa, jolla organisaatio voi puolustautua kyberuhkia vastaan.

Asiasanat: Kyberuhkatiedustelu, kyberturvallisuus, tilannetietoisuus, tiedusteluanalyysi, tietoturva

FIGURES

TABLES

CONTENT

1 INTRODUCTION

Cybersecurity has gained public attention as new attacks with serious consequences are reported constantly. In their company's blog, cybersecurity company IT governance recorded 117 publicly reported security incidents and 18,407,479 data records were compromised in October 2020 (Irwin, 2020). This raises a question if all the incidents are noticed and reported. As number of incidents seems to raise all over the world, IT governance gave to October 2020 a questionable title "the leakiest month we've ever reported" (Irwin, 2020). A pessimist might argue that we have lost the tug of war in cybersecurity.

The topic of Cyber Threat Intelligence (CTI) stirs up debate as it is young concept in the field of cybersecurity. However, there are limited amount of available information about CTI implementation and usability, although some private companies are already turned CTI into a product and advertising its use. For example, one of the leading Cyber threat intelligence providers, Check Point Research, suggest in their report to keep organizations their threat intelligence up to date as it is the most effective proactive cybersecurity solutions available (Check Point Research, 2020, pp 61). Despite statements above, cyber threat intelligence is still under researched subject in academic research. There is professional literature concerning CTI, but they are mainly offering general advice when detailed information about CTI implementation is lacking comprehensive model.

Cyber Threat Intelligence can be divided into three sub-categories. Strategic intelligence is for C-level executives and board of directors of the organisation. It is mainly used for long-term decision-making. Operational intelligence is considering about recognized threat actors and their modus operandi. Tactical intelligence is assisting the CSOC (Cyber Security operations Center) operations and providing technical recommendations.

This thesis is using content analysis as research method to clarify usability of Cyber Threat Intelligence in organisations. To research this phenomenon, 14 documents was chosen for analysis. These documents were coded, and excerpts of these codes were analysed to create preliminary model for CTI usability.

Framework of this study is OODA loop. This model is used to describe CTI usability in organisations.

1.1 Research problem

The research problem of this thesis is closely related to organisations' problem to make use of huge amount of data they have available. Research questions of the thesis are related to organisational cybersecurity and to the goal to improve it. With Cyber Threat Intelligence (CTI), organisations are able to improve the security and provide better situational awareness.

The main research question of the thesis is:

- How CTI can be used to improve organisation's cybersecurity?

To clarify the research problem, the main research question is divided into three separate sub-research questions:

- How can CTI be utilized in organisational decision making?
- How the available information should be used by the organisation in maintaining cybersecurity posture?
- How can CTI improve an organisation's cyber situational awareness?

The first of the sub-research questions relates to organisational decision-making processes. While cybersecurity is continuous competition between defenders and adversaries, this requires constant improvement and process development. To make proper decisions, accurate and timely information is needed in decision-making. With this first sub-question, this thesis is trying to answer if CTI can provide support for decision makers.

Available information can also be utilized in strategic decision-making, in which case it must be possible to assess the state and development of the organisation's cybersecurity in the long term. The second sub-question seeks to answer if CTI can be used in strategic decision making helping executives and governance-level decision makers to improve their judgement on current state of cybersecurity.

The purpose of the third sub-research question is to examine an organisation's ability to perceive events in the immediate vicinity of its cyberspace and recognise immediate threats which can threaten its assets and/or capability to operate.

This thesis therefore seeks to take into account the strategic, operational, and tactical levels of the CTI. In this case, it should be noted that each subsection of intelligence has a different customer in the organisation. For this reason, thesis does not include the medium or type of provided intelligence product. It is assumed that the information exists in a form that the customer is able to utilise it.

It should be also noted that CTI refers to a number of different products that, due to delineation, cannot be covered in great depth. This thesis is meant to be a general overview of CTI usage in organisations.

1.2 Structure

This thesis is divided into five different sections. Firstly, introduction gives a brief overview of the topic. Literature overview discussed about current state of academic literature about Cyber Threat intelligence, cybersecurity, situational awareness, and threat landscape. Next, research method of this study is introduced. The used method – content analysis – is described. In addition, the processes of data acquisition and coding is described. In results section, the outcome of this study is gone through. Lastly, in discussion and conclusion section, there are discussion about limitations of this study and suggestions for further research. Also, research questions are answered.

2 LITERATURE REVIEW

In this section, organisational cyber security is introduced. Organisations are facing various different threats daily. If realised, these threats can seriously hinder organisation's ability to act and perform daily tasks. To counter facing threats, organisations need to have a clear view of the current threat landscape and maintain proper situational awareness.

Cyber threat intelligence (CTI) is also introduced. CTI is divided into three subsections. These subsections have different customers inside the organisation. Every subsection has different goals to improve cybersecurity. CTI is supporting function to improve organisational cyber defence and offering assistance for organisation decision-making.

The OODA loop is one of the well-known decision-making models which originates from Korean War. The loop has four known phases – observe, orient, decide and act. In addition, loop consists of feedback and implicit guidance & control elements, which are used to improve decision-making in next cycle of the loop.

2.1 Cybersecurity

At the same time when information system architectures have become more complex, their attack surface has been increased. Attackers have also developed as they are using more subtle tools and tactics. In organisations' standpoint, cyber breaches can cause serious damage and hinder ability to operate. Therefore, organisations need to reconsider value of their assets and efficacy of their security controls. Control mechanisms can be hard to implement as IS infrastructure consist of multiple different devices, which may have serious security issues. This requires adaptive and agile security. Current situation can be alleviated by allocating resources to more precise situational awareness development. They are already known ways to use security-related data for better security. This data must be utilised more carefully for better security posture and decision-making.

2.1.1 Organisational cybersecurity

During the ongoing, rapid digitalisation, organisations' ways to utilise information technology is changed tremendously. New information systems are becoming more complex than ever before, and organisational daily routines are more dependent on properly functioning and reliable IT-services. At the same time, different threat actors are developing new ways to go around security controls and avoid detection. The fundamental purpose of organisation's cyber defence can be summarised into three different elements as they are the basic parameters, which are needed for secure environment (Stewart, Chapple & Gibson, 2015, pp. 3):

- Confidentiality
- Integrity
- Availability

This is known as the CIA triad and it is one of the most well-known frameworks in cybersecurity discipline. Of course, the order of priority of these elements is dependable on organisation and its goals.

In their paper, Borum, Felker, Kern, Dennesen and Feyes (2015) state that successful cyber defence relies heavily on identifying, assessing, and managing risks. As cyber-related risks are as real as other risk organisation is facing, single breach or incident can cause serious damage to organisations ability to operate. For this reason, cyber risks should be analysed in the context of the organisation's total risk (Borum et al., 2015). In this point-of-view, proper risk-based decision-making for risk mitigation is needed to mitigate risk into acceptable level. As Borum et al. (2015) states, the foundations of risk-informed decision-making is based on three separate factors:

- Recognising value and vulnerability of organisational assets
- Considering threats facing those assets
- Allocating resources accordingly to counter and mitigate identified threats

As complex as information systems are today, this requires more advanced level of cybersecurity. Traditional way of reactive security is no longer be able to undertake this task alone. During the history of computer security, attacks have evolved from fast and destructive to more subtle and cunning way to operate. Mathews, Halvorsen, Joshi and Finin (2012) did notice this change and called for new ways to protect the systems. New and enhanced level of cybersecurity can be implemented by taking an anticipating stance when protecting organisational assets (Saurabh, Baidyanath, Manjot & Manoj, 2020). In addition of updating security controls to a better level, organisations need to create new ways to counter zero-day vulnerabilities and new kind of malicious activities (Bhardwaj & Goundar, 2019).

2.1.2 Threat landscape

When dealing this ever-complexing state of information systems, one old information security adage comes into mind: “security loves simplicity” as these new infrastructures are giving a hard time to cybersecurity experts and personnel. On top of that, any new devices are lacking security updates and can be considered insecure as various vulnerabilities are found. Although, it is very difficult to remove all critical vulnerabilities from source code, this problem continues to exist, and threat actors are using it for their full advantage. 10 years ago, (Choo, 2011) identified smart devices, ATMs, and point-to-sales machines as possible attack vectors. Today, number of these devices have been multiplied as these are now part of people’s everyday lives and ways of working. In addition, new kind of Internet of Things (IOT) devices are beginning to find the way to people’s homes, offices, and workplaces.

The most conspicuous problem of these new type of threats are their dynamic nature (Bhardwaj & Goundar, 2019; Borum et al., 2015). As organisations are becoming more aware of used attack methodologies, adversaries are constantly figuring out new ways to bypass security controls. For the blue teams as defenders, this means that a continuous threat analysis and monitoring has become one of the compulsory processes (Borum et al., 2015). For counter measures, organisations need to re-evaluate their threat analysis and incident response processes (Ring, 2014).

2.1.3 Situational awareness

One of the fundamentals of cyber defence is a proper and accurate security awareness. Awareness requires a broad understanding of the current security situation. After this is achieved, countermeasures can be selected effectively. Safa and Von Solms (2016) support this consideration as they state that, situational awareness is the most important factor that helps to mitigate breaches in organisations. To keep organisations’ situational awareness up to date, internal and external audit must be conducted regularly (Tounsi & Rais, 2018). This is done to gain understanding about state of current security posture of the organisation. Other processes - like penetration testing and Red Teaming - can also be utilised. Here the main goal is to make information-based assumptions about what attacker can do and how organisations security personnel can prevent it from happening.

To develop an effective situational picture, organisation needs information about possible threats and their methodologies. During their research (Kotenko & Doynikova, 2014) conducted a case study about security metrics for situational awareness formation. Even it is possible to successfully create better security awareness by analysing network events, used taxonomy needs reliable knowledge about possible adversaries in this used methodology (Kotenko & Doynikova, 2014). This is one example of ways of external data using, which have already gained attention from scholars and professionals. Critique from Tianfield (2016) implies that even if use of data in network systems have gotten some of researchers' attentions, there is still a need of broader concept of situational awareness than just organisational networks. Also, data must be deal with in a holistic manner to gain better understanding at whole infrastructure (Tianfield, 2016).

Cybersecurity cannot be carried out only by technical manners as there is always a human aspect. In their study, Hibshi, Breaux, Riaz, and Williams (2016) found that security experts sometimes ignore some parts of situational awareness and make decisions based on previous experiences. If current situation appears to be similar on the surface, security personnel might ignore some of the vital information as they are relying on their previous experiences. This implicates that organisation might be lacking proper processes to handle important data for effective security.

2.2 Cyber threat intelligence

Intelligence is evidence-based, actionable knowledge, which is used to support decision-making in different parts of the organisation hierarchy. Cyber threat intelligence (CTI) is used to predict and to warn of imminent or ongoing attacks against organisation. In addition, CTI can be used as educational material for organisation's personnel. Current state of CTI also faces many challenges and criticism which are also discussed in this chapter. In this paper, CTI is divided into three different categories or subsections which all have different characteristics.

2.2.1 Definition

As a concept, it is hard to get exact and pervasive definition on what is cyber threat intelligence (CTI). This is because many academics and professional literature in the field defines this term differently. Situation becomes even more confusing, when many commercial organisations enlist different product as "threat intelligence" (TI) (Tounsi & Rais, 2018).

Generally, we can think "intelligence" as providing to the decision-maker evidence-based, useable information and time to react. When we are talking about "threat intelligence", it can be defined evidence-based knowledge on threats and can be used to support decision-making (Tounsi & Rais, 2018). In this context, threat intelligence is a raw data which has been refined during context-including evaluation process to form a useable product (Dalziel, 2015, pp. 4). The definition of this concept is becoming more relevant than ever before as CTI is one of new ways to fight against adversaries in the cyberspace. As our networks and different solutions are becoming more complex, CTI can be seen as knowledge considering security incidents (Abu, Selamat, Ariffin & Yusof, 2018). When an organisation is looking for improve its cyber defence capability, intelligence plays a key role in this task (Borum et al., 2015). Even if intelligence might be hard to implement into organisation's processes, this is a goal worth pursuing. As an organisation is pushing new measurements to use, proactive security measures are crucial part of more secure cyber environment for organisations (Saurabh et al., 2020).

When defending organisation's network and assets, useful and up-to-date information is highly desired. Knowledge about emerging and current threats may be presented in several different forms. Tounsi and Rais (2018) subdivide threat intelligence as including technical indicators, context, mechanisms, implications, and advisory aspects about current or emerging threat. This underlines intelligence as being a supporting organisational function and process. As intelligence is a supporting process, the product must meet the demands of the intelligence users or customers in order to be useful. Requirements for proper CTI are as following reported by Roberts and Brown (2017) and Abu et al. (2018):

- Relevant to organisation
- Clear to the target audience/readership
- Concise in form
- Timely
- Accurate
- Actionable

In the context of organisational cyber defence, right type, accurate and timely intelligence can help organisations managers and senior leadership consider proper countermeasures through risk management program (Borum et al., 2015). As intelligence is needed to support decision-making, this requires the analyst to be aware of organisation's objectives and goals. Typically, as intelligence is used to reduce uncertainty, effective intelligence analysis requires the analyst to understand the faced problem, desired outcomes and impact and prioritisation of undesired outcomes (Borum et al., 2015). Generally, for critical infrastructure incident handling, intelligence created from incident data is proven to be crucial aspect (Skopik, Settanni & Fiedler, 2016). Similar kind of findings were reported in network analysis studies mentioned above. In addition, one of the main goals of cyber threat intelligence is to create and maintain organisation's situational awareness to identify potential threats and current incidents (Skopik et al., 2016).

CTI can be also used for developing security personnels' professional expertise. As intelligence is now more commonly bought from external service provider or shared with other organisations, this provides real-time learning material to security stakeholders. Exchange and proper use of threat data have been shown to avert potential cyber-attacks and alleviate ongoing attacks including possible future events (Tounsi & Rais, 2018). When experts from various organisations share information, this builds up collective knowledge and helps to identify more complex attacks which organisation is facing (Williamson, 2016). Users of threat intelligence also include threat hunters who use it to facilitate their own processes to perceive suspicious activities inside organisation's network (Bhardwaj & Goundar, 2019). In this perspective, CTI has an educational and directive role.

There are still already known and recognised problems with CTI. Oosthoek & Doerr (2020) states in their paper that, as CTI is still in its infancy, it has several major flaws. Like stated above, CTI is often bought or received from external party. When organisations are using different naming systems, standards, and processes, this also affects to quality of the intelligence. Skopik et al. (2016) wrote at their paper that varying quality of the intelligence causes problems to intelligence analysts. When the quality is questionable, analyst is required to make even more careful judgements about information credibility and integrity (Skopik et al., 2016). CTI can also be considered being too biased for organisations to use. As intelligence providers are focusing on known and influential threat actors, smaller and less know actors continue to stay underestimated (Oosthoek & Doerr, 2020). In other study, Tounsi and Rais (2018) stated that outdated information is one of the major concerns of shared intelligence. Ring (2014) has a same conclusion. Other major defect is that received intelligence is not specific enough to be used in decision-making and products are ineffective or outdated (Ring, 2014; Tounsi & Rais, 2018).

2.2.2 Intelligence subsections

Cyber threat intelligence is divided into different subsections which all have different characteristics, purpose, customer, and form. They are used to support different decisions and are used in different levels inside the organisation. In this study, we are using common tripartition of cyber threat intelligence products. These subsections are (Eom, 2014; Roberts & Brown, 2017, p. 24):

- Strategic
- Operational
- Tactical

It should be noted that some authors describe only strategic and tactical levels of intelligence and some assess technical intelligence as in its own subsection. Nonetheless, tactical, and technical levels are combined as one as they share much of common ground. In the context of this study, exact definitions are not requisite. More important is their level of abstraction which ranges from general, abstract level of strategic intelligence to very specific tactical intelligence.

Strategic intelligence is a high-level information as it is used to support organisation's governance-level decision-making processes. This means that strategic intelligence is mostly consumed by C-level executives and board of directors who make long-term decisions about organisation's goals and objectives (Roberts & Brown, 2017, pp. 25). According to Bautista (2018, pp. 57) typical consumers of strategic intelligence are:

- Chief/Regional information officers
- Chief/Regional information security officers
- Vice Presidents
- Senior managers

Here the main supporting function is to help decision makers to understand current risk landscape and identify yet unknown risk (Borum et al, 2015; Tounsi & Rais, 2018). Here, intelligence is used to inform and support long-lasting decisions and policymaking processes. Heidenrich (2008) argues, that as strategy is not merely a concrete plan but a logic behind this plan. Therefore, strategic intelligence's functional use is to support the creation and implementing this plan we call "a strategy" (Heidenrich, 2008). Being very general and abstract by nature, strategic intelligence is not very technical and is provided as in a form of reports, briefings and/or conversations to inform customers (Tounsi & Rais, 2018). Like Borum et al. (2015) summarises, strategic intelligence typically supports three types of decisions:

- Advancing organisation's goals and objectives
- Gaining advantage
- Risk management across whole organisation

Commonly, strategic intelligence is covering different topics which might have an impact on organisation governing practises and long-term goals. Good examples are malware and cyberattack trends, motivations of different threat actors, and various classifications (Roberts & Brown, 2017, p. 25). Changing cyber landscape can therefore need organisation-wide changes and reviewing old processes. For instance, previously unknown attack method or advanced persistent threat (APT) targeting company's industry sector may require governance-level responses - such as inspecting company's security policies or architectural changes (Roberts & Brown, 2017, pp. 25). Therefore, strategic intelligence provides a forewarning of emerging or possible threat and a possibility to implement necessary changes which require time and resources to plan and execute.

In their paper (Borum et al., 2015) wrote that Department of Defence (DoD) states, strategic intelligence can be utilised to build better defensive architectures, improve situational awareness and understanding of the surrounding cyber domain. For strategic level executives, intelligence can offer valuable insights which can be combined with knowledge of organisation specific characteristics. As a product, there should be risk-based policies and procedures which are used to guide organisation's security posture (Bautista, 2018, p. 57). In some cases, strategic intelligence can also suggest a policy change in order to better protect the organisation (Roberts & Brown, 2017, p. 25).

Benefiting from strategic intelligence is not an easy task to the organisation. It requires knowledge about organisation's own information systems, organisational policies, and procedures. Reliable situational awareness is also significant factor. For strategic intelligence analyst, extensive knowledge of the organisation's threat landscape is crucial (Borum et al., 2015). In addition of organisational processes, highly skilled analysts are required, who can develop external relationships and gain benefit from reliable information sources (Tounsi & Rais, 2018).

From this tripartition, operational is the youngest and may be the hardest to understand. To simplify, operational ties strategic and tactical intelligence together. Compared to strategic level intelligence, operational level intelligence is more specific and focuses more on potential adversaries and their actions. Like the term suggest, according (Roberts & Brown, 2017) operational intelligence usually contains information about different campaigns, different threat actor attributes, capabilities, and perceived area of focus. It may also include higher level of TTPs (Tactics, techniques, and procedures) (Roberts & Brown, 2017, p. 24). Operational intelligence can also include information about adversaries' used attack methodology on specific targeted sector (Tounsi & Rais, 2018).

The benefits of the operational threat intelligence vary greatly depending on the usability and purpose of the intelligence collection. For example, (Tounsi & Rais, 2018) suggest that, if one vulnerability is actively exploited across industry sector, this should lead to vulnerability assessment. In his book, (Bautista, 2018, p. 60) writes that in this level of organisation, leadership is responsible for gathering and reporting different threats and vulnerabilities, enforce policies, and developing intelligence products for organisation stakeholders. To conclude, operational intelligence is mainly consumed my managerial-level personnel inside the organisation. Typical customers of operational intelligence are (Roberts & Brown, 2017, p. 24; Bautista, 2018, p. 60):

- Senior-level digital forensics
- Incident response analysts
- Security team leads
- IT service experts
- Other CTI teams

As information is more searchable than ever before, operational intelligence can be received from various sources. For example, using open-source intelligence techniques (OSINT), collection might be able to access public discussion forums where can be found information about imminent, recent, or ongoing attacks (Tounsi & Rais, 2018). Operational intelligence can also be received from organisations operating in same industry sector. Like (Skopik et al., 2016) argue, the greatest benefit of information sharing can be achieved with information exchange between same sector operatives. (Tounsi & Rais, 2018) support this viewpoint as stolen information from one organisation, can also be used against another organisation in the same sector.

As different levels of intelligence, tactical is the most pragmatic level (Roberts & Brown, 2017, p. 24) The purpose of the tactical level is support technical personnel to implement needed changes to organisation's information systems. Like (Borum et al., 2015) points out, tactical intelligence is used to support organisation's defence on its own networks. It can also be used to counter commonly known attacks adversaries use, hardening networks and blocking lists.

From this it can be concluded that tactical intelligence supports people who are in direct contact with information systems as they found tactical and technical level intelligence the most helpful to perform their daily tasks. Examples could be (Roberts & Brown, 2017, p. 24; Tounsi & Rais, 2018):

- Computer incident-response teams
- Security operations centre (SOC) analysts

Tactical level intelligence contains indicators of compromise (IoC), different threat actors' TTPs (tactics, techniques, and procedures) (Roberts & Brown, 2017). Technical intelligence takes form of different kind of threat feeds and mail lists. To generalize, technical intelligence is easily utilised, practical level of information. Technical intelligence can even be fully automated to be used in organisation's information systems. Tactical intelligence is usually delivered via various technical publications, white papers, and communication among peers (Tounsi & Rais, 2018). For technical threat intelligence, external providers offer data feeds, which help security teams to protect organisation's assets (Li, 2020, p. 18). Technical threat intelligence is far the most productised intelligence product by commercial intelligence service providers. This is because technical threat intelligence is directly actionable and the easiest to quantify (Tounsi & Rais, 2018).

Problems with technical intelligence is commonly associated with huge amount of data available. Like Tounsi and Rais (2018) mention, most of the security teams are unable to put technical intelligence in use because the data amount is overwhelmingly vast. Another problem lies in intelligence vendors unexplained collection methods and lack of accurate categorisation of different threats (Li, 2020, p. 98) This leads to situation where customers are not aware of the context and what actions should be taken according to the received data.

2.3 OODA loop

John Boyd's OODA loop is one of the commonly used decision-making models as it is used in military and business world alike. Loop have several different uses and it represents human's natural way of thinking and making decisions. Loop consists of four phases - Orient, Observe, Decide and Act - which an actor is going through during the process of decision-making. After last phase, the loop starts all over again as it is an everlasting, iterative process. In this chapter, these phases are discussed more in detail in the context of intelligence-driven cybersecurity.

2.3.1 Definition

During the Korean war (1950 - 1953) United States Airforce Colonel and military strategist John Boyd started to develop a concept to describe combat operations processes. This concept is known today as the OODA loop. Since then, OODA has been used in different contexts and applications from private business to military sector. As commonly used as it is, the basic idea is still easily describable, and uses are numerous. Commonly, OODA loop is used as make information-based decisions as a decision-making model. Loop is also considered as a learning model as every loop cycle provides feedback about actor's actions in operation environment (Gherman, 2013). Basically, we as human beings are constantly going through this loop in everyday lives whether, we realize it or not (Maccuish, 2012). The use of OODA loop is justified as this model as it is relatively widely known and used. During this paper, OODA loop is used as intelligence-driven cybersecurity usability context.

OODA loop consist of four different phases - Orient, Observe, Decide, Act - which are needed to collect needed information for the those processes and to decide and implement needed changes according the outcome (Boyd, 1995). The model's loop-like nature suggests that this is an everlasting, iterative process and there can be multiple loops going through at the same time in organisation's processes. The more commonly known and simplified version of the loop is introduced in figure 1:

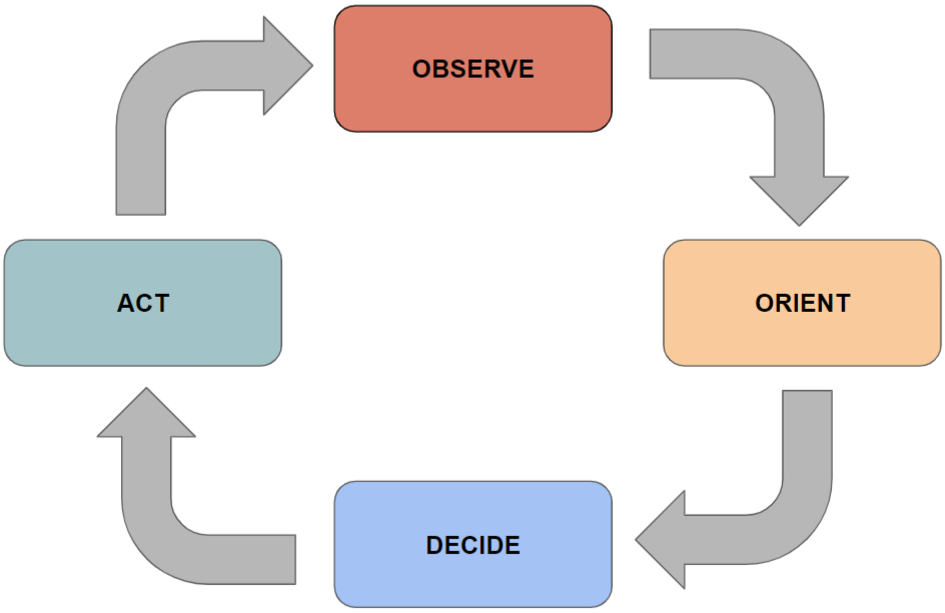

FIGURE 1 The Simplified OODA loop

This simplified presentation of the OODA loop might slightly mislead the viewer into wrong direction of thinking. Like (Maccuish, 2012) describes, if the loop is understood via simplified version, it creates an illusion that the fastest actor always wins. However, this is not the case as quality of decision and proper orienting is as important as speed. For example, if an actor is inadequately oriented, wrong decisions are made and they can even worsen the situation (Maccuish, 2012). In a context of intelligence-driven cybersecurity, the decision-maker need a precise and extensive information to be able to orient organisation's actions correctly into right direction. Speed makes no difference if orientation is wrong (Maccuish, 2012). However, if loop's time span is too slow, decisions might no longer be available or possible. Running the loop creates lag and if the lag is greater than outcome process change, the desired outcome is no longer available (Gherman, 2013).

In his summarising presentation - The Essence of Winning and Losing - Boyd (1995) represents the OODA loop which differs a simplified one as it is more detailed and consists more crucial elements. This version is introduced in figure 2 (Boyd, 1995):

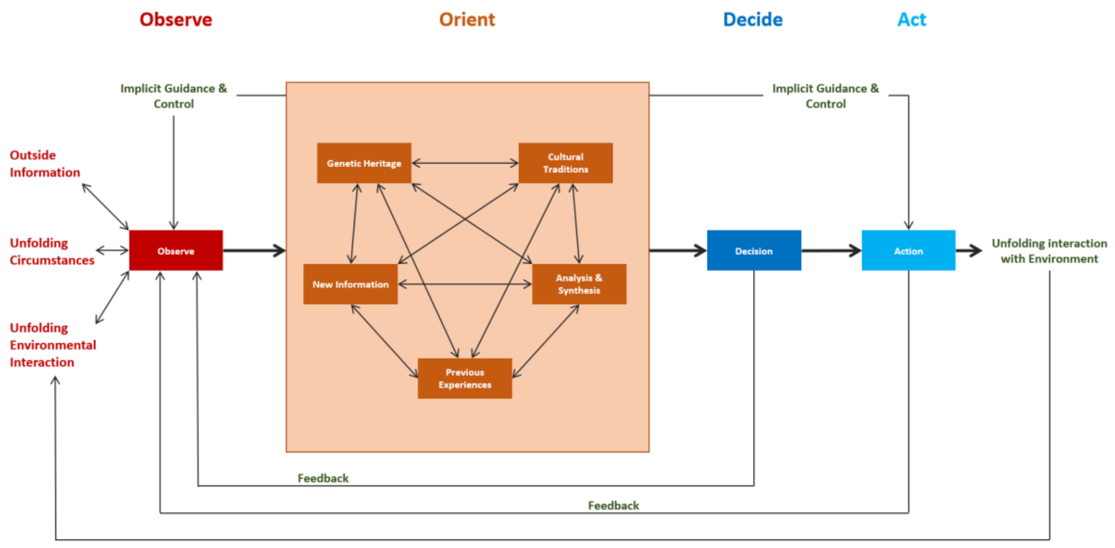

FIGURE 2 The Detailed OODA loop

For Boyd (1995), decision-making process needs to include various cross-referencing processes. These are shown are arrows for implicit guidance and control. As feedback is important to gain organisational tacit knowledge, Boyd also added a feedback mechanism which ensures process development. Also, loop's second analysing phase is pulled apart to different factors which are impacting into actor's orientation and information processing.

2.3.2 Observe

Firstly, there is the observation phase. Yet, information gathering does not end when collected information is forwarded to next phase. Collection needs to be a continuous process. To simplify, observation is about actor(s) are collecting information from surrounding environment. It can be also described as "sensing" or "information collecting". As an example, human beings and wildlife are acquiring information from their surroundings with their five senses. Organisations also have dataflows and streams of external information, which they use. Like Roberts and Brown (2017, p. 15) point out, the main purpose of this phase is to recognise useful information and collect it for later use. The motivation for observation is a concern of environmental or internal disruptions to cause harm to organisation's internal state (Hall, 2005). As observation is ongoing, organisation's perceived situational picture is affected by new information and changes in environment. Of course, in order this to be successful, organisation needs to have a strong focus on external circumstances which are changing due organisation's own or other actors' actions (Hall, 2005). It must be remembered that actor is always interacting with environment. Actor cannot be a passive observer as its own actions also make changes to situational picture. Also changes in actors' internal state is useful information as it alters organisation's balance with its surroundings. In one point-of-view, observation phase is a situational assessment (M'manga, Faily, McAlaney, Williams, Kadobayashi & Miyamoto, 2019) as organisation must be aware of the current situation and any changes that may occur. It must also be noted, that during the observation phase, there is no decisions or judgements about how collected information should be interpreted.

In cybersecurity context, observation might mean network scannings, log gathering and auditing, SIEM (Security Information and Event Management) system control, datafeeds, mailing lists, and collecting security related documents from external sources.

2.3.3 Orient

Observation phase's collected information is forwarded to the orient phase. If observation was about gathering, orient is interpreting. This is when collected information is evaluated into context with already known information (Roberts & Brown, 2017, p. 15). This process is comparison with new and information. When these two differ each other, it should create an error signal (Gherman, 2013). This error signal tells the actor that something in the current situation is changed.

During the orient phase actor is forming mental picture about the situation where is now and intended goal-state - an intentional future. Intentional future is a brainchild of actor's believed ability and opportunity to reach a goal-state by changing oneself and the surrounding environment (Philp & Martin, 2009). This goal-state concludes a deadline - a stated time limit when situation will be measured again. This is done to control the process and supervise effectiveness.

Therefore, orientation phase of the loop ends at situational picture of the current situation and desired goal-state.

Orient phase consists of five different factors which can be examined separately. All the factors influence on how an actor or organisation making constructions on ongoing events and forming choices for reaction. Next, we are going to examine these factors more closely.

New information means previously unknown information which has now made visible to the actor. It is provided by observation phase and considered important to take notice as it describes changed state in observed situation. Analysis & Synthesis refers to interpreting new, available information. Like (Boyd, 1995) states, the process of analysis and synthesis requires projection, empathy, correlation, and refection. This is a multi-sided process which needs to consider many sources of information (Boyd, 1995).

Cultural traditions indicate on organisational or personal cultures characteristics. For example, this relates to organisational cultural theories and behaviour. As culture is mostly unconscious, it still plays a major role on who we make judgements and assumptions. (Hall, 2005) also adds up organisational tacit knowledge - like organisational routines - to the cultural factors. In general, cultural factors plays a significant role on how we interpret information and make decisions (Maccuish, 2012). Previous experiences refer to individuals' professional knowledge, tacit knowledge, and available knowledge of historic events (Hall, 2005). As some part of decision-making is based on some event which has happened in the past, we might recognise similarities between historic and current situation. Generic Heritage explains the impact of our DNA and generic traits on how we interpret new information.

According to Boyd (1995), cultural traditions, generic heritage and previous experience forms a baseline of needed psychopsysical skills shaped by environments and events which are happened to us before. This human element in decision-making is crucial. Even if provided information is correct, cultural, and generic aspects can cause the result to be wrong (Maccuish, 2012).

2.3.4 Decide

When the actor has oriented itself, the next step is deciding. This phase means concrete decision-making as we are making a choice as actors between different options. Like (Hall, 2005) states, that deciding is choosing executable plan or hypothesis. This should not be confused with plan implementation as it is only deciding a course of action (Roberts & Brown, 2017, p. 15) In practice, during this phase actor analyses the difference between the reality and desired outcome and sets goals (Gherman, 2013). As different options have been recognized, actor makes a choice and moves to the next phase.

During current age of information systems and technology, there is also computer-assisted decision-making. This can be beneficial especially at complex problems where there are vast number of parameters to consider. However, this phase is only for humans as they make a final decision (Gherman, 2013).

In context of cybersecurity and cyber threat intelligence, rapid and unexpected situations may occur from collected information and are recognised to be actionable. Therefore, decision-making should be as quick as possible in order to make required changes before risk of threat realises. Implementing changes requires resources and time. Therefore, it is important to make a correct decision. When desired goal-state starts to draw closer, the more important is to correct any undesired errors and misalignments (Philp & Martin, 2009).

2.3.5 Act

After all other stages, the act stage is very straightforward. As nothing happens without action, during act phase actors puts decided option into action. Acting means assembling and executing decided response into current situation (Hall, 2005). Or as described more abstract way: acting means that actor uses available resources and tools to change reality to meet goal-state (Gherman, 2013). Even if an actor follows the chosen plan of action, this does not equal success. For this reason, OODA loop is described as an iterative as actors' own actions start to make impact on the surrounding environment, the loop cycles back to observation phase.

After the contextualised information has triggered a need and desire to change, decision-makers give orders to managers or employees who will initiate needed implementation. This can mean a new system implementation, auditing policies or guidelines or adding a new security control.

3 RESEARCH METHOD

This thesis was conducted as qualitative research. The research method employed was descriptive content analysis. This section of the thesis introduced the research method, reasons why it was chosen and known problems with qualitative research.

In addition, the data acquisition and coding process is explained in detail. The sample included 14 different documents from different sources. For coding, codes were created from the used framework – OODA loop. Specific software was used to assist the coding process.

3.1 Content analysis

This thesis is conducted as qualitative research. The research problem of this study cannot be dealt with numerically and the problem is context-specific including multiple factors. However, Cyber threat intelligence already have written documents, discussions, and other written material. For this reason, qualitative research approach was chosen to conduct this research. As stated by Conboy, Fitzgerald and Mathiassen (2012), the purpose of qualitative research is to answer research questions where the context is complex, uncertain, and multi-faceted. For this reason, qualitative research was chosen.

The research method of this thesis is descriptive content analysis. There are some known frameworks for Cyber Threat intelligence usability available. However, the purpose of this study was to create a framework based on one already known decision-making framework – OODA loop. The content analysis was chosen to create an initial framework to describe this process. For this reason, content analysis was chosen to search meaningful factors of this phenomena. According to Adams, Khan and Raeside (2014, p. 159), content analysis is used to describe the content systematically and classify the meaning that emerge from the material. Content analysis is also suitable for systematic research of electronic documents which every document in this study was (Bowen, 2009). This is why content analysis was seen as a good option for this kind of research.

The known problems of qualitative research and content analysis is estimating quality of results, repeatability, and transparency. These points are underlined by Rolfe (2006), who claims that there is no accepted consensus of standards for qualitative research. To tackle these problems, the research process will be explained as detailed as possible for this kind of research. This principle of transparency is encouraged by Flick (2008, p. 65), who asserts the transparency to be one of the essential factors for qualitative research. Also, qualitative research requires recognising biases on sampling and chosen methods (Sandelowski, 1993). The analytical process and data acquisition will be discussed in the next two chapters.

3.2 Data acquisition

The chosen sample for research for this reason was formed by publicly available documents from the Internet. As for restrictions, included documents should be available for public, be able to find by common search engines and not include any payments nor subscription. The reason for there restrictions was to exclude any commercially sold documents and case study documents from commercial cybersecurity companies. For this restriction, the goal was to not include any specific IT architecture or organisational structure to the study as purpose of the study was to be as general as possible. Another requirement was that chosen document must include information about Cyber Threat Intelligence at a general level and holistically. One of the restrictions was that searched material should be white papers and reports from different organisations. This excluded books and eBooks from the sample.

Needed documents were searched from 20th December 2020 to 10th January 2021. The search engine used was Google. To perform the search, multiple different keywords and various combinations were used. Used keywords were following:

- Cyber threat intelligence
- CTI
- Cyber security
- Process
- Communication
- Decision-making
- Decision making
- White paper
- Report

During the search process, multiple white papers and reports were found and skimmed through. Search process ended on 10th of January 2021 and 14 documents were accepted as sample for analysis phase. List of the documents is introduced in appendix 1.

The sample included documents from public and commercial actors. The oldest document was from year 2013 and latest from year 2019. The range of pages amount in documents was from 3 to 74 pages, average being ~23,7 pages.

3.3 Coding process

Coding process started with skimming every document thought once for superficial examination and gain better knowledge about the content. After skimming, every document was also read though once for better understanding. After reading process was done, the process was taken to coding phase. This reading process was described by Bowen (2009) and was necessary to gain knowledge from code acquisition.

Before beginning analysis phase, premade codes were made. Different codes of analysis were taken from OODA loops different elements presented in Library Review section. So, taken from OODA loop, code list looked like this:

- Observe
- Orient
- Decide
- Act
- Feedback
- Guidance (Implicit Guidance & Control)

In this point of analysis, it was decided that results of the coding process would be more accurate if child codes were also used in process. To achieve this, every code was given sub-codes or child codes to complement already existing codes. These child codes were created using knowledge gained from prereading of the documents. Also, for orient phase coding, elements in OODA loop were also accepted as child codes. Child codes are introduced in Results-section.

The coding process was software-assisted. The used software for coding was Dedoose 8.3.45. During the coding process every document was read through and coded for found excerpts. Every excerpt was at least one sentence long. In some cases, excerpt included few sentences. This coding approach was chosen because context of the sentence was considered very important. Also, Dedoose gave a possibility to view every excerpt in context, which was very useful during writing the results. During the process, the child codes were mainly used for coding for better categorisation. Only if, there were uncertainty of the child code but certainty of parent code, parent code was used. It must be noted that in some cases, coding was not very straight-forward. Sometimes, some excerpts were coded with more than just a single code. For example, following excerpt was coded with “Tacit knowledge” and “Previous knowledge and professional experience”-codes:

> Human analysts then apply a critical level of judgement to this filtered data to ensure the final intelligence product contains minimal false positives (Bank of England, 2016, p. 48).

After the coding process was done, the results were viewed on Dedoose software. Every code was downloaded from software in .txt form and were read again to ensure proper coding. This concluded the coding phase.

4 RESULTS

In this section, the results of research are introduced. The source material was coded with codes taken from the OODA loop and knowledge gained by reading the source material before coding process. The total sum of coded excerpts was 429. However, during analysis there were excerpts which were coded with multiple codes, so the given number do not represent unique excerpts amount. The given sum of excerpts represents all of the child codes added up to parent code's amount. The total amount of excerpts is represented in table 1:

TABLE 1 Total excerpts

CODE	N
Observe	111
Orient	51
Decide	38
Act	122
Feedback	37
Implicit Guidance & Control	70
Total	**429**

The source material was focusing heavily on observe and act phases of the OODA loop. Also, implicit guidance & control was also somewhat described in source material. Orient phase of the loop and feedback were the least described.

4.1 Observe

In observe phase, the coded excerpts distribution was uneven with used codes. Excerpts were focused under information collecting (N=69) which was expected when codes were created. Some excerpts were also found in Changes in situational picture (N=11) and External data feeds & mail list (N=10). Unsurprisingly, organisational internal data sources were the least represented in the source material. Observe phase's excerpts distribution is represented in table 2:

TABLE 2 Observe excerpts

CODE	CHILD CODE	N
Observe		1
	Changes in internal state	4
	Changes in situational picture	11
	Data from organisational security controls	8
	External data feeds & maillists	11
	Information collecting	69
	Observable assets	7
Total		**111**

Observation phase is responsible to provide data for orientation phase. This collection process has received a lot of attention from academic and professional literature. This is not in vain as high-quality data is a raw material helps analysis phase tremendously. Next, general data collection factors are introduced. In addition, collection methods and co-operation with external providers are discussed briefly. Lastly, the general factors which were found during document analysis are summed up as prevalent appearing findings.

For the observation phase, the common bedrock found during the document analysis was creating and re-evaluating organization's threat landscape profile. To create usable and efficient collection plan, cyber threat intelligence (CTI) team must have shared understanding of threats organization is facing. The profile must consist different attacker types, their modus operandi and used tools. These can be referred or summarised as TTPs (tactics, techniques, and procedures). This adversary recognition is important as it enables prioritization for data collection.

> In this context, it is equally important for organizations to understand where they fit within a given sector, supply chain, and geostrategic location in order to help identify the range of potential adversaries and how they are likely to act (INSA, 2014, p.16).

As common guideline, security team should use a broad spectrum of collection techniques to achieve deeper understanding. This is also matter of information reliability during later phases as if same information can be verified from different, independent sources, it can be considered more reliable. For these reasons, using diverse sources of data are highly advised.

During the document analysis, few nominators raised up regarding data type and content. Collected data should be relevant for organisation's cyber defence and it should be as comparable as possible. It must be acknowledged that collection phase is expensive and time consuming. As collection is takes a large part of the budget, the usability of the data can be considering a huge factor what to collect and store for later phases. Compatibility refers to different medias and mediums for collected data. Even if using different sources for data collection is recommended, paying attention on compatibility of different sources helps especially during the analysis.

> Gathering relevant information is the first step toward generating actionable intelligence. This activity represents the largest proportion of budget because of the effort and expense of collecting information from diverse sources (KPMG International, 2013, p. 12).

Documents analysed resembled about the importance of constant monitoring of the chosen data sources. Monitoring consists of many different questions to answer when planning and developing collection process. First question to answer for monitoring is matter of breadth and depth. To simplify, collection can be broad but shallow or detailed but narrow. However, these are the two extremities and there are many shades of grey between. The breadth and depth of collection should be interlocked with threat landscape profile and needed information. Secondly, monitoring frequency is another important factor for observation.

> Monitoring is a cyclic process driven by a pulse. The pulse should be sufficiently short such that the monitored entity does not deteriorate beyond correction between pulses. On the other hand it should be sufficiently long such that it does not incur unnecessary computational expense or cause undue delay (Hickman et al. (1989) according to Bank of England, 2016, p. 48).

Lastly, two different monitoring methods should be considered and selected to fit to the collection plan. The source material introduced two different types of monitoring: pull-type monitoring (e.g., periodic, analysis-driven, and event-driven monitoring) and data flow-based push-type monitoring (e.g., log data and threat feeds). These types of monitoring are part of collection strategy as they are highly dependable on security team and their assets.

For data usability point-of-view, these are decisive factors as threat data and information have always a shelf live. For these reasons, the matter of monitoring is one of the most significant aspects of useful observation and situational awareness. During constant development, security team should aim to create constant stream of data for analysis.

> If an intelligence function is stressed it may fixate on the influx of new data rather than dealing with the data, it has in hand. This can be managed by developing a 'battle rhythm' -- (Bank of England, 2016, p. 48)

To control and evaluate observation-related tasks and data flows, team should standardize the collection process. In addition, collection feed analysis should be re-evaluated constantly as if they meet the requirements set of the threat landscape profile and requests for information. As part of the collection, source material recommends establishing an internal threat intelligence library. This historical database provides context for analysis phase of intelligence process and helps to fulfil incoming intelligence requests.

There are many different sources for collected data. In the analysed source material, different sources are coarsely categorized to technical intelligence (TECHINT) and open-source intelligence (OSINT) collection methods. As this study is mainly focused on non-governmental actors and their cyber threat intelligence needs, covert collection methods typical to law enforcement or military actors are omitted.

Technical intelligence is considered as signals from hardware devices and software applications. This kind of data sources includes data from organisation's Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), honeypots, spam traps and firewalls to name a few. Basically, this categorization includes systems which are used to monitor organisation's network activity. In addition, malware signatures, registry keys and file artifacts can be considered as TECHINT. As a rule of thumb, TECHINT includes everything technology-based attack methods which security team can analyse and create useful intelligence for organisation's cyber defence and does not include any covert activity. For the same reason, Covert Human Intelligence Sources (CHIS) are not included in this study.

> Indicators such as created registry keys or file artifacts can be more useful, as they are less commonly changed by attackers (MWR, 2015, p. 36).

It must be noted that even if threat feeds from various commercial providers can help tremendously with organisation's cybersecurity, alone they are not sufficient to fulfil organisation's intelligence needs. For this reason, providing more deeper situational picture and threat landscape is advised.

> Contrary to the marketing messages of some providers, indicators of compromise are not threat intelligence, they are a component of threat intelligence but by themselves add little value. Instead, threat intelligence must contextualize IOCs for defenders as part of full-formed threat intelligence. (Dragos, 2018, p. 17)

Open-source intelligence (OSINT) have a different meaning for different people. To simplify, according to Bazzell (2018, pp. IV), OSINT can be considered as any intelligence which can be produced from publicly available information to satisfy a specific intelligence requirement. For cyber threat intelligence, renowned, OSINT-based sources are different white papers, reports, and articles. Furthermore, collecting data from social media, chat rooms and blog posts are typical form of OSINT. In this study, also different databases (e.g., Common Vulnerability and Exposures (CVE) database by MITRE), code repositories and RSS feeds are considered as OSINT-based collection.

> Start slowly – use Open Source Intelligence (OSINT) reports (and other relevant sources, e.g. reports shared by government and industry on CiSP) to refine the process of collecting, analysing and reporting intelligence relevant to your department (Gov.uk., 2019, p. 64).

During the analysis, external sources were also included to the collection process. These consists of different organisations, commercial intelligence providers and other cybersecurity-related peers of the security team. One of the obvious sources for threat intelligence are public, governmental actors such as law enforcement, government security bodies and Community Emergency Readiness Teams

(CERTs). As source material suggests, it is useful for organisation to create and maintain relationships with these kind of actors for mutual benefit. Other public organisations are also listed, such as Internet Safety Advisory Committee (ISAC), Financial Services Information Sharing and Analysis Centre (FS-ISAC) and European Network and Information Security Agency (ENISA). Other notable intelligence-based providers are proprietary cyber threat intelligence companies, Real-Time Blacklist (RBL) providers and independent cyber security labs and researchers. In addition, professional CTI networks, peers and business partners may provide valuable insight for security team as they can provide industry-specific intelligence and informal information exchange. As reference material used in this study and during the document analysis, information sharing is highly encouraged.

> Regardless of origin, sharing intelligence between peers is critical to achieving success, and we encourage all departments be actively involved in contributing to cross government threat intelligence (Gov.uk., 2019, p. 64).

Furthermore, including external providers turns out to be very useful for organisation in addition information received. This applies more to the next phases, but it is included to observation phase as this phase is responsible to provide needed information for next phases. As source material states, using external providers offers independent validation, insight and complements existing understanding for problem at hand. In addition, organisation can develop its own analytical capabilities and to mitigate analytical biases such as group think. These factors may be useful at orient phase and should be included into collection if they are considered useful.

> External intelligence can provide insight into potential threats while an organization works to adopt an intelligence driven approach and develop their own analytic capabilities (Lockheed Martin, 2015, p. 12).

To conclude the observe phase, data collection requires careful planning and constant, internal development mentality. Careful observation requires situational awareness and constant re-evaluation of data sources. As the threat landscape is the main factor which guides collection, changing circumstances and new information changes the landscape constantly. Of course, OODA loop's implicit guidance & control and feedback phases influence collection decisions and therefore organisational internal discussion and feedback mechanisms are highly encouraged. For collection, there are various data sources and methods from which to choose. The main problem is to direct collection mechanism to sources and methods which provide the most useful source for next phases for the loop and therefore the best intelligence product to the customers while carefully considering budgeting limitations. At the same time, sources must be selected carefully as too much data might cripple whole analytical process. For this reason, it is advised to start slowly and build better collection capacity as the overall process matures.

4.2 Orient

Orient phases number of excerpts was little surprising after the coding was ended. In the source material, main part of coded excerpts was at Analysis & Synthesis (N=16). The orient part of material included a lot of information about commonly known intelligence analysis and intelligence cycle, which was expected. The source material also emphasized CTI team's self-assessment and constant development of processes, which also implies strong influence of intelligence studies in general. The coded excerpts of the orient phase are introduced in table 3:

TABLE 3 Orient excerpts

CODE	CHILD CODE	N
Orient		1
	Analysis & synthesis	16
	Comparison of new and old information	4
	Evaluation process	7
	Machine learning	6
	Organisational culture	4
	Precious knowledge and professional experience	4
	Scenario analysis	6
	Tacit knowledge	3
Total		**51**

During the OODA loop's orient phase, data received from observation phase is transformed to useable intelligence for the customers. The phase includes various methods of content processing and analytical techniques. The main goal is to provide actionable intelligence to aid specific decisions, maintain situational awareness or clarify organisation's risk landscape.

> The purpose of the analysis phase is to take processed content and convert it into actionable intelligence products for consumption by the CTI function's customers and partners (Gov.uk., 2019, p. 38).

To create intelligence, raw data must be processed to find different patterns, trends, clusters, or sequences. The intelligence needed defines used techniques and methods. Analytical strategies found from source material included data-driven and hypothesis-driven which are dependent of available data and purpose of needed intelligence. Data-driven analysis is mainly performed with machines via number-crunching. For example, using artificial intelligence to find patterns or performing statistical analysis. Hypothesis-driven is performed by human analyst or analyst team.

Before performing any analysis and after new data has arrived, it needs to be rendered to remove noise – the unneeded or unnecessary data. The goal is to make needed signals easier to find. Even is data selection have been made in observation phase, source material concludes that there are still unnecessary data, which must be removed to ease the analysis. As there not a clear definition for data filtering, it can be argued that major part of needed data selection must be done in observation phase. As OODA's orient includes the *new information* component, the fine adjustments for data filtering are done in orient phase. This data processing can be performed by parsing, correlating, filtering, de-duplicating, and aggregating data.

> Before raw data can be analysed it needs to be processed to render it amenable to downstream analysis. -- This is a critical and often-overlooked step in the threat intelligence cycle. Although it is generally described as being part of the collection phase it could just as easily be said to form a bridge between collection and analysis (Bank of England, 2016, p. 20).

Data-driven analysis is machine-performed analysis method. It is mainly used huge data sets which are too vast to people to handle. As the data amount organisations are facing is increasing, this method is becoming more vital for analysis phase. Machines are especially used with technical intelligence since input data can be partially or fully automated and indicators have usually short lifespan. This leads to situation where rapid adjustments are needed for technical controls. In addition, many organisations can be use different kind of analytical tools to monitor network to seek suspicious activity. As for OODA's point-of-view, *analysis & synthesis* and *new information* components are included in data-driven analysis. Also, historical database – which was mentioned in observation phase – provides context for analysis and therefore can be considered as *previous experience* component.

Hypothesis-driven analysis is performed by analysts in the organisation's security team. Like intelligence analysis in general, cyber threat intelligence analysis requires different skills and traits for the analyst. The source material mentions intuition, curiosity, and imagination as needed characteristics for analyst. During orient phase, analysts also perform risk assessments as there is critical level of human judgement needed. Human judgement is also needed for trying to minimise false positives. In source material, it is assumed that CTI analysts work as a team or part of the team which includes professionals from different fields. With this interdisciplinary skillset, the team can provide comprehensive situational awareness when needed.

> The team consisting of multi-disciplinary skillsets across crisis management, CTI, social engineering and criminology were able to provide in-depth situational awareness during the crisis. (Deloitte, 2019, p. 7)

As it is stated in source material, one of the most important tasks of threat intelligence team is attacker attribution. For this threat actor profile, attacker's activities and modus operandi must be clarified. To identify, the attack must be traced to a single point of origin, specific actor, or organisation. The team can use models for *analysis & synthesis*. The source material gives few examples as The Diamond Model, Cyber Kill Chain® by Lockheed Martin and ATT&CK framework by

MITRE. These frameworks can be more accurate as they are based on actual adversary behaviour rather than just hypothetical thinking. As mentioned previously, CTI-team needs to create and develop their own way of working and organisational culture to perform this task. This can be seen as OODA's *cultural traditions*.

> How do we blend technical, regional (understanding of the actors and their motivation), and functional (e.g., cybersecurity or counterintelligence) expertise on motive and intent in performing cyber threat analysis (Office of the Director of National Intelligence, 2018b, p. 2)?

OODA loop includes implicit guidance and control from orient phase to observe phase. During the analysis, information gaps need to be recognized and directed to the observation phase to guide collection. Security team needs to recognise what they already know which can be seen as knowledge which already exists inside the organisation. This knowledge includes previously encountered and recognized attacks which can be found from historical database as *previous knowledge*.

Lastly, the intelligence gained through analysis and production will be given for decision makers on chosen medium of communication. The intelligence cycle calls this as dissemination. It closes the orient phase.

> Intelligence is information that has been validated and prioritized, connected to specific actors and attacks, customized for specific enterprises, and tailored for specific security consumers within the enterprise (Friedman & Bouchard, 2015, p. 38).

Orient phase includes a lot of different factors which the CTI must consider. Analytical methods vary according to the need and data available. Of course, data-driven analysis and hypothesis-driven analysis can be used in side by side. As organisation's threat landscape is constantly changing, CTI team is required to develop their ways of working to protect the organisation.

4.3 Decide

The decide phase is mainly focused on the intelligence product's medium and discussion between CTI team and the customer. The benefits of intelligence are discussed in moderate detail. Coded excerpts were mainly focused on organisational decision-making (N=17) and stakeholder interaction (N=8), which mean that the co-operation with intelligence customers is the main focus of this phase. Stakeholder interaction also implies the situational picture of the organisation's threat landscape and recommendations for actions. Also, the differences of intelligence sub-sections are noticeable. The excerpts of the decide phase are introduced in table 4:

TABLE 4 Decide excerpts

CODE	CHILD CODE	N
Decide		3
	Computer assisted decision-making	3
	Implementation plan	1
	Organisational decision-making process	17
	Roadmapping	6
	Stakeholder interaction	8
Total		**38**

Through dissemination, intelligence gained in orient phase is distributed to customers. Mainly, threat intelligence contains two different components: vulnerability analysis and description of adversary operations. In other words, intelligence is presenting threat in context. The intelligence product itself, needs to meet three different criteria: Right content, proper presentation and it is delivered at the right time. Right content means that intelligence product needs to provide sufficient understanding of the threat and the possible consequences. Presentation needs to be concise and easy to understand for target group. Intelligence does not meet its goals if it is delivered at the wrong time. This timeframe is matter of effectiveness and proactivity.

> Threat intelligence provides three critical elements: describe the threat, illustrate the impact, and recommend action (Dragos, 2018, p. 17).

The main benefits of intelligence are to provide stakeholders situational awareness and reduce uncertainties. As these uncertainties are recognised and understood, management can make decisions about countermeasures. Situational awareness includes all the needed knowledge of the organisation, partners, attack surface and threat environment. The source material stated that intelligence distribution is most efficient with constant dialogue with the management and CTI team. This can be done via daily tasking or co-ordination meetings. Through these meetings, stakeholders can gain the latest situational picture for organisational decision-making. When intelligence can advertise about potential future threats, there is a possibility for proactive changes in organisation and intelligence-lead cyberresilience.

> In law enforcement and intelligence organizations, intelligence directly informs all core business decisions. It is evident that corporate boards do not follow this approach consistently (KPMG International, 2013, p. 12).

> The key learning takeaway is to embed the use of intelligence into core business by aligning the development of intelligence products to the tempo of formal decision making (KPMG International, 2013, p. 12).

The source material states that one of the most prevalent consumers of intelligence are IT managers and Chief information security offices. As these stakeholders are gaining knowledge about new attack surfaces, adversaries, techniques, and tactics they use. This comes back to reducing uncertainty of decision-making as intelligence is a supporting function for decision-making.

> This is a highly proactive stance where the consumer's mindset moves towards 'what do I want to happen?' (Bank of England, 2016, p. 48)

Through intelligence, these stakeholders can evaluate the possible impact's effects on potential loss of revenue, impact on regulatory compliance, and ability to launch new products to organisation's customers. With this proactive stance, the organisation can make proactive changes before impactful events occur. Yet, this also requires stakeholder evaluation about offered intelligence. The stakeholders should judge the intelligence by its relevance and priority on current situation and if suggested actions are wasting expensive organisational resources. However, with vulnerability analysis, stakeholders can prioritize needed changes as they prefer.

> Consciously choosing not to take action is just as important as taking action; threat intelligence should inform both action and conscious non-action (Dragos, 2018, p. 17).

The previously emphasized constant dialogue with CTI team and stakeholders also includes CTI team's constant self-monitoring of their processes. As OODA loop describes, decision must provide feedback for observation. This means that intelligence quality and relevance must be reviewed. Feedback from stakeholders about quality, relevance and new requirements are used in next cycle. Of course, CTI team must be aware about various stakeholder groups and if they find provided intelligence useful.

> Across all departments surveyed, the distribution of CTI was noted to be critical to its usefulness. Where possible, CTI teams should maintain a view of who in their department is receiving intelligence and whether they are finding it useful (Gov.uk., 2019, p. 64).

Decision-making process is not a straight-forward task as it requires human judgement and accurate communication among various stakeholders. Intelligence can dampen uncertainties, provide insight about current threat landscape, and provide situational awareness. For decision-makers, intelligence is a supporting function for decision making as they try to develop and maintain organisation's security posture. CTI team must keep evaluating their products to develop their processes for better quality products.

4.4 Act

The act phase is highly dependable on intelligence sub-sections and the customers. The coded excerpts were somewhat more evenly distributed. Executing and implementation (N=47) was the most coded excerpt as it included every single implementation or change made in organisation. Stakeholder communication (N=30) was also heavily represented as OODA loop includes implicit guidance and control from orient phase to act phase. Excerpts for act are shown in table 5:

TABLE 5 Act excerpts

CODE	CHILD CODE	N
Act		2
	Stakeholder communication	30
	Executing & implementation	47
	Resource allocation	21
	Task allocation	22
Total		**122**

After decision-making process, organisations take needed actions towards better security posture. After the organisational decision-making process in done, the plans must be executed. This process is highly dependable on what part of organisational hierarchy the customer is and intelligence sub-section.

Strategic intelligence is a high-level information, and its consumers are mostly C-level executives, high level management and board of directors. As intelligence serves as a supporting function inside the organisation, strategic intelligence offers insight to governance-level decision making in a long-term perspective. When C-level and the board is discussing about strategic choices for the organisation, strategic intelligence provides for knowledge about threat landscape which can be used to develop long-term, risk-based strategy. At the same time, the budgeting and resource allocation can be directed to mitigate the most dangerous risks organisation is facing.

> A strategic approach to understanding your cyber threats will enable budget to be allocated and a long-term strategy developed – often at Board level (CREST, 2019, p. 24).

With clarified threat landscape and proper communication strategic intelligence is also able to assist organisation's Chief information security officer (CISO) to be informed about latest changes in threat landscape. While being informed, CISO is more able to communicate with top executives and board members and give recommendations. The value strategic intelligence gives are the current risks organisation is facing, likely development of threat landscape including adversaries and their actions and assistance for return on investment in security.

When governance-level executives are aware of current and impending threats, precautions can be made before possible incident. This proactive stance can lead to new implementation plans and policies.

> Policy guidance to protect the organization from a potential disruption hopefully leading to threat prevention (Dragos, 2018, p. 17).

Effective cybersecurity requires knowledge about organisation's own systems and as well the threat landscape. Strategic intelligence provides actual knowledge and understand about threats to governance-level consumers. As different organisations' threat landscape differs, strategic intelligence is also able to clarify which threats are current for organisation. The threats may differ from those what are hyped in the press. When threats are recognised and understood, this can be developed to risk-based decision-making.

> Threat scope and impact details supporting risk-based strategic decision-making (Dragos, 2018, p. 17).

Operational intelligence is more specific than strategic intelligence and focuses more on different adversaries and their actions. The main point of interest is different adversaries or adversary groups. This intelligence also includes threat actor's attributes, capabilities, and focus. With operational intelligence assistance, the security team can launch a vulnerability assessment if exploitation on own industry sector is detected. Operational intelligence can also give a forewarning of incoming attack. This gives a possibility to ensure organisation's defences and to monitor and evaluate attack. The gained knowledge can be used to attacker attribution for future organisation's own used and for other CTI-teams in different organisations.

> Cyber threat intelligence activities are also organized around specific adversaries, especially cybercriminals, cyber espionage agents, and hacktivists. The enterprise that knows its opponents can optimize its defenses to protect against those adversaries and the attacks they employ (Friedman & Bouchard, 2015, p. 74).

The customers for operational intelligence are mainly managerial-level personnel, incident response teams, digital forensics, and expert-level IT personnel. In some cases, even fraud detection departments may use operational intelligence as part of their operations. Here, operational intelligence provides context around the attack, event, or alert. For incident response and digital forensics this means more knowledge about complex attacks. This allows more comprehensive analysis. For IT managers, operational intelligence provides needed knowledge for different kind of gap analysis which can be used to identify gaps in defences, assessing risks and develop responsive actions.

> Cyber threat intelligence helps infrastructure groups prioritize patches based on rich information about vulnerabilities. That information can include technical descriptions of vulnerabilities and their effects, how hard they are to exploit, and whether exploit tools are currently available in the wild (Friedman & Bouchard, 2015, p. 74).

Even if operational intelligence is more high-level than technical, assisting organisation's Cyber Security Operations Centre (CSOC) can also be beneficial for security. Operational intelligence can provide context and assists on actions or escalations with observed Indicators of Compromise (IoC).

> For example, a threat intelligence service that includes a moving threat level based upon specific operational and tactical intelligence can allow the SOC to activate a heightened state of readiness (CREST, 2019, p. 24).

From this tripartition mentioned, tactical intelligence is the most pragmatic level. Tactical intelligence is used to support organisation's defence in information system level. There is also technical level of intelligence, and some scholars and professionals treat it separately from tactical intelligence. However, in this thesis, tactical and technical levels are combined as they share much of common ground.

> The aim of tactical threat intelligence is to understand how threat actors are likely to attack the organisation, and to map this understanding to the ways in which the attacks can be mitigated or detected (MWR, 2015, p. 36).

Tactical intelligence is the most utilized intelligence subsection and the main purpose of it is support organisation's CSOC operations. With tactical intelligence, CSOC can prioritise for alerts, reduce false positives, and conduct effective blacklisting.

> In addition to reports and briefings, a key part of cyber threat intelligence is delivering technical intelligence to the CSOC (Gov.uk., 2019, p. 64).

Tactical intelligence provides CSOC different kind of indicators and adversary TTPs (tactics, techniques, and procedures) to harden IT infrastructure. As threat feeds are easily automated, this can save a lot of time from CSOC personnel's daily tasks. Including to this, indicators have a limited timeframe when they are valid. Intelligence can also assist removing old ones from the blacklist that they do not block legit content in the future. Intelligence can also monitor different indicators and their occurrence. If already known indicator is still sighted, it can be still considered a threat. Email indicators can also be blacklisted to save work from CSOC personnel. To conclude above, as threat feeds allow automatic dissemination, these implementations will save a lot of work form CSOC to let them focus on more important tasks.

> If you can program a SIEM to flag high-priority alerts based on tags and enterprise-specific rules, and to quickly assemble related threat information, you will automate some of the most time-consuming tasks required of SOC analysts (Friedman & Bouchard, 2015, p 74).

The knowledge gained from tactical intelligence can also be used for technical recommendations and assisting new implementations in organisations. As CTI team is aware of how adversaries attack to the systems, they can cooperate with other IT personnel when organisation is refreshing the IT infrastructure.

> Consult architects and systems administrators to identify planned refreshes of technologies, environments, or key systems. Identify opportunities to feed tactical intelligence into these refreshes to mitigate attacks at the design and implementation phase (MWR, 2015, p. 36)

One of the tactical intelligence's tasks is also to observe vulnerabilities which are exploited in the wild. Also, code repositories provide information about exploits which are available for adversaries. This information can be compared to organisation's infrastructure. Gained knowledge is valuable when conducting patching to systems.

> Code repositories, such as exploit databases, can provide insight into which exploits are available for adoption by threat actors, and which vulnerabilities should be prioritised for patching as a result (CREST, 2019, p. 24).

From cyber threat intelligence's point-of-view, OODA loop's act includes various tasks which all are used to support organisations current cybersecurity posture. Strategic intelligence provides insight to governance-level decision making processes by maintaining accurate situational picture and enabling risk-based decision-making. Strategic intelligence also supports Chief Information Security Officer to communicate with top executives and board members with up-to-date knowledge about current threat landscape. Operation intelligence provides knowledge about threat actors and context about attack to its customers. Also, operational intelligence gives a forewarning of an attack, new adversaries in organisation's own industry sector and supports other security groups with needed knowledge. Organisation's CSOC is supported with operational and tactical intelligence with indicators of compromise and context around it. Tactical intelligence also supports CSOC operations with prioritisation of alerts, reduces false positives and blacklisting. Technical intelligence can be provided to SIEM (Security information and event management) systems via threat feeds. Tactical intelligence is also giving recommendations to other IT teams and supervises exploits enabling effective patch management.

4.5 Feedback

The feedback phase had only two child codes as they are only codes deemed necessary. Excerpts were describing OODA loop's feedback and development mechanism accurately. The main emphasis was on process development via feedback from customers and correcting possible flaws. The idea of continuous development of the process was also present. Feedback excerpts are introduced in table 6:

TABLE 6 Feedback excerpts

CODE	CHILD CODE	N
Feedback		4
	Postmortems	9
	Process evaluation & deployment	24
Total		**37**

Like any other process, intelligence also needs a way to measure success or failure. This quality management process maintains and develops quality of intelligence product via self-assessment and feedback from stakeholder groups. For usability it is necessary that threat intelligence remains a cyclic, evolutionary process with aims to continuous improvement.

> To ensure that a CTI function provides and demonstrates value to the business, it must continuously examine the quality and usefulness of its outputs. For each product type that the CTI function produces, an appropriate performance metric should be set (Gov.uk., 2019, p. 64).

To improve and find flaws in process, stakeholders' feedback is a vital part of improvement and for customer satisfaction. For this reason, the source material suggests keeping up constant dialogue with stakeholders and hold meeting where intelligence process can be discussed and evaluated. The main point is to ensure that intelligence function in organisation is understood correctly and set up objectives.

> Decision-makers need to identify what they specifically want to know and what the TI programme should be telling them. (MWR, 2015, p. 36)

If intelligence was delivered in report form, it can be evaluated many ways. Firstly, stakeholders can clarify if the report meet the original requirements. If it succeeds, more deeper requirements can be employed in the future. Failure to meet requirements detonates a flaw or failure at some point of process. Estimation can be made when comparing expected results to actual results. In this case, CTI team needs to unravel the root cause of failure and employ corrective actions.

There is always a possibility that delivered report was not used. In which case it should be clarified if intelligence was actionable, timely and included necessary contextual information for action. There is always a possibility that ignoring the report was cause by factors with are not in CTI team's control (e.g., human error or resource shortages).

> Annual threat assessments. Scoring from a templated feedback report can provide useful feedback. Key metrics to include are whether the customer found the product useful, and whether they took direct action as a result (Gov.uk., 2019, p. 64).

> Most customers are rarely satisfied with a single delivery since receiving an intelligence product usually acts as a catalyst for additional requests (Bank of England, 2016, p. 48).

In case of technical intelligence, providing feedback must be done differently. As main source of technical intelligence is various threat feeds, CTI must evaluate their usefulness and how well they perform to prevent attacks. Therefore, the evaluation must be done with other security team members who work with defensive infrastructure.

> Technical threat intelligence can be a complex endeavour – not to mention expensive, if feeds and analytical solutions are purchased commercially. It should therefore be rigorously evaluated: specifically, the number of prevented attacks that would not have been prevented by other means (MWR, 2015, p. 36).

> Enriched IOC feed to defenders. Measurement of the enriched IOC feed can be achieved by taking statistics from defensive infrastructure, such as the number of positive alerts, and the ratio of positive alerts to false positives (Gov.uk., 2019, p. 64).

For feedback process, CTI team can create own Key Performance Indicators (KPIs) for constant evaluation. Team can measure speed of delivery, volume of quality content, number of requests per year, and different statistics from various sources.

> Organisational structure aside, with regard to organisational culture, the best environment is one that encourages self-awareness, peer review and questioning of existing procedures (Bank of England, 2016, p. 48).

Feedback might be sometimes overlooked but it is necessary part to provide better quality products to CTI team's customers and achieve better security for organisation. As OODA loop states, feedback must be collected form decide and act phases of the loop to observe phase. AS OODA loop is cyclic process, every cycle gives to CTI team a change to improve their processes and quality of their products.

4.6 Implicit Guidance & Control

Implicit guidance and control were very much in line with OODA loops idea of directive mechanism of the loop. The main emphasis was at orient phase's recognized information gaps and re-directing them back to collection. Still, implicit guidance and control requires CTI team to have proper situational picture and sufficient knowledge about adversaries. In addition, guidance also must prioritize on what to collect as unneeded data can become a burden in the process. Guidance from orient phase to act phase was not directly found. However, it can be speculated that by giving recommendations for actions can be counted as guidance and control for act phase. The implicit guidance and control experts can be found in table 7:

TABLE 7 Implicit Guidance & Control excerpts

CODE	CHILD CODE	N
Guidance		0
	Behaviour analysis	2
	Focus & Scope	12
	Information from & type	24
	IoC re-evaluation	13
	RFI (Request for information)	9
	TTPs re-evaluation	3
	Task reallocation	7
Total		**70**

In OODA loop, implicit guidance & control directs the intelligence collection by giving directions to observe phase. Like mentioned in observation phase, collection is requiring resources and is expensive. That is why proper direction is necessary to direct available assets to the most important matters.

Like in feedback from customers, intelligence collection should be measured and evaluated constantly. CTI team can conduct a collection feed analysis which informs and modified collection. This also include determining the scope of collection. Collection feed analysis is based on learning about relevant threats, organisational concerns, and the needs of individual stakeholder groups. In addition, this requires knowledge and understanding of organisation's assets, system vulnerabilities, and threat landscape. When information needs are recognised and understood, resources can be allocated for collection.

> Commercial organisations, like law enforcement agencies, cannot dedicate resources to counter every threat they face. Therefore the allocation of resources to implement a threat intelligence capability should be informed by a prioritised understanding of assets, threats and vulnerabilities (Bank of England, 2016, p. 48).

Intelligence strategy guides the collection. The strategy should include the goals of intelligence function inside organisation. For strategy, CTI team should be able to issue key measures to monitor and measure performance. Key measures are also used as a tool to manage strategy. Form general strategy, CTI team is able to prioritise collection according to given requirements. Of course, collection should be based on anticipated threat level and threat landscape.

> When considering a threat intelligence strategy, a mature cyber threat assessment (TA) should be the primary guidance for departments. Foreknowledge about adversaries' tactics, techniques, and procedures (TTPs) is extremely valuable. It not only helps enterprises learn what to look for to detect attacks, it guides them on where to strengthen security technology, staffing, and processes (Gov.uk., 2019, p. 64).

During the intelligence collection and analysis, CTI should monitor threat behaviour because this may reveal more about adversaries used TTPs (tactics, techniques, and procedures) and identify collection gaps. Gaps should be recognised in orient phase and request additional material for analysis. Threat actor behaviour monitoring is beneficial for organisation also for the reason that behaviour is harder to change than single indicators. Thereby, behaviour have longer lifespan and increases robustness of detection. On the contrary, Indicators of Compromise (IoC) are much easier to modify by the threat actor, so they are not considered as reliable as behaviour in attacker attribution process.

> Threat Behavior Analytics identify system or user actions indicating suspicious or malicious activity. Like their name, they detect adversary tradecraft (i.e., behavior) rather than specific technical elements known to be bad. Threat behavior analytics have a long lifespan and are difficult for adversaries to modify, unlike IOCs which have a short lifespan and are easier for adversaries to modify (Dragos, 2018, p. 17).

> Robust behavior analytics improve detection effectiveness by orders of magnitude beyond traditional detection mechanisms (such as anti-virus) because they're neither generic like anomaly-based approaches nor static like signature-based approaches (Dragos, 2018, p. 17).

The main purpose of guidance from orient back to observe is fill up the collection gaps, request extra material and direct collection to fulfil the needs of the analysis. Success in this communication improves the quality of intelligence products and maintains CTI team's own situational awareness. It must also be notices that orient phase also guides and controls the act phase of the loop. This can be seen as recommendations for action in intelligence products. During the document analysis, no direct link about this guiding process was found. However, as intelligence offers guidance of how to improve organisation's security posture and assists in decision-making, it is relatively safe to assume this link also being present in the organisation's cyber threat intelligence operations.

4.7 The framework

After describing the results, a preliminary framework was made. Like coding, this framework is based on OODA loops and contains same elements. As one of the objectives of this thesis was to try to describe Cyber Threat Intelligence process in a concise and understandable form, a simple model was made trying to achieve this goal. Found framework is introduced in figure 3:

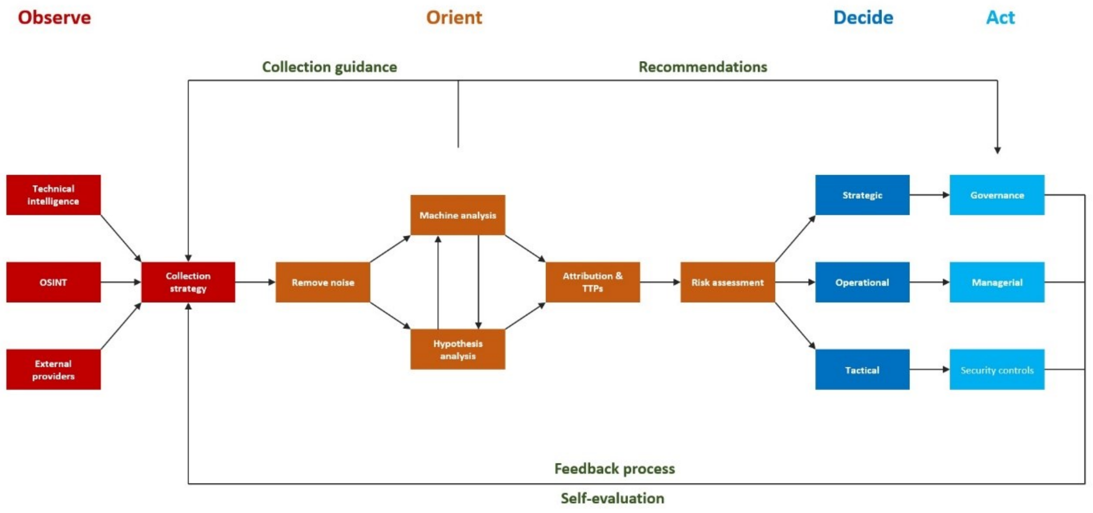

FIGURE 3 The Cyber Threat Intelligence Framework

Firstly, the framework consists three major collection sources in observe phase. These are technical intelligence, OSINT (Open Source Intelligence), and external providers. Like discussed in the observe chapter, these are the major sources for needed data.

Orient phase contains removing noise, two different analysis methods, adversary attribution and TTP. Removing noise was considered to be important because there was a strong emphasis of it and its necessity in source material. Also noise removal eases and quickens the analytical process. Machine and hypothesis analysis depict two different analysis methods which were found from source material Of course, these can be used alongside if needed to achieve the best result possible. After analysis, CTI team should have an idea of adversaries and their TTPs (tactics, techniques, and procedures). If the threat actor cannot be recognized, at least CTI team have some understanding about threats they are facing. After this, risk assessment is needed. As CTI team should be aware of the organisation's infrastructure and current threat, should be evaluated the threat, risks, and possible impact of the threat. From this evaluation, recommendations can be made.

In decide phase, intelligence products are divided according to the intelligence sub-types and customers. The gained intelligence is distributed to customers for decision-making process. Strategic intelligence for C-level executives, operational for managerial level and tactical for people responsible for technical aspects and infrastructure. Act is very straight-forward as every level in the organisational hierarchy starts to execute the decisions made in decide phase.

According to the OODA loop's feedback process, two main elements were included to this model. Constant and systematic feedback collection from customers and self-evaluation were seen as two most important elements of the feedback element of the loop. Implicit guidance and control are described by two different factors: collection guidance from orient to observe and recommendations to orient to act phase. Feedback and guidance to collection are directed to collection strategy to direct collection for the next cycle of the loop.

5 DISCUSSION AND CONCLUSION

In this section, the results of this research are introduced. Cyber threat intelligence (CTI) can provide useful assets to organization's cyber defense. Depending on intelligence subtypes, CTI can provide useable knowledge to all levels of the organizational hierarchy.

During this chapter, answers to research questions are provided. Also, discussion about limitations and suggestions about further research are introduced. As this thesis was a preliminary research to CTI usage in organizations, more research is needed to confirm the results.

5.1 Answers to research questions

In this section, answers to research questions are introduced. This thesis was conducted to answer to one research question and three sub-research questions. During the analysis and writing phase, these questions were answered. This section will go through each question and with found answers. The main research question was:

- How CTI can be used to improve organisation's cybersecurity?

As for intelligence in general, Cyber Threat Intelligence can provide time to react and prewarning for organisation. The benefit of the CTI is highly dependable on the organisational hierarchy and therefore the customer. Providing strategic intelligence for C-level executes and board of directors, CTI can effect on policy changes and long-term strategic decision in organisation. As CTI provides situational picture of threat landscape and situational awareness, this knowledge can influence on high-level decision-making in organisation. Operational CTI is able to provide context to TTPs and name potential adversaries which are capable to threaten the organisation. Organisational CTI is also supporting CSOC (Cyber Security Operations Centre) for better security. Tactical intelligence can be used to block malicious actor in beforehand and support CSOC for cutting out some of the unnecessary tasks.

Sub-research questions were the following:

- How can CTI be utilized in organisational decision making?
- How the available information should be used by the organisation in maintaining cybersecurity posture?
- How can CTI improve an organisation's cyber situational awareness?

Like intelligence in general, cyber threat intelligence is able to bring needed knowledge to decision-making. For strategic decision-making, CTI can provide insight on organisations threat landscape and situational awareness. Operational threat intelligence can provide a forewarning for impending attack, identify gaps and provide context for CSOC. Tactical threat intelligence is able to assist CSOC operations by providing needed intelligence to blocking and needed knowledge about Indicators of Compromise (IoC). Technical intelligence dissemination can be automated to lighten the workload of the CSOC personnel. In addition, tactical intelligence is able to give technical recommendations and assistance for infrastructure changes in organisation.

Using cyber threat intelligence can improve organisation's cyber security posture by observing the treat landscape and assisting in decision-making. The knowledge CTI provides can be used for implementing new security controls and making changes to processes. As CTI will provide recommendations for actions, these can turn out to be valuable to counter incoming attacks. CTI can be used to improve situational awareness to keep eye on potential adversaries and their TTPs.

5.2 Limitations

When conducting this thesis, some limitations of the study was also found. Mainly, these are concerning about research method, research, and the way this study was done. For the limitations, the results are descriptive but not completely robust.

Firstly, the process of data acquisition was done only by one researcher. Like stated in research method section, there is always a possibility of bias when selecting sample for analysis. For more reliable results, multiple researchers should be used. However, this thesis was done by only one, single researcher so using multiple researchers for document selection was not an option. Still, this can be considered one limiting factor in this thesis.

Secondly, like sample selection, coding process also was done by only one person. This means that coding process can be also biased. To avoid this, multiple persons should be used for coding to minimise bias.

Thirdly, the sample used included different documents form different sources. For this distribution, the goal was to reach some robustness for the research. When used documents from different organisation, some kind of data triangulation was achieved.

Fourthly, this research was conducted using only one research method. Methodological triangulation would provide more reliable and valid results for this kind of phenomena. However, Cyber Threat Intelligence is gaining more attention in academic research and more research is advised to gain more understand on threat intelligence usability in organisations.

Lastly, this study was conducted as qualitative research. Like stated in Research method section, qualitative research might be considered as questionable in terms of quality of given results, repeatability, and transparency. To tackle this problem, the goal was to describe the research possible as transparently as possible. However, this still leads some room for speculation about validity and reliability of the results. Again, further research is advised.

5.3 Further research

After conducting this thesis, some suggestions for further research were found. Like stated before, this was preliminary study about Cyber Threat Intelligence usability in organisations. Even if this is complex phenomena and it was contemplated only in general level, possible options for further research are advisable.

To achieve better validity and reliability, the matter of usability should be studied in context. Using case study research could bring new perspectives. In addition, further document analysis research combined with interviews can be used to bring new viewpoints and advance the framework introduced in this thesis. Also, focusing on decide and act phases of the OODA loop can brighten the organisational decision-making process using Cyber Threat Intelligence.

REFERENCES

Abu, M. S., Selamat, S. R., Ariffin, A. & Yusof, R. (2018). Cyber threat intelligence – issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), 371-379. doi:10.11591/ijeecs.v10.i1.pp371-379

Adams, J., Khan, H. T. A. & Raeside, R. 2014. *Research methods for business an social science students.* (Second edition) New Delhi: SAGE Response.

Bautista, W. (2018). *Practical cyber intelligence* (1st edition). Birmingham: PACKT Publishing.

Bazzell, M. (2018). *Open Source Intelligence Techniques*: Resources for Searching and Analyzing Online Information. Sixth Edition. ISBN-13: 978-1984201577

Bhardwaj, A. & Goundar, S. (2019). A framework for effective threat hunting. *Network Security, 2019(6),* 15-19. doi:10.1016/S1353-4858(19)30074-1

Borum, R., Felker, J., Kern, S., Dennesen, K. & Feyes, T. (2015). Strategic cyber intelligence. *Information & Computer Security, 23(3),* 317-332. doi:10.1108/ICS-09-2014-0064

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal, 9*(2), 27-40. https://doi.org/10.3316/QRJ0902027

Boyd, J. (1995). The essence of winning and losing. Retrieved from https://danford.net/boyd/essence.htm

Check Point Research. (2020). Cyber security report 2020. Retrieved from https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

Choo, K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30(8),* 719-731. doi:10.1016/j.cose.2011.08.004

Conboy, K., Fitzgerald, G. & Mathiassen, L. (2012). Qualitative methods research in information systems: Motivations, themes, and contributions. *European journal of information systems, 21*(2), 113-118. https://doi.org/10.1057/ejis.2011.57

Dalziel, H. (2015). *How to define and build an effective cyber threat intelligence capability* (First edition). Waltham, MA: Elsevier Science & Technology Books.

Eom, J. H. (2014). Roles and responsibilities of cyber intelligence for cyber operations in cyberspace. *International Journal of Security and its Applications, 8(5),* 323-332. doi:10.14257/ijsia.2014.8.5.29

Flick, U. (2007). Quality in qualitative research. In *Designing qualitative research*. SAGE Publications, Ltd, https://www-doi-org.ezproxy.jyu.fi/10.4135/9781849208826

Gherman, L. (2013). Information age view of the ooda loop. *Review of the Air Force Academy, (1),* 69-72. URL: https://search.proquest.com/docview/1370173901

Hall, W. P. (2005). Biological nature of knowledge in the learning organisation. *The Learning Organization, 12(2),* 169-188. doi:10.1108/09696470510583548

Heidenrich, J. G. (2008). The state of strategic intelligence: The intelligence community's neglect of strategic intelligence. *Studies in Intelligence, 51(2).* Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/the-state-of-strategic-intelligence.html

Hibshi, H., Breaux, T. D., Riaz, M. & Williams, L. (2016). A grounded analysis of experts' decision-making during security assessments. *Journal of Cybersecurity (Oxford), 2(2),* 147-163. doi:10.1093/cybsec/tyw010

Irwin, L. (2020). List of data breaches and cyber attacks in october 2020 – 18.4 million records breached. Retrieved December 1st 2020 from https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-october-2020

Kotenko, I. & Doynikova, E. (2014). Security evaluation for cyber situational awareness. *2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC,CSS,ICESS)*, Paris, 2014, pp. 1197-1204, doi: 10.1109/HPCC.2014.196.

Li, G. (2020). *An empirical analysis on threat intelligence: Data characteristics and real-world uses.* (Doctoral dissertation). eScholarship, University of California. Retrieved from osoitteesta https://escholarship.org/uc/item/5h9983b0

M'manga, A., Faily, S., McAlaney, J., Williams, C., Kadobayashi, Y. & Miyamoto, D. (2019). A normative decision-making model for cyber security. *Information and Computer Security, 27(5),* 636-646. doi:10.1108/ICS-01-2019-0021

Maccuish, D. A. (2012). Orientation: Key to the OODA loop--the culture factor. *Journal of Defense Resources Management*, 3(2), 67. Retrieved from https://search-proquest-com.ezproxy.jyu.fi/scholarly-journals/orientation-key-ooda-loop-culture-factor/docview/1288095343/se-2?accountid=11774

Mathews, M. L., Halvorsen, P., Joshi, A. & Finin, T. (2012). A collaborative approach to situational awareness for cybersecurity. *8th International Conference on Collaborative Computing: Networking, Applications and*

Worksharing (CollaborateCom), Pittsburgh, PA, 2012, pp. 216-222, doi: 10.4108/icst.collaboratecom.2012.250794.

Oosthoek, K. & Doerr, C. (2020). Cyber threat intelligence: A product without a process? *International Journal of Intelligence and Counterintelligence, ahead-of-print (ahead-of-print), 1-16.* doi:10.1080/08850607.2020.1780062

Philp, W. R. & Martin, C. P. (2009). A philosophical approach to time in military knowledge management. *Journal of Knowledge Management, 13(1),* 171-183. doi:10.1108/13673270910931242

Roberts, S. J. & Brown, R. (2017). *Intelligence-driven incident response* (First edition). Beijing ; Boston ; Farnham ; Sebastopol ; Tokyo: O'Reilly.

Rolfe, G. (2006). Validity, trustworthiness and rigour: Quality and the idea of qualitative research. *Journal of Advanced Nursing, 53*(3), 304-310. https://doi.org/10.1111/j.1365-2648.2006.03727.x

Safa, N. S. & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451. doi:10.1016/j.chb.2015.12.037

Sandelowski, M. (1993). Rigor or rigor mortis: The problem of rigor in qualitative research revisited. *Advances in Nursing Science, 16*(2), 1-8. https://doi.org/10.1097/00012272-199312000-00002

Saurabh, K., Baidyanath, B., Manjot, S. B. & Manoj, D. (2020). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management, ahead-of-print (ahead-of-print)* doi:10.1108/JEIM-06-2020-0240

Skopik, F., Settanni, G. & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security, 60(C),* 154-176. doi:10.1016/j.cose.2016.04.003

Stewart, J. M., Chapple, M. & Gibson, D. (2015). *CISSP (ISC)2 certified information systems security professional official study guide*. 7th edition. Sybex.

Tianfield, H. (2016). Cyber security situational awareness. *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Chengdu, 2016, pp. 782-787, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.165.

Tounsi, W. & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security, 72,* 212-233. doi:10.1016/j.cose.2017.09.001

Williamson, W. (2016). Distinguishing threat intelligence from threat data. Retrieved from https://www.securityweek.com/distinguishing-threat-intelligence-threat-data

APPENDIX 1 DOCUMENTS

Bank of England. (2016). *CBEST intelligence-led testing: Understanding cyber threat intelligence operations* (Version 2.0). [Whitepaper]. Bank of England. https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf

CREST. (2019). *What is cyber threat intelligence and how is it used?* [Whitepaper]. https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf

Deloitte. (2019). *Cyber threat intelligence: Information to insight.* [Whitepaper]. Deloitte Southeast Asia Ltd. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-jun2019.pdf

Dragos. (2018). *Industrial control threat intelligence*. [Whitepaper]. Dragos, Inc. https://www.dragos.com/wp-content/uploads/Industrial-Control-Threat-Intelligence-Whitepaper.pdf

FireEye, Inc. (2019). *Threat intelligence foundations.* [Whitepaper]. FireEye, Inc. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/intel/ds-threat-intel-foundations.pdf

Friedman, J. & Bouchard, M. (2015). *Definitive guide to cyber threat intelligence.* [Whitepaper]. Annapolis, MD: CyberEdge Group, LLC. https://cryptome.org/2015/09/cti-guide.pdf

Gov.uk. (2019). *Cyber threat intelligence in government: A guide for decision makers & analysts* (Version 2.0). [Whitepaper] https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf

INSA. (2014). *Operational cyber intelligence.* [Whitepaper]. Intelligence and National Security Alliance. https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Op_Cyber_FIN.pdf

KPMG International. (2013). *Cyber threat intelligence and the lessons from law enforcement* (Publication number: 121412). [Whitepaper]. KPMG International Cooperative. https://assets.kpmg/content/dam/kpmg/pdf/2013/02/cyber-threat-intelligence-final3.pdf

Lockheed Martin. (2015). *Seven ways to apply the cyber kill chain with a threat intelligence platform.* [Whitepaper]. Lockheed Martin Corporation. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf

MWR. (2015). *Threat intelligence: Collecting, analysing, evaluating.* [Whitepaper]. MWR InfoSecurity. https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf

Office of the Director of National Intelligence. (2018a). *Explaining the 'see it, sense it, share it, use it' approach to thinking about cyber intelligence.* [Whitepaper] https://www.hsdl.org/?view&did=819359

Office of the Director of National Intelligence. (2018b). *A guide to cyber attribution.* [Whitepaper]. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf

Webroot (2014). *Threat intelligence: What is it, and how can it protect you from today's advanced cyber-attacks?* [Whitepaper]. Webroot. https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf