Cyber Threat Intelligence: A Proposal of a Threat Intelligence Cycle from an Enterprise perspective

July 2020

2407996M

18114415

95801502

CEDRIC MELI TSOFOU

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count: 23 777

Supervisor: Eamonn Butler McIntosh

Date of Submission: 17/07/2020

Table of Contents

Chapter 1: INTRODUCTION

Over the past decade, businesses have faced a rise in cyber security attacks which has resulted in data breaches, loss of money and reputation, and altogether affected their turnover. In 2019 alone, there have been several data breaches that affected users and companies around the world. These occurred by the counts of hundreds of millions of stolen accounts representing real people and their personal information. Some incidents have been recorded in Orvibo Smart Home Records (2 billion records), TrueDialog – an American communications company (1 billion records), First American (885 million records), Two Facebook third-party apps (540 million records), MongoDB – a job search website with Chinese and Indian versions (about 500 million records), amongst others.[1] Other well-known attacks of the previous years are the Yahoo data breach of 1 billion user accounts and their passwords in 2013,[2] and the release of secret hacking tools used by the National Security Agency (NSA) in 2016 and 2017 by a notorious hacker group called Shadow Brokers.[3] Furthermore, EUROPOL Predicts more data breaches since the motive behind network intrusions – which is the most common type of cyber attacks – is the illegal acquisition of data for a variety of purposes including phishing or payment fraud.[4] Also, distributed denial of service (DDoS) attacks continue to grow as tools to launch them are easily available, allowing even unskilled individuals to launch significant DDoS attacks. In addition, an analysis of operating system-related vulnerabilities from 1st January to 31st December

[1] Maria Henriquez, "The Top 12 Data Breaches of 2019", Security Magazine, (December 2019). https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019 (Accessed: June 10, 2020)

[2] V. Goel and N. Perlroth, "Yahoo Says 1 Billion User Accounts Were Hacked," *Washington Post, 2016*. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0. (Accessed: June 10, 2020)

[3] Gibbs, S., "Shadow Brokers Threaten To Unleash More Hacking Tools." *The Guardian, (May 2017)*. https://www.theguardian.com/technology/2017/may/17/hackers-shadow-brokers-threatens-issue-more-leaks-hacking-tools-ransomware. (Accessed: June 10, 2020)

[4] European Cybercrime Centre, "Internet Organised Crime Threat Assessment", *EUROPOL, (*2018*)* p.10

2019 found out that Microsoft products – the most popular operating system in the world – has eight out of ten vulnerabilities targeted by hackers, with this tendency being true for the third time in a row.[5] Such examples are non-exhaustive and can go for a couple of paragraphs but the point is that businesses and government agencies are not getting safer online.

As one can notice, a variety of businesses have been affected; from small and medium-sized enterprises to large corporations and even governmental agencies. One might be tempted to think that large organisations and government agencies have a higher propensity to defend themselves from cyber attacks due to their financial resources however the data breach figures that were mentioned at the beginning show that both large and small organisations are targeted indiscriminately even though small enterprises suffer the repercussions a little bit more.[6] These examples of data breaches with vertiginous figures are caused by a new category of cyber threats called the advanced persistent threats (APTs).

APTs are cyber attacks launched against organisations, institutions or individuals. APTs are advanced by the fact that they are deployed by highly-skilled individuals or organisations with the necessary tactics, and resources (financial, technological). Compared to other cyber threats which attack at random and just try to maximise their victims, APTs are very structured, targeted and complex. They are termed persistent because after infection, the attacker goes undetected for as long as possible in order to infect other computers or systems in the network.[7] Indeed, most organisations are compromised without even being aware and only notice when it is too late.[8] Specifically, APTs have equally been on the rise in 2019. There has been an

[5] Kathleen Kuczma, Briana Manalo, "Criminal Underground Continues to Target Microsoft Products", *Recorded Future*, (2019).

[6] Eurostat, "Power from Statistics: data, information and knowledge", *Eurostat statistical report* (2018)

[7] James A. Lewis, ''Raising the Bar for Cybersecurity,'' *Centre for Strategic and International Studies, Washington, DC,* (2013)

[8] European Cybercrime Centre, "Internet Organised Crime Threat Assessment"

increase in compromise of supply chains especially those used to deliver BIOS and UEFI systems, a spike in disinformation especially in the Middle-East. It was equally found that established APTs actors are increasingly becoming more powerful. Finally, there has been a large number of APTs-linked data breaches especially the leak of more than 773 million emails and 21 million unique passwords which later turned out to be part of an immense collection of the credentials of 2.2 billion compromised accounts.[9]

A report published by CISCO in 2019 showed that enterprise cyber security is not always based on the amount of money allocated for it.[10] According to the report which was based on an online survey of 80 influential IT managers, what matters is that the business invests wisely on the right skills and technology that is most profitable for the protection of its critical assets. Therefore, budget matters if and only if it is invested in the appropriate way. In the same way, a research paper published by SANS institute with 326 respondents showed that 85% are already or are planning to use cyber threat intelligence.[11] However, the report does not say whether there is or they plan to use a dedicated cyber threat intelligence team inside the company. Neither does it mention how the threat intelligence is produced and used. The same CISCO report affirms that a conclusion made by 451 Research, a cyber security research company, in 2011 and 2013 which said that lots of companies suffer from the ‘security poverty line’ was still relevant in 2019. The CISCO report further asserts that an astounding 84% of respondents said they can only afford *some* of the *minimum* cyber security requirements. In view of the increase in the number and virulence of APTs in spite of the current use of cyber threat intelligence by some companies, one may suggest that the cyber threat intelligence used may not be efficient, not well applied, or

[9] David Emm, “APT Review: what the world’s threat actors got up to in 2019”, *Kaspersky*, (2019). https://securelist.com/ksb-2019-review-of-the-year/95394/ (Accessed: June 10, 2020)

[10] CISCO, “The Security Bottom Line: How much security is enough?”, October 2019. P. 3

[11] Shackleford, “Who’s using Cyber Threat Intelligence and How?” SANS Survey, no. 1, (2015). p. 26

may not even be cyber threat intelligence. This doubt may arise because cyber threat intelligence has been praised by numerous experts as *the* solution to APTs through informed decisions and the provision of actionable threat intelligence in order to understand the threat landscape, actors, and the threats specific to the business.[12][13][14] Therefore, in order to know why APTs attacks are rising we should look at what is wrong with the current cyber threat intelligence and not necessarily look at the amount of money spent towards cyber security as the CISCO report demonstrated.

Indeed, a closer look reveals that what most companies that offer cyber security services branded as threat intelligence is instead raw threat data, threat information, or just even a threat platform.[15] More often than not, these products are just untargeted streams of data from diverse news feeds which contain IP addresses, lists of compromised websites, amongst others. Most of the time, the data source is not checked for reliability and credibility therefore it could even contain false positives. Sadly, these raw data still need to be further analysed in order to establish its context, relevance and importance to the company. Moreover, an internet search of the term 'cyber threat intelligence' returns about forty-six million results including several companies that offer cyber threat intelligence services. A closer look reveals that these companies all sell different products under the same label of cyber threat intelligence. For example, Checkpoint, a company offering cyber threat intelligence, actually just sells data feeds which the customer will transform into threat intelligence by itself,[16] while Fireeye provides six intelligence

[12] Sid Snitkin, "*Critical Industries Need Active Defence and Intelligence-driven Cybersecurity*" https://dragos.com/wp-content/uploads/ARCViewDragos-01.pdf (Accessed: 30th Oct. 2019)

[13] Jorl Kalkman, Lotte Wieskamp, "Cyber Intelligence Network: A Typology", *The International Journal of Intelligence, Security, and Public Affairs, 21:1, 4-24,* (April 2019)

[14] National Cyber Security Centre (NCSC), *Annual Review 2019*, UK Government, (2019)

[15] InfoArmor, "Threat Intelligence vs. Threat Information", (2019) https://www.infosecurityeurope.com/__novadocuments/362143?v=636312780187970000 (Accessed: June 10, 2020)

[16] Checkpoint, "Threat Intelligence," (2019). https://www.checkpoint.com/products-solutions/threat-intelligence/ (Accessed: June 10, 2020)

products such as executive, fusion, operational, tactical, motivation-based, and vulnerability as cyber threat intelligence. Besides these companies are other companies like CISCO, Microsoft, Recorded Future, SANS institute, Forcepoint, amongst other, which all provide cyber threat intelligence services and have their own version of what constitutes cyber threat intelligence.

In sum, most of the times, all that clients get is a dump of data after which they are left to make their own conclusions. For example, this is akin to being told something bad will happen in the city between Monday and Thursday rather than being told a bomb will be planted at the main entrance of the train station on Tuesday between 7 am and 11 am. This then exemplifies how the latter is very actionable while the former only adds more confusion and panic, reflecting what current cyber threat intelligence is. This is not only due to the idea of cyber threat intelligence being recent but mostly because of a lack of a solid definition/understanding of what cyber threat intelligence is to both the developers and consumers of threat intelligence.[17][18] Also, there is a lack of academic literature on what exactly is cyber threat intelligence and its creation process (cycle) within the context of enterprise cyber security. Indeed, cyber intelligence or even just intelligence was seen as a military or government tool and this has brought about a lack of adequate academic literature on cyber threat intelligence in terms of enterprise cyber security.

In addition, most cyber security providing companies are for-profit hence are not willing to change their product and their ways to reflect the real security-needs of organisations – their attention is pulled in many directions. Hence, this proves the need for companies to create their own security department hosting a cyber threat intelligence team for a more original, enterprise-centric approach to cyber threat intelligence.

The end result is that companies may try to look for guidance in

[17] InfoArmor, "Threat Intelligence vs. Threat Information"

[18] Control Risks, "Cyber Threat Intelligence; Actionable insights to help you understand the cyber threat." https://www.controlrisks.com/our-services/creating-a-secure-organisation/cyber-security (Accessed: June 10, 2020)

agencies that have been practicing intelligence for years like the Central Intelligence Agency (CIA), the Mossad, the MI5/MI6, amongst others because they have been around for longer and have been subject of numerous academic and scientific research which has contributed to the amelioration of their work. One example is Robert M. Clark's book which teaches intelligence and also how to manage an intelligence organisation and its personnel.[19] Even though this brands intelligence as an established domain, it is undeniable that there is still some lack of consensus on the definition of intelligence which has a spill over effect on the intelligence creation process. However, it cannot be denied that there are at least some groups of nations, organisations or supranational organisations which share a common goal and definition of intelligence like the North Atlantic Treaty Organisation (NATO), EUROPOL, amongst others. Even such forms of consensus is lacking in the realm of cyber threat intelligence in the context of enterprise cyber security. This lack of consensus and a clear cut definition of cyber threat intelligence and its creation process in the context of enterprise cyber security has hindered collaboration and adoption of cyber threat intelligence between companies and it has even benefited attackers.[20] Therefore, there is a need for a clear and specified concept and process of cyber threat intelligence within the perspective of companies.

Before continuing, it is imperative to clarify a few concepts that will used frequently in the rest of the dissertation. Throughout this dissertation, a cyber threat will be understood as an expression of intent to do harm or imminent harm, an agent judged as harmful, and the tactics, techniques, & procedures of such agent.[21] Harm here refers to the intent or action to deprive, weaken, damage or destroy a system or network. It is important to notice that a

[19] Robert M. Clark, *Intelligence Analysis a Target Centric Approach*, (London: 4th ed. CQ Press, 2013)

[20] Hewling Moniphia, "Cyber Intelligence: A Framework for the Sharing of Data" *International Conference on Cyber Warfare and Security*, (2018)

[21] CREST "Understanding Cyber Threat Intelligence Operations", *CREST Intelligence-Led Testing, Bank of England, version 2,* (2016). P. 7

bug in a software program is not necessarily a threat but a vulnerability, the real threat is the agent that exploits this vulnerability.[22]

For the definition of the cyber space, the UK cyber security strategy defines the cyber space as;

'*An interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet and also the other information systems that support our business, infrastructure and services*'[23]

A section of the US army gives a more precise definition of the cyber space by saying that it is an interdependent network of electronic devices including the internet, telecommunication networks, computer systems, and embedded systems.[24] In order to understand this definition deeper, we need to put it into context. It is important to realise that the cyber space is a man-made dimension of war (as compared to land, air, and sea which are naturally occurring) and exists in all the other dimensions. For example, defending the airspace will also mean defending satellites, which are part of the cyber space. Defending the sea will also mean protecting sub-marine cables, which are, again, part of the cyber space.

Pertaining to intelligence, the cyber space can be seen as having 3 dimensions. A physical dimension which comprises the core physical devices that make up the cyber space like servers, satellites, computers, amongst others. An informational dimension which is the content that flows between these devices. These is also where personal identifiable information of people who are active in the cyber space resides. This dimension is important in cyber threat intelligence as it is used for attribution of actions/attacks. Finally, a cognitive dimension which comprises the beliefs, ideologies, and concepts that

[22]451 Research, 'Threat intelligence', 451 Research, LLC. (2014)

[23] Cabinet Office, 'The UK cyber security strategy: protecting and promoting the UK in a digital world'. Crown Copyright, (2011)

[24] US Army, 'Field Manual 3–38: cyber electromagnetic activities'. Department of the Army, (2014)

cyber space users adhere to.

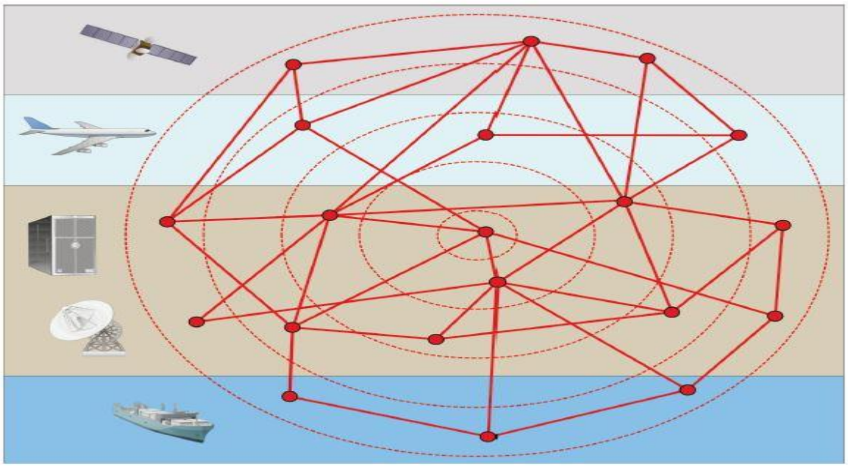


Figure 1: The cyber space.[25] The cyber space exists both in the space, air, land and sea.

This dimension reflects the societal, political and security spheres of the real world.[26] Finally, another aspect worth mentioning is that the terms business, organisation, company and enterprise will be used interchangeably throughout this paper.

The remaining parts of this paper will first start by explaining the methodology and methods used in carrying out this research and equally outline the research question and objectives. The next section will show an extensive literature review which will also highlight the themes and factors which are favourable for a cyber threat intelligence cycle within the perspective of an enterprise and a definition of cyber threat intelligence because definitions are important as they set a clear basis for analysis. Following this, a cyber threat intelligence cycle will be proposed and the ways in which it could be validated will equally be outlined. The paper will end with a conclusion and propose further research pathways.

[25] CREST "Understanding Cyber Threat Intelligence Operations" P. 8
[26] Ibid. p. 9

Chapter 2: RESEARCH DESIGN AND METHODOLOGY

The structure and organisation of the research and how the researcher thinks about the subject at hand is of utmost importance.[27] It is necessary to understand that during research, it is normal that changes be made to overcome difficulties. That is, research is everything but a smooth process.[28] Therefore whenever such circumstances arise, whatever the case be, it is always best to follow the research design that does not pose any *practical* restriction.[29] The remaining parts of this section will start by elaborating how this research accommodated the changes that came as a result of the Covid-19 pandemic. Next, the aim, objectives and research questions will be stated. The section will end by a theoretical justification of the research method chosen and how it advantages and limits the aim of the thesis, and finally explain how the method shall be applied during the research.

2.1 Aim and Objectives

Due to the Covid-19 pandemic, the original aim and objectives of this research have been altered. The Covid-19 virus brought about a lockdown imposed by the British government like in other parts of the world in order to curb the spread of the infectious virus. In the same vein, the ethics approval committee at the University of Glasgow advised against any research method that would result to a close contact – human to human contact – with the participants. Consequently, the research aims and objectives were changed because the initial methodology became incompatible with the situation created as a result of the Covid-19 pandemic.

Originally, the aim of the research was to deeply investigate just how practical it is for Small and Medium-sized Enterprises (SMEs) – given their

[27] Ragin, Charles C. *The comparative method: moving beyond qualitative and quantitative strategies,* (Berkeley (CA): University of California Press, 1987), p. 165

[28] Peter Burnham et al. *Research Methods in Politics*, (United Kingdom: MacMillan Education UK, 01 August 2008), p.39

[29] Russell L. Ackoff, *The design of social research*, (Chicago: University of Chicago Press, 1953)

large number, low resources and high vulnerability to attacks – to adapt to an intelligence driven cyber security, that is, cyber threat intelligence. The research was aimed at focusing on 3 SMEs in Greater Glasgow Area, each providing different services in order to diversify the source of data. The former research plan constituted the following objectives:

1. Find out when the SMEs started implementing cyber threat intelligence and what was their biggest challenge at that time, are they still facing the same challenges? Furthermore, understand how they are personalising their use of cyber threat intelligence.

This would have been done by collecting information from the companies through questionnaires. Note that prior to the Covid-19 situation, collecting information through questionnaires was first chosen because its ethics application is straight forward and less demanding than online surveys. Online surveys were not chosen as an alternative after the Covid-19 restrictions were imposed because they would still require that someone fills out the forms, albeit online. Online surveys would have equally required an extra 1-1.5months' time before being approved and more paperwork involved in the process.

This objective had the goal of collecting information that is specific to the practice of each SME with regards to its cyber security implementation policies. This means it had a huge weight in the dissertation and its outcome. Therefore, taking this into consideration together with the global pandemic and the mental and psychological repercussions that it can have on people which could have affected and/or influenced the ability of the participants, it was decided to switch to a full desk based secondary research.

2. The results of the first objective will serve as a substrate for the evaluation of the practical implementation of cyber threat intelligence by SMEs, its sustainability and efficiency.

This objective again highlights how central the first objective is to the whole dissertation. It further justifies why a change to a full desk based research was made. Finally, the research question tied to these objectives was: What are the implications of cyber threat intelligence on SMEs in terms of their resources and structure/organisation?

Now that we have discussed what the former aim, objectives and research question were and the circumstances that led to the change of these, we can now talk about how we arrived at our current aim, objectives and research question. For the new aim and objectives, there was a desire to still remain within the themes of cyber intelligence and SMEs. This time, firstly, cyber intelligence was restrained to a more specific type of intelligence that is employed in cyber security, that is, cyber threat intelligence. The previous aim and objectives were ambiguous on this because it sometimes stated cyber intelligence when it actually meant cyber threat intelligence. Now, it is crystal clear that we will be engaging with cyber threat intelligence. This emphasis is important because cyber intelligence is rather broad and does not say much pertaining to cyber security. It is a broad topic that one needs to dive in, explore, before extracting what is relevant to cyber security. However, cyber threat intelligence explicitly shows it focuses on threats and threat actors that helps mitigate harmful events in cyber space.[30]

Secondly, the restriction to focus on small and medium-sized enterprises have been relaxed to include enterprises, organisations, businesses, and even national and supra-national agencies that deal with cyber security and use cyber threat intelligence. This decision was taken for two reasons: The first one is because obtaining information on a company's cyber security practices is difficult and the ones that are available sometimes do not give much details. Therefore, keeping the restriction to small and medium-sized enterprises would have reduced the amount of material/literature we could have obtained to be able to make a desk based research. The second reason is

[30] CBEST, "Understanding Cyber Threat Intelligence Operations", p. 12

because we are no longer collecting data from companies through questionnaires due to the Covid-19 pandemic. Therefore maintaining this restriction would have, again, further reduced the amount of material we could have obtained to be able to make a desk based research. In addition, few of the small enterprises have cyber security policies. If they do have one, they rarely publish it online. Obtaining more information on their internal cyber security practices through questionnaires was the best method. To finish, relaxing this condition was essential so as to obtain as much as possible information on enterprises cyber security practises from a wide range. Now that these have been clarified, we can now go on and talk about the new aim and objectives of this research.

The aim of the research is to clarify the concept of cyber threat intelligence and propose a cyber threat intelligence cycle in order to help companies better understand the concept and how to apply it. The research comprises the following objectives:

1. Clarify the concept of cyber threat intelligence by providing a concise definition of cyber threat intelligence
2. Based on the first objective, propose a cyber threat intelligence cycle.

2.2 Research Question

There is need to provide clarity and stimulate innovative ideas and processes. Clarifying concepts is important as it sets the base for a strong argument and for a clear elaboration of the context.[31] To achieve that, the research will be centred on the question;

[31] As explained by the author on the importance of defining concepts. John Gerring. "Social Science Methodology: A Unified Framework", *Cambridge University Press, 2nd ed.* (2012): p. 112

How can cyber threat intelligence be defined and modelled within the context of a company?

Yet, before being able to propose a cyber threat intelligence cycle, it is important that we first understand what cyber threat intelligence means within the context of a company.

2.3 Research Design & Methodology

A research design is the set of steps needed to collect and analyse data and to transform it into information so as to effectively serve the purpose for which it was intended. A research methodology allows one to gain insight into the correlation between a research topic and the minor questions around it. A research design is the framework used to answer the questions set by the researcher through the generation and analysis of data.[32] For Hakim, research design is more about solving issues raised in political and theoretical debates.[33] Burnham et al. give a more comprehensive definition of research design by concluding that the aim is to generate new knowledge by testing, applying and refining existing theories.[34]

Academics will often classify research as either being qualitative, quantitative, or even both. While quantitative research involves quantities, numbers, and measurements, qualitative research involves descriptive data on phenomena that can be observed but not measured. Indeed, Punch reaffirms that qualitative research is essentially one in which the data are not in the form of numbers.[35]

The highest level of methodological classification or separation

[32] Bryman, Alan, & Emma Bell, *Business research methods*, (Cambridge: Oxford University Press, 2011)

[33] Hakim, Catherine, *Research design: successful designs for social and economic research*, (London: Social research today. (2nd Re). Routledge, 2000)

[34] Burnham et al. *Research Methods in Politics*, p.40

[35] Punch K. *Introduction to Social Research: Quantitative and Qualitative Approaches,* (London: Sage, 1998) p. 4

is between qualitative and quantitative methodologies. Pickard shares the same point and concludes by saying they are the only 2 basic methodologies.[36] While this is true, above these highest levels of methodological classifications is another level which is less talked about but is worth mentioning just so we can have an all-round view of the science of methodology. This level is called the metatheoretical level. Metatheory is the general higher-level assumptions, paradigms, and world views that underpin the researchers' work.[37] Qualitative methodology is often associated with an interpretivist or allied metatheoretical stance while quantitative methodology with post positivist and positivist stance.[38] Qualitative research often involves collecting lots of information but from a small sample size. It prioritises in-depth knowledge at the expense of generalisation.[39] The table below clearly summarises qualitative and quantitative research while illustrating their differences at the same time.

Characteristic	**Quantitative**	**Qualitative**
Metatheory	Positivist, Post positivist	Interpretivist
Nature of reality	Singular, stable, independent of observer; external reality	Multifarious, culturally determined, socially constructed; holistic reality
Relation of investigator to what is studied	External, observing from outside; in artificial setting	In the study setting, observing from within; in real-life setting
Relation to social phenomenon	Neutral Empirical	Engaged Normative
Research aim	Nomothetic; hypothesis testing; generalizing	Idiographic; hypothesis generating; contextualizing

[36] Alison J. Pickard, *Research methods in information,* (London: Facet Publishing, 2007), xvi

[37] Peter Johan Lor. *International and Comparative Librarianship*, (Berlin, Boston: De Gruyter Saur, 2019) Chapter 4, p. 1

[38] Hantrais Linda discusses this in her book: *International comparative research: theory, methods and practice*, (Basingstoke (England): Palgrave Macmillan, 2009)

[39] Burman et al. *Research Methods in Politics*, p.40

Strategies	Structured, theory-derived variables identified beforehand; controls; operationalization & measurement	Unstructured, open-ended, theory developed during research; concepts that are rich in meaning
Typical methods	Experiments, surveys	Participant observation, case studies
Criteria for judging research	Validity & reliability; objectivity	Credibility, transferability, dependability; authenticity

Table 1: Qualitative and quantitative analysis[40]

Therefore, in view of these, this research will be qualitative in nature for various reasons: it allows for the close involvement of the researcher into the field thereby permitting the researcher to have an insider view. This then allows for ambiguity, contradiction, and the generation of new ideas in the field that is being researched.[41] Furthermore, the goal of qualitative analysis is to understand the social reality of the subject at hand and equally seek to explain the phenomena or behaviour of the subject in their natural setting or in a particular context as outlined by the researcher.[42] This means there is no single reality of the subject at hand – its interpretation is purely subjective and exist in reference to the observer (researcher). In addition, this research does not involve any data collection in general, and numeric data in particular. Qualitative analysis therefore provides us with the necessary tools to attain our aim and objectives. Within the qualitative methodology, the comparative literature analysis method was chosen. More specifically, this thesis will use the comparative analysis method whereby selected cyber threat intelligence texts will be compared, analysed, and inferences drawn from them.

[40] Lor, *International and Comparative Librarianship*, Chapter 4, p. 7

[41] Denscombe, M. The Good Research Guide: for small-scale social research. (McGraw Hill, 2010))

[42] Saul McLeod, "Qualitative vs Quantitative Research: Simply Psychology." *Qualitative vs Quantitative Research | Simply Psychology*. https://www.simplypsychology.org/qualitative-quantitative.html. (Accessed: May 16, 2020.)

Comparative literature's name is quite self-explanatory: it is a research method that compares literary work, arguments, historical events, and theories across different time and from different authors. Also, it does not only entail comparing but also contrasting that is, it addresses both the differences and similarities found within the texts. Indeed, comparison is present in all scientific disciplines, and social sciences is not an exception. It has played an important role in the development of these disciplines. However, in the social sciences, it has not always brought about consensus on whether or not it should be treated and considered as a separate subfield of research methods. Lijphart considered the comparative method as a separate entity with its own rights,[43] Sartori later endorsed this by firmly stating that comparative politics is a "field characterised by a method".[44] This did not suffice to end the debate as Kelly et al. in their discussion saw it more as an area of content.[45] On the other hand, Ragin concluded that the comparative method indeed has its place because comparing two entities help in bringing out similarities and differences which, has helped in understanding key historical events, their processes and significance.[46] Furthermore, comparing and contrasting is not just a mechanical exercise which entails listing the similarities and then the differences. It is more about combining the similarities and difference into a coherent meaningful argument.

The act of comparing is present in our everyday lives. More often than not, we compare one thing with another in order to appreciate it more. In fact, the process of comparison is the natural function of reasons. Even great writings do not only look into their own time, but also forward and backward.

[43]Arend Lijphart. *Comparative politics and the comparative method*, (American political science review 65(3), 1971), p. 682

[44] Giovanni Sartori, "Comparing and miscomparing." *Journal of theoretical politics* 3(3), (1991): p. 243

[45] Gail P. Kelly, Altbach, Philip G., Arnove & Robert F, Comparative Education, (New York: Macmillan; London: Collier Macmillan, 1982), pp. 511-515

[46] Ragin, *The comparative method: moving beyond qualitative and quantitative strategies,* p. 6

When criticising a theory, in order to get the most out of it, it is necessary to compare it to something similar or to a benchmark. In view of this, it is just to say that the study of literature in some sense is always comparative. Before diving into how we shall use comparative literature analysis, it is important to mention the pitfalls our research method can have.

Reliability and validity are necessary conditions in social science research. However, the two measures do not always go hand in hand. Reliability does not automatically grant validity. "*A valid measure is one that is actually measuring what you think you are measuring*".[47] What then is reliability? McIntyre goes on to explain that reliability simply means giving consistent values.[48] Therefore, we must ensure that our research remains valid and reliable. Another point to watch out for is ecological fallacy. Ecological fallacy happens when someone draws conclusions about individuals based on information they have from the group these individuals belong.[49] The reverse is true for individual fallacies: making general conclusions from individual behaviours.[50] This research will be engaging cyber threat intelligence literature from all entities, that is, literature from academics, enterprises (both small and large), government agencies, and even grey literature. These categories represent all actors in the field. Therefore, this research will be free from any ecological or individual fallacy.

Generally, researchers use different methods for data collection so that one method will complement the short-comings of the other and vice versa.[51] It is true that this would have made this paper more rigorous because as we explained earlier, obtaining information on how companies use cyber threat intelligence through questionnaires was the best way to obtain first hand and more precise information. However, the use of a single method – comparative

[47] Donald McIntyre, "Bridging the gap between research and practice", *Cambridge Journal of Education*, 35:3, (2005): p. 66
[48] Ibid. p. 67
[49] Ibid. p. 42
[50] Ibid. p. 43
[51] Burman et al. *Research Methods in Politics*, p.42

literature analysis – still enables us to make sober analyses and credible conclusions, albeit not as good as if we could have been able to use questionnaires or online surveys.

Now that we have discussed the theoretical foundation of the choice of our research methodology and method, we can now go on to say how our choice of comparative literature analysis will be used in the research. We hope that through the lens of comparative literature analysis, we will challenge the stability of currently existing cyber threat intelligence cycle by a thematic analysis of various cyber security white papers and academic literature. Indeed, when looking at an object, say object A through the lens of another object, say object B (or using B as a framework to observe A), it helps in seeing A in other ways that, before the analysis, seemed perfectly understood. This method of comparative analysis is called lens comparison and is usually influenced by time: earlier events or texts help explain later ones and vice versa.

Comparative literature transcends culture, nationality, and political entities (countries). Therefore, literature – including grey literature – produced by different scholars, companies, and government agencies in the cyber threat intelligence domain can be compared irrespective of the nationality, culture, or other ideological characteristic of the author(s). Comparative literature is often understood to depict the relationship between the two texts or two the authors in one country, or between two authors in different countries in different languages. This does not pose a problem as Pennings et al. concluded that comparisons can occur across territorial space.[52] In our case, this territorial space represents different authors across different fields – that is, academics, engineers/professionals, companies, government agencies, and individuals. Therefore, this paper will apply the concepts of comparative literature analysis onto to cyber threat intelligence's literature. Another difficulty or limitation is

[52] Pennings, Paul, Keman Hans, & Kleinnijenhuis, *Doing research in political science*, (London; Thousand Oaks (CA): Sage Publications, Jan. 1999), p. 50

finding appropriate literature to compare with: sometimes the literature will treat the same topic but with different variables. Also, we will equally need to establish a basis for comparison. In our case, it represents the aim and objectives of the research.

It is important to note that the cyber security requirements for each company differs depending on specificities like the size of the company, the product and services they offer and finally the resources – financial, infrastructural – that can be moved to support it. As mentioned many times before, we will make use of comparative literature analysis for the definition of cyber threat intelligence. This will be done by using:

- Intelligence academic literature
- Grey (non-academic) literature on cyber threat intelligence, company white papers, blogs
- Attributes in a comparative analysis will be used to analyse the existing definitions of cyber threat intelligence; context and main themes/words contained within these definitions. The context and key themes will be analysed in order to decide which key themes and context a cyber threat intelligence definition must possess. The chapter will end by attempting to provide a concise definition of the term cyber threat intelligence

Use of comparative literature analysis to propose a cyber threat intelligence model

- Shall be done by analysing the failures and loopholes in the intelligence cycle in the intelligence sector and in current cyber threat intelligence models in the cyber security field. After analysing what works and what does not work in the models previously cited, we will use this knowledge to establish a cyber threat intelligence model from the perspective of a company.

In conclusion, this research has accommodated the effects of the Covid-19 by changing the research method, aim, and objectives. The research method used goes as such:

Qualitative analysis → comparative literature analysis → thematic analysis

Chapter 3: LITTERATURE REVIEW

This chapter will be in 2 parts. The first part will be dedicated to reviewing literature in order to establish a sound definition of cyber threat intelligence within the context of enterprises. The second part shall deal with reviewing literature on existing cyber threat intelligence cycles. Documents will be selected on the basis of what they have offered on the academic and professional scene that, that is, based on their relevance – how many times they have been cited or how known the author or company is in the field. Some documents may not be chosen because the content they offer might be redundant. It is important to note that throughout this chapter, only the definitions of intelligence and cyber threat intelligence within the context of the field shall be taken into account. Other forms of intelligence such as artificial intelligence, human intelligence, amongst other shall be excluded.

3.1 Literature Review for the Definition of Cyber Threat Intelligence

Making the definition of cyber threat intelligence clear does not only help in clarifying the key concepts of cyber threat intelligence itself but equally sets the scene for the proposal of a cyber threat intelligence cycle that will follow later in the paper. But before defining cyber threat intelligence, it is necessary that we first understand its parent component – intelligence – within the context of enterprise cyber security. This is so because, as it will be seen, there is no consensus on the definition of intelligence and everyone seems to define it based on the context and domain in which it will be used. To begin, definitions of intelligence from various dictionaries will be analysed. Next, we will look at intelligence from academic sources and grey literature. These will help orient on what type of definition of cyber threat intelligence we will be looking to review. Finally, we will review the definitions of cyber threat intelligence from both academic and grey literature and propose a concise definition of cyber threat intelligence from the perspective of an enterprise.

3.1.1 Intelligence in Dictionaries

A selection of the definition of intelligence from 3 of the top English language dictionaries was made. The Cambridge dictionary describes intelligence as:

'*a government department or other group that gathers information about other countries or enemies, or the information that is gathered.*'[53]

The Oxford dictionary sees intelligence in three ways:

'The collection of information of military or political value',
'People employed in the collection of military or political information' and
finally, '*Military or political information*'[54]

Lastly, the Merriam-Webster dictionary defines intelligence as two things:
'*information concerning an enemy or possible enemy or an area*', and
'*an agency engaged in obtaining such information.*'[55]

These definitions are supposed to depict what the general public thinks of intelligence and what they think it should entail. Even though there can be debates about how the definition of intelligence has come about in these dictionaries – which can influence our analysis – we shall assume that dictionaries are inherently neutral and impartial.

The contrary of this neutrality and impartiality is highlighted when

[53] Cambridge Dictionary, "*Definition of Intelligence*", https://dictionary.cambridge.org/dictionary/english/intelligence, (Accessed: May 23, 2020) Oxford dictionary, "*Definition of Intelligence*", [54] Lexcio dictionary for free English, https://www.lexico.com/definition/intelligence, (Accessed: May 23, 2020)

[55] Merriam-Webster Dictionary, "*Definition of Intelligence*", https://www.merriam-webster.com/dictionary/intelligence, (Accessed: May 23, 2020)

we study these definitions because there is a clear pattern that arises. The political and military nature is seen by the use of words like 'political', 'enemy', 'military'. There is equally a reference to geographical locations by the use of words like 'other countries', '…an area'. This is clearly a characteristic that is not present in cyber security as cyber attackers are not defined in relation to their position in the cyber space. The Structured Threat Information Expression (STIX) on this point say that physical location does not count when defining threat actors, rather tactics, techniques and procedures are what matters.[56]

In sum, definitions from dictionaries, which reflect the way in which the general public thinks of intelligence, have both a political and military connotation. They define intelligence within the context of politics, conflict, and military and highlight themes of spying, and information gathering. These cannot be taken out of their context in order to use them to define cyber threat intelligence because a definition of cyber threat intelligence within the context of enterprises should not have a military or political connotation. However, information gathering is a positive aspect.

3.1.2 Intelligence in Academic and Grey Literature

Before diving into the literature, it is essential to understand the steps intelligence has taken throughout history to become what it is today. This can give hints for a definition of intelligence and later on cyber threat intelligence.

It is difficult to say exactly how far intelligence dates back to. However, the practice of intelligence gathering and analysis is so old that it is considered the second oldest profession.[57] The oldest historical sources are sometimes considered to be in the Bible, Quran, Art of War, and Arthashastra. In the

[56] S. Barnum, "*Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIXTM)*", MITRE Corp. (July 2014): pp. 1–20

[57] Phillip, Knightley, *The Second Oldest Profession. Spies and Spying in the Twentieth Century*, (W. W. Norton & Company, 1986).

Bible, Moses sent 12 spies into Canaan based on God's advice.[58] This story is an example of intelligence requirement management – the requirements that were given by Moses to the spies. It equally exemplifies uncertainty in intelligence analysis: of the 12 spies, 10 were against an invasion and only 2 reported that it was possible to capture Jericho. Their plan was followed and Jericho was successfully captured and destroyed. This shows that the amount of information is not always important – what is important is to get the right thing. Again, the context in which this occurred was in the context of war conflict and highlights a military theme.

In the Quran, spying '*on one another'* is precluded.[59] This means that for Islamic nations, spying is only correct towards other non-Islamic nations, perhaps telling us it is not okay for allied nations and/or nations who share the same ideology and religious beliefs to spy on each other? Whatever be the case, the effect of these two instances of intelligence in the Bible and Quran is that it is being used as a moral justification of intelligence work in Western and Muslim nations. A palpable example is the CIA unofficial motto which is a passage taken from the gospel according to John '*And ye shall know the truth and the truth shall make you free'*[60]

Sun Tzu in the Art of War equally wrote on the use of spies. However, what is interesting is his mention on counterintelligence. He argued that:

- The enemy's spies who have come to spy on us must be sought out, tempted with bribes, led away and comfortably housed. Thus they will become converted spies and available for our service.
- It is through the information gotten from converted spies that we are train our local spies

[58] Read more of the story in the BIBLE, Numbers, Chapter 13-14

[59] Quran 49:12

[60] "CIA Observes 50th Anniversary of Original Headquarters Building Cornerstone Laying". *Central Intelligence Agency*, https://www.cia.gov/news-information/featured-story-archive/ohb-50th-anniversary.html (Accessed: May 24, 2020).

- It is through these converted spies that we can, again, covey false information to the enemy

Arthashastra is a management handbook that was very influential in the 12th century. In this book, Kautilya is a teacher and guardian of the Emperor. He wrote on basics of all intelligence techniques; recruitment of spies, deceits, secret diplomacy, using women in spying, interrogation, amongst other. He equally wrote on organization of intelligence; mainly use of intelligence for internal and external purposes.

Marcus Fabius Quintilianus (ca.35–ca.100) allegedly came up with the 5W or 5W1H which are; *Quis, quid, quando, uni, cur, quem ad modum (quibus adminiculis)* in Latin, which stands for Who, What, When, Where, Why, and How (by what means) in English. These represent the important questions that must be answered in intelligence.

Today and for the past decades, changes in politics, economy, science and technology has helped foster the change in intelligence organisations. In the United Kingdom (UK), intelligence has been first used in the 16th Century where Sir Francis Walsingham was a messenger and spy for the Queen. The year 1909 saw the creation of the Secret Service Bureau (SSB), 1920-Secret Intelligence Service also known as MI6, 1931-Security Service known as MI5. In 1989 the Security Service act was passed, later in 1994 the intelligence service act. In the United States of America (USA), the Naval Intelligence is the oldest continuous serving US intelligence service since March 23, 1882. Overtime, the USA's Intelligence Community has grown to 16 intelligence agencies each in charge of a specific area of security. Now that we have had a very brief review of the evolution of intelligence, we can now dive into the literature.

There is no consensus on the definition of intelligence. Intelligence is generally defined for a specific purpose and depending on a circumstance or context as well. Also, each expert tends to see intelligence through the lens of their profession. There is need for a common definition to serve as a link towards unanimity. For cyber threat intelligence, it is important because if there is cooperation and sharing of information on cyber attacks, it is important that both parties understand concepts the same way. Kent described intelligence as

'*The knowledge and foreknowledge of the world around us – the prelude to decision and action by US policymakers*'[61]

Deconstructing this definition, we can get 2 sub-definitions of intelligence from it:

- Intelligence as knowledge: as a result of the collection and analytical activity to support the decision making process of a government/official ('*knowledge and foreknowledge*')
- Intelligence as an activity: the process leading to the creation of knowledge/intelligence ('*prelude'*)

R.A Random, writing for a Central Intelligence Agency (CIA) intelligence magazine saw intelligence as

'*the official, secret collection and processing of information on foreign countries to aid in formulating and implementing foreign policy, and the conduct of covert activities abroad to facilitate the implementation of foreign policy'*[62]

This definition reveals a strong governmental scope when it says intelligence is helps in the facilitation of formulation and implementation of (foreign) policy while making reference to collection of information on foreign entities. Moreover, this definition describes the process in which governments obtain intelligence and their action on foreign territory. As such, this definition cannot be taken out of its context to help define cyber threat intelligence, just like the definitions gotten from dictionaries. The same can be said for the

[61] KENT, SHERMAN. *Strategic Intelligence for American World Policy,* (PRINCETON, NEW JERSEY: Princeton University Press, 1966) doi:10.2307/j.ctt183q0qt. (Accessed May 24, 2020)

[62] Intelligence as a Science," Studies in Intelligence", Vol. 2, No. 2 (Spring 1958): p. 76

definition from North Atlantic Treaty Organisation.

The NATO definition of intelligence says that intelligence is: '*The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.*'[63]

This definition is equally used by the UK's Ministry of defence and US' Department of Defence.[64][65] This definition in addition to having a military scope by the use of words like '*hostile forces or elements*' and '*operations*', present intelligence as the result of a process. Therefore, we can extrapolate and assert that cyber threat intelligence should equally be the result of a process/cycle. The scope of this definition equally depicts the different levels of intelligence: strategic, operational, and tactical intelligence. Strategic intelligence can be noticed by the use of words like "*the formation of policy and military plans*", which show the intention to make long-term goals, for example.

Lieutenant colonels Glass and Davidson wrote a book on military intelligence that provides some knowledge that seems to be still relevant till date despite the book being written in 1948, in full context of post-World War II. The authors claim

'*intelligence is not an academic exercise nor an end in itself*'[66]

The interesting part is '…*nor end in itself*' meaning intelligence complements the actions of another thing, which is, decision making.[67] This means cyber threat intelligence should aim at improving, supporting or accompanying

[63] NATO, "AAP-06; NATO Glossary of Terms and Definitions," *Allied Joint Publication*, (2014): p. 443

[64] US DoD, "Department of Defence Dictionary of Military and Associated Terms," *US DoD*, (June 2015): pp. 1–513

[65] UK Ministry of Defence, "Understanding and Intelligence Support to Joint Operations (JDP 2-00)," *Joint Doctrine. Publication*, (2011): p. 155

[66] Glass, Robert, Philip Davidson, *Intelligence is for Commanders*,(Harrisburg, Pennsylvania: Military Service Publishing Company), (1948): xvi

[67] Ibid

existing cyber security measures. Moreover, the book presents intelligence in principles because "*principles have a universal application*" thereby strengthening the need for a consensual definition of cyber threat intelligence, especially if such intelligence is to be shared amongst companies or agencies to help combat cyber attacks. Furthermore, the book equally shares interesting views on strategic intelligence and argue that it is the opposite of tactical intelligence. The authors go on to say that strategic intelligence is produced for the long run and in the time of peace as in time of war and must include all information on the enemy while tactical intelligence produced in the field from the moment war begins.[68] What we can learn from this is that companies should incorporate cyber threat intelligence into their cyber security and make it a habit because intelligence is for both war and peace times – a company should have cyber threat intelligence whether it undergoes cyber attacks or not.

Another theme that is constantly highlighted in intelligence definitions is that of secrecy. This view of intelligence is pervasive in dictionaries, and also shared by Mr. Random (an anonymous person who wrote for a CIA intelligence magazine) and Warner, former FBI analyst and CIA employee. Warner sees intelligence as

'*a secret, state activity to understand or influence foreign entities.*'[69]

Before talking about the 'secrecy' nature of the definition, notice how intelligence is also restricted to state/government activity that is solely performed for other foreign entities. This is certainly not right as intelligence nowadays can be carried out by any entity. Now, back to the secretive nature of intelligence definitions, notice how both definitions of R.A Random and Mr. Warner state that intelligence is a secret activity; M. Warner says intelligence a *"secret, state activity"* and R.A. Random not only argues that it

[68] Ibid, p.3

[69] Michael Warner, "Wanted: A definition of Intelligence", CIA, (April 2007) https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html#author1 (Accessed: May 26, 2020)

is "*secret collection and processing*" but also the "*conduct of covert activities abroad"*. Most companies will most probably not carry out covert actions in cyber space targeted towards another company, everything being equal. It should also be noted that, all the intelligence definitions talked of so far are somehow biased because they are influenced by the profession of their author. For example, lieutenant colonels Glass and Davidson both argued that intelligence is solely military, Random & Warner equally saw intelligence as secretive and a government activity as ex CIA employees. Organisations or government departments are also influenced by their roles when they define intelligence. All these also support the point earlier made; that each entity will define intelligence in its own way based on how it will serve its purpose and in a specific context. We should therefore strive to look for a less biased definition and looking at Mark Lowenthal seems like a good choice.

Lowenthal is expected to be less biased in his definition because despite having worked for the US Intelligence Community in the past, he has worked in several other intelligence organisations. Therefore his intelligence experience is not restrained to one single organisation and hence ideology, by ricochet. He defines intelligence as:

'*[I]nformation that meets the stated or understood needs of policy makers and has been collected, processed, and narrowed to meet those needs. Intelligence is a subset of the broader category of information. Intelligence and the entire process by which it is identified, obtained, and analysed responds to the needs of policy makers, all intelligence is information not all information is intelligence*'[70]

Intelligence is different from information because information is anything that can be known regardless of how it has been discovered. Intelligence is the subset of information, which is broader. Generally, what most companies that offer cyber threat intelligence services propose is information collection or

[70] Lowenthal, Mark, *Intelligence: from Secrets to Policy*, (Washington, D.C.: CQ Press, 4th Edition), (2009): p. 2

gathering and not intelligence. Most of it is just raw data that clients will have to analyse, contextualise, and give meaning by themselves. Lowenthal further argues that it is necessary to keep a record of threats, forces and events that might endanger the nation (in our case, the company/enterprise).[71] This is important in order to avoid surprises like in World War II where Americans were surprised by the pearl harbour attack. This is a strategic action, which should not be compared with tactical surprises which have a much bigger magnitude of effects.

We can then notice how a more generalist definition was attempted to make. Apart from the use of '*policy maker'* in Lowenthal's definition, which gives it a slightly governmental tone/scope, we can see that if '*policy maker'* is replaced with another word of choice depending on the context – in our case, customers/clients – then the definition takes on a new turn which is purely general. This then simply means intelligence is just the result of processed information delivered to meet the needs of the entity that needs it.

Finally, Lowenthal clarifies the aim of secrecy in intelligence, as used by many of the definitions previously discussed. He argues that much of what goes on in the intelligence process is secret and that:
'[...] governments seek to hide some information from other governments, which, in turn, seek to discover hidden information by means that they wish to keep secret.'[72] This gives a new aspect to intelligence as it explains that it is normal for a government/organisation to seek to hide its intelligence. Likewise, a company delivering cyber threat intelligence will not seek to reveal its methods and intelligence on adversaries or attackers as it will simply undermine all the efforts they have done so far because the attacker will be able to adjust his strategy. This will obviously be damaging as the company will need to allocate more money in cyber security in order to regain advantage.

[71] Ibid.

[72] Ibid. p. 1

To finish, now that intelligence definitions from top popular English dictionaries and from academic literature have been analysed, we can now deduce the themes that are important for a correct definition of cyber threat intelligence. The first one is the tone; all these definitions had one or multiple tones. They were either military, governmental, amongst other. Our definition of cyber threat intelligence should equally highlight a specific one. The second one is secrecy; like we have just discussed, secrecy is important as it helps to keep an edge over the opponent. Finally, all these definitions of intelligence omit counterintelligence, which is crucial to intelligence like brakes are to an automobile. Counterintelligence is an integral part of intelligence and not a separate entity that accompanies intelligence, as often thought.[73]

3.1.3 Cyber Threat Intelligence in Academic and Grey Literature

So far, we have reviewed definitions of intelligence from dictionaries, academic and grey literature with the aim of finding themes, patterns, or terms that could be relevant for a concise definition of cyber threat intelligence. It should be reminded that the global aim of section 3.1 of the literature review is not only to perform a literature review but to also come up with a concise definition of cyber threat intelligence from the perspective of an enterprise. In order to be able to finish this section of the literature review with a definition of cyber threat intelligence, it is essential that we lastly review previously proposed definitions of cyber threat intelligence in academic and grey literature.

Before starting, it is important to note that the literature on cyber threat intelligence is scarce. Most papers are on cyber intelligence. Where these papers talk about cyber intelligence we will still review them while trying as much as possible focus on the threat aspect of it. Indeed Brett et al.

[73] Martin T. Bimfort, "A Definition of Intelligence" (CIA, May 8, 2007), https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm. (Accessed: May 27, 2020)

confirmed that cyber threat intelligence is a sub-discipline of cyber intelligence because cyber threat intelligence results from other collection operations that involve other forms of intelligence collection disciplines like signal intelligence and human intelligence.[74] Then, cyber threat intelligence in conjunction with cyber counter intelligence, and the said collection disciplines altogether form cyber intelligence.

Similar to the definition of intelligence, there is no consensus on the definition of cyber threat intelligence. Again, every entity defines it based on their own context and how it will help attain their requirements thereby leaving a gap to define cyber threat intelligence within the context of an enterprise.

In 2015, a report published by the MWR, an information security company, in partnership with the Centre for the Protection of National Infrastructure (CPNI) and CERT-UK defined cyber intelligence as '*information that can aid decisions, with the aim of preventing an attack or decreasing the time taken to discover an attack. Intelligence can also be information that, instead of aiding specific decisions, helps to illuminate the risk landscape*'[75]

This definition suffers from the fact that it does not precise the domain in which threat intelligence occurs because of the lack of the word 'cyber' in it. On the other hand, it does well of endorsing that threat intelligence helps in giving more information on the threat landscape and preventing attacks. Robert M. Clark, former US army lieutenant colonel and member of the US intelligence community gives a more detailed and expanded definition by arguing that cyber intelligence is a collection discipline that does not fit in the tradition collection 'INTs'. He further argues that it is an extension of human

[74] Brett van Niekerk et al. "*An analysis of selected cyber intelligence texts*", 18th European Conference on Cyber Warfare and Security, At Coimbra, Portugal, (2019): p. 551

[75] David, Chismon & Martin Ruks, "Threat Intelligence: Collecting, Analysing, Evaluating," *MWR Infosecurity*, (2015): p. 5.

intelligence (HUMINT) because it is often an extension of the technical collection efforts carried out by HUMINT operatives.[76] This definition extends the first one by asserting that the collection of information for cyber threat intelligence can occur both in the real world – as HUMINT – and in the cyber world.

Troy Mattern et al. describe cyber threat intelligence as a tool that must be able to track the capabilities, intentions, and activities of potential adversaries and competitors as they evolve in the cyber realm.[77] They further assert that network activity is only part of what influences operations in cyberspace, and represents only one level of cyber defence and intelligence activities comes to complement/strengthen these operations. Furthermore, intelligence helps explain the behavioural dimension of cyber attacks. This definition does bring many aspects to the table: cyber intelligence is not only about getting to know attackers but also competitors. This is an important aspect for enterprises as they always have competitors whom they seek to know more about whether they suspect their competitors of cyber attacks or not. Another interesting aspect of this definition is that it argues cyber intelligence equally tracks the intentions of the attacker. Troy Mattern et al. expand on this and say that behind every computer/machine that is used to perform a cyber-attack, there is a human being and cyber intelligence should be able to undercover his/her motives and intentions.[78] Mark Lowenthal with regards to this asserts that traditional human intelligence collections are still very much valued in the intelligence community and are capable of tilting the balance of power.[79] Cyber-HUMINT is the term used to describe this aspect of cyber threat intelligence. Robert Steele, a former US intelligence officer wrote that cyber-HUMINT includes the use of traditional HUMINT such as agent

[76] Robert M. Clark. "Intelligence Collection". Washington D.C.: CQ Press, (2014): p 121

[77]Troy Mattern , John Felker , Randy Borum & George Bamford, "Operational Levels of Cyber Intelligence" *International Journal of Intelligence and CounterIntelligence*, 27:4, (2014): p. 704

[78] Ibid.

[79] Lowenthal, *Intelligence: from Secrets to Policy*

recruitment, information gathering through deception, together with deception *technologies* like social engineering.[80] This then confirms that cyber threat intelligence can involve intelligence collection both in the real world and in the cyber realm. Brett et al. also claim that, depending on the intended activities, the sources of cyber threat intelligence may differ.[81]

Other definitions of cyber intelligence and cyber threat intelligence from other authors more or less revolve around the definitions previously reviewed but still fail to define cyber threat intelligence within the context of an enterprise. Eric M. Hutchins et al. similarly to Troy et al. argue that cyber threat intelligence should be able to analyse adversaries' objective, capabilities and even doctrine.[82] They further ague that attackers behaviours should not be regarded as single isolated actions, but as a chain of actions and progressions.[83] Katie Nickels from SANS institute sees cyber threat intelligence as analysed information about the hostile intent of an attacker, with emphasis on the human aspect of the threat. However she fails to clarify what hostile intent may be.[84] Katie equally makes reference to the cyber kill chain. Several other papers mention the kill chain or at least make reference to it in their discussion on cyber threat intelligence.[85][86][87][88] Thereby highlighting its importance as a tool in cyber threat intelligence.

[80] Robert Steele, "Human Intelligence(HUMINT): All Humans, All minds, All the Time", Strategic studies institute, June 2010, https://phibetaiota.net/2011/11/reference-human-intelligence-humint-all-humans-all-minds-all-the-time-full-text-online-for-google-translate/ (Accessed: May 28th, 2020)

[81] Brett van Niekerk et al. "An analysis of selected cyber intelligence texts"

[82] Hutchins Eric et al. "*Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*", *Lockheed Martin Cooperation*, (2011): p. 3

[83] Ibid.

[84] Katie Nickels, "The Cycle of Cyber Threat Intelligence", *SANS Institute*, (2019): p. 16

[85] Edilson Arenas, "Cyber Threat Intelligence Information Sharing", *Conference Paper, Central Queensland University*, (2017)

[86] Wiem Tounsi, "What is Cyber Threat Intelligence and How is it Evolving?", *Institut Mines-Telecom*, (April 2019): p. 5

[87] Brian H. Nussbaum, "Communicating Cyber Intelligence to Non-Technical Customers?", *International Journal of Intelligence and CounterIntelligence, 30:4,* (2017): p. 754

[88] Sara Qamar et al. "Data-driven analytics for cyber threat Intelligence", *Elsevier*, (2017)

Defining Cyber Threat Intelligence

Now all reviews of definitions in all three domains; dictionaries, intelligence, and cyber threat intelligence has been done, a definition of cyber threat intelligence can now be made within the context of an enterprise. It was argued that a good definition of cyber threat intelligence within the context of enterprises should fulfil the following:

- Contain (cyber) counterintelligence
- A cyber threat intelligence report should answer the 5W1H questions – Who, What, When, Where, Why, and How (by what means)
- Intelligence is not an end in itself hence it should provide foreknowledge and knowledge for decision making. Intelligence should prevent attacks, illuminate threat landscape and may or may not be a secret activity.
- Should not be plain information but contextualised information
- Collection of information can occur both in cyber and real world, that is, collection of network activity as well as human activity/behaviour. Cyber threat intelligence should track intentions, behaviours for adversaries as well as competitors.
- Have a neutral scope and not a military or a governmental scope.

In view of these, this thesis proposes the following definition for cyber threat intelligence within the context of an enterprise:
The result of a process that involves information collection either in the real word or cyber realm or both in order to provide foreknowledge, knowledge and counterintelligence on the threat landscape, the intentions and behaviours of the attacker or a competitor, and support the cyber security decision making of an enterprise.

This definition will help in setting the scene and as well serve as a solid foundation for a cyber threat intelligence cycle within the perspective of an enterprise. However, before proposing a cyber threat intelligence cycle, it is essential we start by reviewing the literature on the previous ones in order to further understand what the current debate is and what is lacking.

3.2 Cyber Threat Intelligence Cycle Literature Review

While a definition of cyber threat intelligence tries to explain a phenomenon, a model describes/defines a process. The main objective of this section is to review the literature on classic intelligence cycle models from academic literature and cyber threat intelligence cycles from grey literature. As it will be seen, all existing cyber threat intelligence cycles are based on the classic intelligence cycle. Due to this strong dependence, both literature on the intelligence cycle and the cyber threat intelligence cycle will be reviewed. The end of this section will single out some requirements needed for an efficient cyber threat intelligence cycle within the context of an enterprise which will later be used in the next chapter to propose a cyber threat intelligence cycle.

The intelligence cycle or process is the logical and sequential process of gathering information on a required subject of interest (opponent, adversary and the operating environment, business competitor amongst other), and turning it into useful intelligence. Finally, this product is provided to those who need it. Simply put, it is the process or cycle through which raw data is transformed into meaningful contextualised information.

Davydoff, manager of global security at AT-RISK, a cyber security company active since 2003, wrote a paper which argues that there is necessity to re-invent the cyber threat intelligence cycle in the private sector. This is because just like any set of guidelines, the cyber threat intelligence cycle needs to be regularly updated in order to adapt to clients' new requirements, new consumers, and limited resources.[89] This is also because the private sector faces different kinds of struggles during each phase of the

[89] Daniil Davydoff, "Rethinking the Intelligence Cycle", *ASIS International*, (2017): p. 1

intelligence cycle because of some inherent difference between the public and private sector. These challenges are:[90]

- The wider variety of hierarchies and reporting line types in corporate intelligence
- Different rates and priorities concerning technology implementation
- Higher variation in workplaces
- Widely different organizational goals
- Potentially faster rates of change, growth, and organizational restructuring
- Limited resources for security in relation to other institutional focus areas

Using a 5-phase cyber threat intelligence cycle, the paper further identifies some deficiencies in each phase of these cycles. In the first phase, planning & direction, enterprises face the challenge that their customers have very basic knowledge of threat intelligence hence cannot clearly formulate their requirements. The burden then rests on the intelligence analysts. As for collection, intelligence analyst in an enterprise need to be more versatile because budget constraints usually impose fewer staffs in the cyber security departments thereby forcing analysts to be apt in a multitude of intelligence collection disciplines like HUMINT or signal intelligence (SIGNINT) as compared to government intelligence services who have the luxury to recruit analysts who are highly specialised. Davydoff further notes that intelligence analysts have a much larger and diverse area to cover thereby putting them under more stress. In one day, the analysts could jump from political risk in Africa to arms control in America, to intellectual risk in Asia, this on top of dealing with checking the reliability of sources. In dissemination, the main challenge here lies in explaining intelligence in layman's terms to clients who have very little to zero knowledge of intelligence reports. The same could be

[90] Ibid. P. 2

said for policy makers in the government but at least they are used to listening/reading to intelligence reports. Finally, Davydoff heavily criticises the fact that in the evaluation and feedback phase, customers do not give feedback unless something bad comes up.

However, above all, Davydoff argues that this is not a call for changing the entire cycle but looking closely at what does not work and make appropriate changes. Further looking deeper into why enterprises' cyber threat intelligence do worse compared to governments', he asserts that: '*...government institutions are committed to the safety and security of citizens at virtually any cost, the core objectives of businesses revolve around profit'*[91] and urges that cyber threat intelligence ceases to be seen as a burden – that is, a department where money is just spent – but instead as something that can create value.

Zane Pokorny wrote for Recorded Future, a company that provides threat intelligence in order to amplify security programs. Pokorny proposes a 6-phase cyber threat intelligence cycle.

[91] Ibid. p. 5

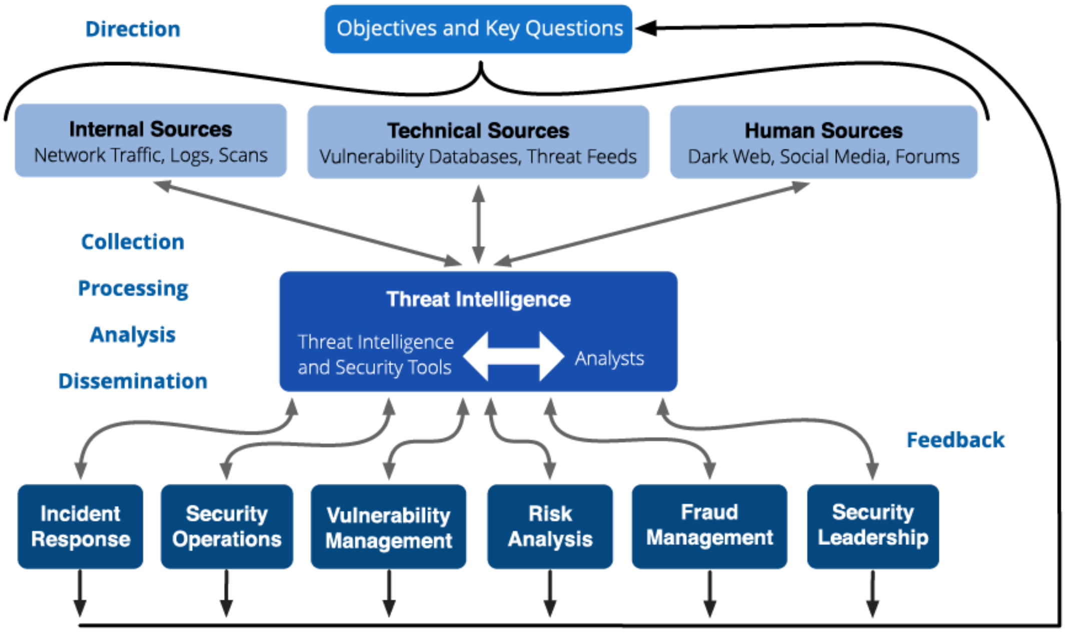


Figure 2: Cyber threat intelligence cycle, Recorded Future. [92]

When talking about intelligence requirements and directions, Pokorny took the example of an intelligence requirement to understand adversaries. This further confirms that the enterprise/business nature of cyber threat intelligence is not necessarily directed towards cyber attackers but also towards company rivals/adversaries as it was mentioned in the definition that this thesis proposed for cyber threat intelligence.

As it can be seen from the diagram, collection can involve both finished intelligence reports in combination with other raw information. These sources can be technical sources, media, social media, forums, and dark web. Pokorny further argues that intelligence analysts should spend as less time as possible in collecting information and instead automate the collection, and as much time as possible in analysing and dissemination but does not really say

[92] Zane Pokorny, *The Threat Intelligence Handbook*, Annapolis: CyberEdge Group, LLC, (2019): p. 14 https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/ (Accessed: May 31st, 2020)

why.[93] However, this again exemplifies the burden that intelligence analysts face in the private sector, as earlier argued by Davydoff. According to Pokorny, in the intelligence cycle, processing could be carried out by humans or machines and analysts must have a clear understanding of who is going to use their intelligence in the dissemination. Also, analysts should articulate in business terms and avoid overly technical jargon. Finally, because the feedback guides all phases of the intelligence cycle, it makes it vital.[94]

More recently in April 2020, the Royal United Services Institute for Defence and Security Studies (RUSI), published a paper that was aimed at studying the impact artificial intelligence would have on the UK's national cyber security as recommended by the Government Communications Headquarters (GCHQ). RUSI is the world oldest and the UK's leading defence and security think tank. The researchers found out that artificial intelligence would be of great help in cyber security in the detection of abnormal traffic, malicious software, and respond to attacks in real time. More importantly, the researchers argued that artificial intelligence could also help in intelligence analysis by the use of 'Augmented Intelligence' (AuI), a system which could be used to support human analysis. AuI could also help in intelligence collection by filtering and triage of the material collected in bulk. This provides a good solution to Zach Pokorny who encouraged the automation of intelligence collection. In addition, the RUSI researchers also found out that AuI could help in natural language processing and audio-visual analysis, and in behavioural analytics, all of which are key to cyber threat intelligence. However, the researchers assert that none of the artificial intelligence or AuI methods can replace human judgement arguing that any artificial intelligence that is designed to mimic human behaviour is of limited value. Nevertheless, they credit that AuI systems are of vital help in collecting information from multiple sources and should flag items for human review which will increase

[93] Ibid. p. 15
[94] Ibid. p. 19

the efficiency of AuI.[95] The researchers equally warn that all these artificial intelligence innovations may be used by state and non-state actors with malicious intent and may pose digital (use of polymorphic malware), political (use of 'deep fake' to generate synthetic media), and physical (IoT, autonomous vehicles) security risks.[96]

Katie Nickels working for SANS institute, writes on a cyber threat intelligence cycle similar to that of the intelligence cycle but without a feedback phase. The phases consist of: planning & direction, collection, processing & exploitation, analysis & production, dissemination. According to Katie, an intelligence team in an enterprise should be made up of the security operations centre, incidence response, system engineering and IT, business operations, and vulnerability management.[97] The planning and directions should be understood as seeking to fill and 'intelligence gap'. In short, intelligence requirements are there to prevent the analysts from defining the problem and solving it again himself. This goes in conjunction with Davydoff's point on the lack of knowledge of intelligence with customers.

Nickels further recommends to group the requirements on strategic, operational or tactical requirements. Key collection sources are internal and external data such as intrusion analysis, malware, domains, external datasets, TLS (transport later security) certificates. However, Nickels recognises that what most companies have historically been providing is malware report and not threat intelligence.[98] As for analysis, most data analysis models rest on putting data into buckets which helps in identification of patterns. However, the analyst must always beware of biases, especially confirmation bias, Nickel argues. Structured analytic techniques such as red teaming helps in reducing this. In dissemination, Nickel asserts that knowing your audience is key in

[95] Alexander Babuta, Marion Oswald, and Ardi Janjeva, "Artificial Intelligence and UK National Security", *Royal United Services Institute for Defence and Security Studies (RUSI)*, (April 2020): p. vii
[96] Ibid. p. viii
[97] Nickels, "The Cycle of Cyber Threat Intelligence", p. 8
[98] Ibid. p. 18

delivering an impactful report. Different cultures and different professions require intelligence reports in different formats.[99] In conclusion, this cyber threat intelligence cycle is very close to that of the traditional intelligence cycle, it even recommends the BLUF format when writing cyber threat intelligence reports.

Indeed, the classic intelligence cycle has 4-6 phases. However despite the difference in phases, the principles behind it remains the same. Michael Warner at the CIA made a research on the origins of the intelligence cycle and makes reference to a document written by Clausewitz, a Prussian general.[100] This document rather gives the first mention of the word intelligence. In order to uncover the origins of the intelligence cycle, Warner focuses on the research done by Kristan Wheaton and finds that the word ‘intelligence cycle’ was first used in the book written by lieutenant colonels Glass and Davidson.[101] According to Wheaton’s research, the intelligence cycle proposed by Glass and Davidson consisted of 4 phases; direction of collection effort, collection, processing, consumption. However the same research showed that the model used by Glass and Davidson in their book was already taught to officers during the Second World War. Another researcher on the origin of the classic intelligence cycle is Dr. J. Richards who found a connection in one of the documents issued by the US government.[102] In another document Dr. Richard asserts that the intelligence cycle is a process that is made up of collection, processing, analysis and dissemination for policy makers or ‘intelligence customer’.[103] Whatever be the case, the intelligence cycle has become the ultimate tool in explaining the process of intelligence

[99] Ibid. p. 43

[100] M. Warner, “The past and future of the Intelligence Cycle,” in *Understanding the Intelligence Cycle*, 1st ed., M. Pythian, Ed. Oxfordshire: Routledge, 2013, p. 160.

[101] Glass, *Intelligence is for Commanders,* p. 160

[102] N. Quarmby and L. J. Young, *Managing Intelligence: The Art of Influence*, (Federation Press, 2010)

[103] J. Richards, “Pedalling hard,” in Understanding the Intelligence Cycle, 1st ed., M. Pythian, Ed. Oxfordshire: Routledge, 2013, p. 160

creation. It has become so trusted that some authors even affirm that it has become a theological concept whose validity is never questioned.[104]

Each model starts off with a phase that describes the problem that is being solved. Next, the analyst determines which data to be collected and roles are allocated. This represents a single step in the 4 and 5 phase models and 2 different steps on the 6-phase model.

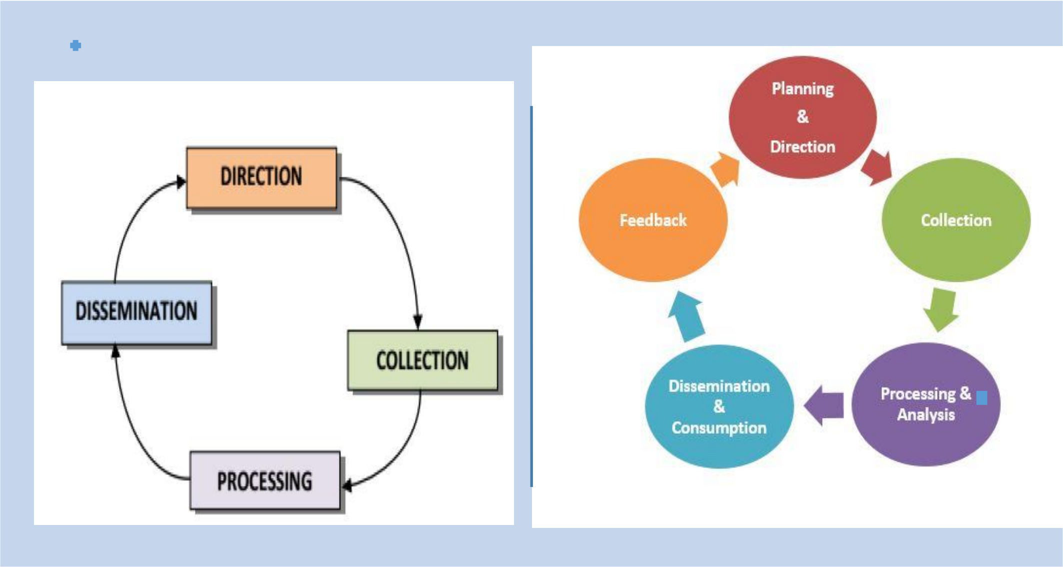


Figure 3: Left: Canadian 4-phase intelligence cycle.[105] Right: A general 5-phase intelligence cycle

Following this is the collection phase. Collection of data can often be from either open source or private sources. It is important to note that just because information comes from a private source it does not necessarily make it more useful, that is, reliable and credible. Indeed, 95-98% of all information handled by the US intelligence community is open source.[106]

Next is the processing phase. Here, information is basically made

[104] Robert M. Clark, *Intelligence Analysis a Target Centric Approach,* p. 5

[105] A. Frini and A.-C. Boury-Brisset, "An intelligence process model based on a collaborative approach" *Defence Research & Development Canada, no. Paper 113*, (2011)

[106] Gibson S.D. "Exploring the Role and Value of Open Source Intelligence" In *Open Source Intelligence in the Twenty-First Century. New Security Challenges*, Hobbs C., Moran M., Salisbury D. (eds). (London: Palgrave Macmillan, 2014), p. 10

ready for analysis through techniques like decryption, language analysis, amongst other. Analysis the phase where intelligence is actually produced. It involves using information in conjunction to what is already known, connecting the dots, amongst other. The result of which is written into a report and shared with the policy makers or 'intelligence customers'. Often, policy makers come back with more requirement thereby re-triggering the intelligence cycle.[107]

In spite of the high appraisal this classic intelligence cycle has gotten, some academics and researchers still thought necessary that new intelligence cycles be created that shows the reality of cycle and the factors that influence it.[108] Indeed Dr. Mark Phythian, Professor at the department of politics and international relations at the University of Leicester and Dr. Gill, a research professor in intelligence studies at the University of Salford came up with a series of criticisms on the intelligence cycle. Firstly, they draw attention on the fact that the intelligence cycle is a closed loop, lacking interaction with the environment which prevents the consumers of intelligence from giving their feedback. Secondly, they assert that the command on internal issues is not clear. For example, who decides if a factors is still considered a threat or not. Thirdly, they argue that the intelligence cycle is not a straight forward 'linear' process: some phases can go back and forth. For example, at the analysis phase, something can be discovered that makes the analysts go back to collect more information. Next, they argue that the cycle lacks the incorporation of covert action which all nation-states carry out. This point is more political and does not fit in our interest of cyber threat intelligence within the context of enterprises. The last flaw they discover in the classic intelligence cycle is the lack of consideration in technological advancements.[109] All these criticisms

[107] Federation of American Scientists, "The Intelligence Cycle". Fas.org, https://fas.org/irp/cia/product/facttell/intcycle.htm, (Accessed: June 2, 2020)

[108] Frini, "An intelligence process model based on a collaborative approach", p. 9

[109] Peter Gill, Mark Phythian, *Intelligence in an insecure world*, (Polity, 2nd Edition, 2012)

culminated with a proposition of an intelligence cycle called the intelligence web in order to attempt to account for these flaws.

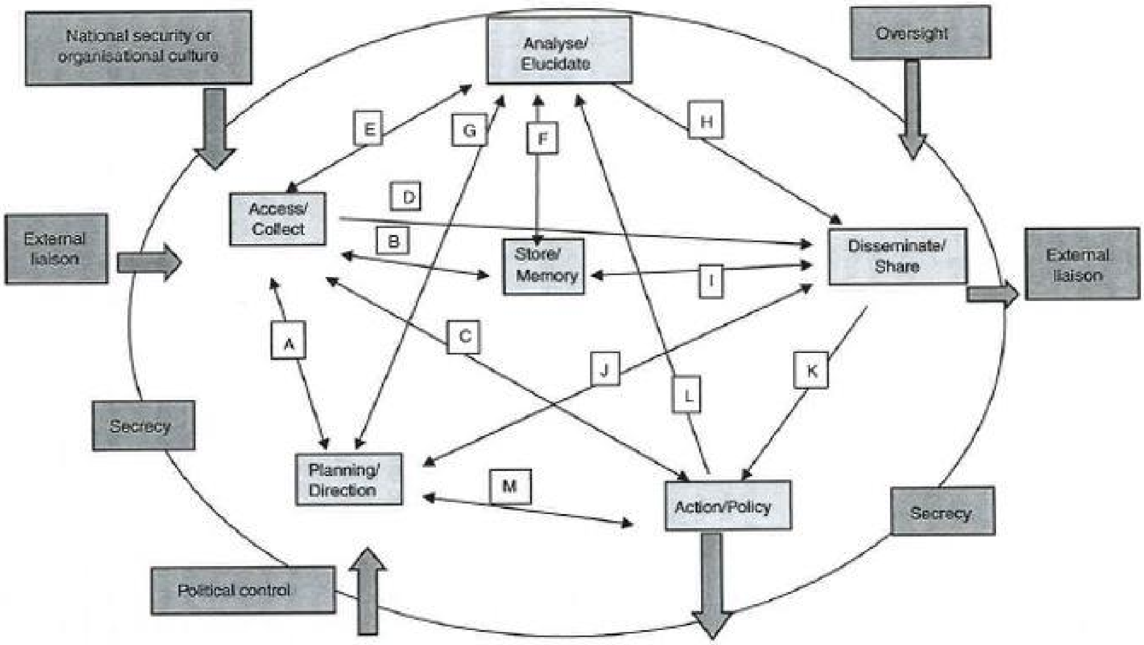


Figure 4: Intelligence web, Dr. P. Gill & Dr. M. Phythian.[110]

Indeed, the September 11 terrorist attacks in the US revealed gaps in intelligence collection and analysis. However, these gaps were ignored and the Madrid 2004 & London 2005 are the results. Gill and Phythian assert that there has been changes in intelligence collection notably with the advent of technology, the role of the private sector and the general public. However these advances have led to the collection of tremendous amounts of information so much so that it cannot all be analysed thereby reducing its utility. The same dynamic can be spotted in companies offering cyber threat intelligence services whereby loads of information is collected on malware infection but very few analysis carried out. Finally, the authors also raise the ethical issues that have arose as a result of technological advancements in intelligence collection and praise the fact they have brought about the

[110] Ibid.

democratisation of intelligence collection.

In the same way, Frini and Boury-Brisset equally criticised the classic intelligence cycle and came out with many flaws some of which are:

- The classic intelligence cycle is not iterative
- Makes it difficult to trace errors
- Intelligence is used to support the policy maker rather than inform him
- Does not allow for evaluation of the activities within tach step
- Intelligence collection is only driven by decision makers
- Analysis and collection can work simultaneously

Similarly, they proposed an intelligence model called the 'All-source intelligence model' which makes information accessible, involves all resources, promotes enhanced evaluation, and favours the exchange of intelligence between everyone involved in the process.[111]

Another interesting intelligence cycle is that of the UK's Ministry of Defence as published in the Joint Doctrine Publication. It is interesting because it addresses some of the flaws previously stated. The cycle comprises many other cycles with tasks that overlap which could be done simultaneously, rather than sequentially.[112] Even though this is a good point, the cycle still remains complex compared to the classical model, even after stating that the said model was an over simplification. Another good point is that the model tries to account for bias by using structured analytical techniques. Notice that so far, the issue of bias was not mentioned in all previous models reviewed. The document further asserts that in order to reduce bias, where appropriate, external actors like academics may be consulted for their differing perspective.[113] Other ways of reducing bias is by red teaming, using a key-assumption check, peer reviewing, using the same

[111] Frini & Boury-Brisset, "An intelligence process model based on a collaborative approach"
[112] UK Ministry of Defence, "Understanding and Intelligence Support to Joint Operations (JDP 2-00)," p. 53
[113] Ibid. p. 73

data collected to disprove the current outcome, and playing the devil's advocate.

Robert M. Clark brings up an interesting argument on the relationship between the intelligence cycle and the actual, 'real-life' implementation of the cycle by stating that:

'*The traditional cycle may adequately describe the structure function of an intelligence community, but it does not describe the intelligence process. [..] The cycle is still with us, however, because it embodies a convenient way to organize and manage intelligence communities like those in large governments and large military organizations.*'

It should be noted that the book written by Robert M. Clark from which this quote was taken has a governmental/military theme which explains the references made to the latter. Clark equally proposed an intelligence model after equally detecting the same flaws in the classic intelligence cycle like linearity, lack of policy makers' feedback loop, and no interaction between the parties involved in the intelligence cycle. Clark's model is target-centred and in addition to being used for government, can be also used for criminal intelligence.

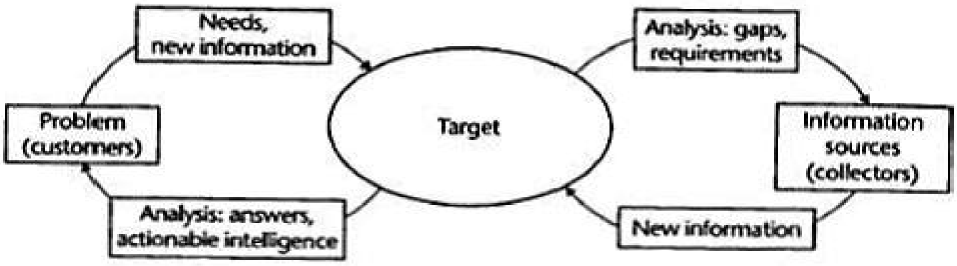

Needs, new information
Analysis: gaps, requirements
Problem (customers)
Target
Information sources (collectors)
Analysis: answers, actionable intelligence
New information

Figure 5: Robert M. Clark's Intelligence model

The basic idea behind this model is that all participants in the intelligence cycle have access to the target and can extract the information they need and can equally contribute from their resources in order to create a more a fair depiction of the target.[114] The goal being that thanks to the parallel nature of

[114] Clark, *Intelligence Analysis a Target Centric Approach*,

the model, new requirements, information or intelligence can be injected and shared in the cycle at any time from all parties.

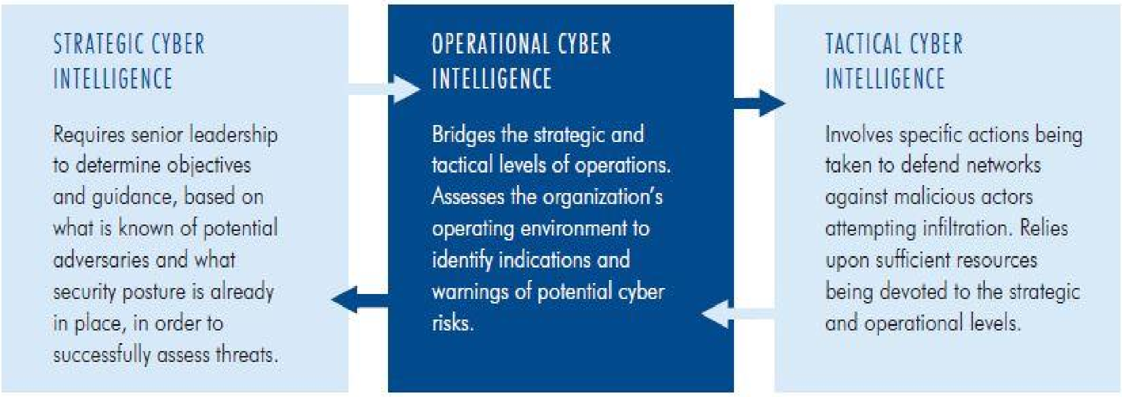
Another model worth mentioning is that developed by the CBEST, an intelligence-led security company in partnership with the Bank of England which published a paper that presents the most favourable ways for the production and consumption of threat intelligence. From the start, the paper asserts that cyber threat intelligence in companies remains relatively highly immature when compared to the public sector. It is immature in the sense that it is still very much *ad hoc* rather than methodological and that the cycle should be tailored to each enterprise. In order to remedy this, enterprise cyber threat intelligence can benefit from decades of government's intelligence practices. Government intelligence practice equally testifies that a consensus on a cyber threat intelligence cycle is possible. The document equally reveals that there is poor intelligence sharing within the public sector. Cyber threat intelligence will not only improve cyber security by combatting advanced persistent threats through an actionable approach diagnoses, predictions, executions and influences but can equally help in business strategy.[115]

The paper further argues that the cyber threat intelligence cycle should answer the 5W1H questions an also raises an interesting aspect of cyber threat intelligence that has not be talked about so far; to consider allocation of resources for the good functioning of the cycle. In fact they argue that only a good understanding of threats and vulnerabilities should drive the allocation of resources. It presents a cyber threat intelligence cycle very similar to that of the traditional intelligence cycle and the SANS institute but are conscious of the fact that it is misguiding because the cyber threat intelligence cycle is not linear and the phases are not of equal complexity and duration.[116] The document asserts that the direction should take into account previous success and losses and that intelligence directions may be divided into short-term,

[115] CBEST "Understanding Cyber Threat Intelligence Operations", *p. 3*
[116] Ibid. p. 15

medium-term, and long-term directives.

The Intelligence and National Security Alliance, INSA, in their model of cyber threat intelligence cycle pose a strong emphasis on the importance of tactical cyber threat intelligence. This paper greatly helps in understanding all levels of cyber intelligence, contrary to other papers do not mention it, if so do it very briefly.



STRATEGIC CYBER INTELLIGENCE

Requires senior leadership to determine objectives and guidance, based on what is known of potential adversaries and what security posture is already in place, in order to successfully assess threats.

OPERATIONAL CYBER INTELLIGENCE

Bridges the strategic and tactical levels of operations. Assesses the organization's operating environment to identify indications and warnings of potential cyber risks.

TACTICAL CYBER INTELLIGENCE

Involves specific actions being taken to defend networks against malicious actors attempting infiltration. Relies upon sufficient resources being devoted to the strategic and operational levels.

Figure 6: Cyber intelligence – responsibilities and inter-dependency.[117]

This emphasis on the importance of cyber threat intelligence is not only because of the advantages cyber intelligence bring in general but also because it is '*predictive and not reactive.*'[118]

Lastly, the cyber kill chain which has been mentioned several times as an effective tool in cyber threat intelligence is worth mentioning. Prior to the existence of advanced persistent threats, cyber security used a model that only recognised pre-defined threat signatures which was expected of the adversary to use. The cyber kill chain was devised by the Lockheed Martin Corporation in 2011 shifts from trying to keep all adversaries outside of the network to assuming that the adversary eventually forces its way into the system. Originally devised from military operations, and later on adapted to the cyber space, the cyber kill chain consists of 7 phases starting from

[117] Geoff Hancock, Christian Anthony, and Lincoln Kaffenberger, "Tactical Cyber Intelligence", *Intelligence and National Security Alliance (INSA)*, (December 2015)
[118] Ibid. p. 3

reconnaissance to actions. It has gained momentum and high appraisal as mentioned earlier. The cyber kill chain describes the stages in which an intruder or attacker will go through in order to compromise a system and carry out its objectives.

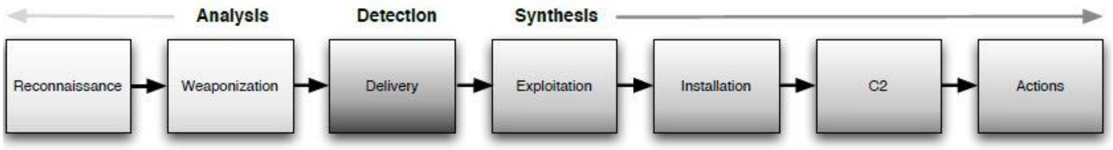


Figure 7: Cyber kill chain.[119]

- The reconnaissance stage helps to identify and select targets
- Weaponisation stage serves to tie the intruder with the deception method that was used against him like spear phishing, honey pots, amongst others
- The transmission of the weapon to the target takes place in the delivery phase
- Exploitation stage is where the code that was contained in the deception method that was used against the target is ran in order to take ownership of the computer/system.
- The installation stage is where more software is downloaded and installed in order to strengthen the intruder's presence in the target's system.
- The C2 stage, which stands for command and control, serves to establish a connection that will allow the intruder to gain control.
- Finally, the actions stage is where the intruder extracts confidential data, damages the system, and harms the target's operational capability, amongst others. In short, the intruder simply applies his objectives. All of which is done while carefully ensuring that more machines are compromised within the network.

[119] Hutchins Eric et al. *"Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", p. 7*

The paper further asserts that the intruder needs to be successful in all these stages for the attack to work and the defender needs only break one stage of the kill chain which will force the intruder to start all over. The kill chain presents a linear model with well-ordered evolution.[120] However, in real life, the actions of the intruder may not always be linear. Also, the kill chain does not take into consideration the motives of the intruder, nor the fact that 2 or more intruders may carry out the same action which may be misinterpreted, nor the fact that there may be insiders from within the organisation that will cooperate with the intruder. That is why gathering intelligence on the attacker himself, where it is possible to identify him, is important.[121]

Other organisations devised their own kill chain based on Lockheed Martin's one. Some of which are:

- Intelligence gathering, initial exploitation, command and control, privilege escalation and data exfiltration from CREST, a company offering cyber security services.[122]
- Motivation and decision to act, determine objective, select avenue of approach, acquire capability, develop access, implement actions, assess and restrike – INSA.[123]
- Staging of attack components, reconnaissance against target, and execution of the attack and exploitation of attack's successes – Jellenc E.[124]
- Reconnaissance, incursion, discovery, capture and exfiltration.[125]

[120] Ibid.

[121] CBEST "Understanding Cyber Threat Intelligence Operations", *p. 12*

[122] CREST, "Cyber security incident response guide", *CREST (GB), Version 1,* (2013)

[123] INSA, "Operational levels of cyber intelligence". Intelligence and National Security Alliance, (2013)

[124] Jellenc, E, "Unpublished research materials", VeriSign-iDefense, Inc. (2013)

[125] Kapuria, S, "IT threat intelligence to anticipate, stop and counteract targeted attacks", *Symantec Corporation*, (2011)

Considering all the criticisms raised in the literature review for cyber threat intelligence cycle and the intelligence cycle, it can be retained that the most salient appraisals that are pertinent to cyber threat intelligence from the context of an enterprise are:

- Include feedback in order to make the cycle iterative. Note that even though some intelligence cycles include this stage, it is not present in the classical/traditional intelligence cycle. Also, the model should come out of the twentieth century industrialisation mind-set style which looks like a factory assembly cycle
- Allow for parallelism and flexibility (stages can go back and forth) across the necessary stages of the cycle. Facilitate the localisation of errors that occur within the cycle
- Planning & direction and dissemination stages suffer from the customers having little to zero knowledge on intelligence. Recommend that every agent in the cycle is a domain specialist
- Collection process it not driven by policy makers only and the use of structured analytic techniques to reduce bias
- Businesses focus too much on profit and see intelligence as a burden. This affects allocation of resources for the functioning of the cycle
- Semi-automation of collection, processing, and analysis stages in conjunction with human guidance/effort.
- The cycle should be adapted to fit each objective in the planning and direction. That is, the cycle should not assume the same process irrespective of the objective.
- Make use of the cyber kill chain
- Lastly, taken from the definition of cyber threat intelligence that was earlier proposed, it should include counter-intelligence.

In conclusion, the lack of academic literature on cyber threat intelligence and its creation process (cycle) within the specific context of enterprise cyber security is evident. This is owing not only to the newness of the term but mainly because cyber threat intelligence or even just intelligence was long seen as a military or government tool which brought about a lack of adequate academic research on cyber threat intelligence in terms of enterprise cyber security. There is equally little to no consensus between the developers and consumers of cyber threat intelligence because the companies providing cyber threat intelligence are more focused on profit which makes them likely to define cyber threat intelligence in the most attractive way to customers even though the definition may not be accurate. Therefore, the research question presented in this paper rightly identifies the need to understand how cyber threat intelligence can be defined and modelled in the perspective of enterprises. This is useful because as demonstrated in the introduction, cyber threat intelligence has been recognised as the most effective protection against APTs and understanding it within the context of enterprises will help them enhance their cyber security.

Chapter 4: CYBER THREAT INTELLIGENCE CYCLE MODEL PROPOSAL

The previous section after a thorough literature review identified the most salient points that are pertinent to cyber threat intelligence. These points will be used in this section to propose a cyber threat intelligence cycle. This section first starts by justifying the need for a cyber threat intelligence cycle that is different from the traditional intelligence cycle. We will then go on to explain how these points are applied at different stages of the proposed model, introducing novel practices, while doing so from the perspective of enterprise cyber security. This will end with a critical analysis of the proposed model in order to establish its advantages and limitations.

Recall the definition of cyber threat intelligence from the perspective of enterprises that was proposed by this paper in the previous chapter which was: *The result of a process that involves information collection either in the real word or cyber realm or both in order to provide foreknowledge, knowledge and counterintelligence on the threat landscape, the intentions and behaviours of the attacker or a competitor, and support the cyber security decision making of an enterprise.*

This definition, which is the fruit of the analysis other definitions and theories of intelligence as seen in the literature review, together will the salient points that were listed will be used as the theoretical framework throughout this section when building up a cyber threat intelligence cycle from enterprise perspective.

A cyber threat intelligence cycle or an intelligence cycle in general conveys messages through 2 aspects:

(1) the whole picture, presented as a graphic or diagram. That is, the visual/graphic aspect, and;

(2) the actual meaning of the stages in the cycle.

However, before diving into the design, one may ask; if what is generally referred as cyber threat intelligence is indeed just threat information or threat data, then why must this raw data go through another form of cycle – the cyber threat intelligence cycle – rather than just go through the common traditional intelligence cycle?

This paper argues that the answer lies in;

1. The sphere in which the resulting threat intelligence will be applied, which is the cyber space.

2. The dimension in which data is collected and analysed is largely in the cyber space (use of computers, AI tools, internet, amongst other). Even though we will come across a cycle that includes HUMINT collection, a great deal of information is still collected from the cyber space.

3. Note that collection methods like HUMINT, open-source intelligence (OSINT) are methods that were designed to fit the intelligence cycle and the issues that it was meant to solve those days. In the present era, the cyber space has grown in importance and has been recognised as a realm on its own. In view of all these, it is safe to say that cyber threat intelligence is distinct enough to have its own cycle.

Back to the cycle design, one can notice that the more details added on the graphics, the more it becomes complex. Therefore, one of the challenges also resides in trying to show much without making it look complex.

Taking into account the findings in the previous chapter concerning the factors to consider when designing an effective cyber threat intelligence cycle for enterprises, it was argued that while some models had 4 to 5 stages, it would be optimal to have more to facilitate error detection. This paper proposes a cycle with eight stage with are:

- Requirements
- Planning and direction
- Collection
- Processing
- Analysis

- Dissemination/Sharing
- Consumption/Implementation of threat intelligence
- Feedback

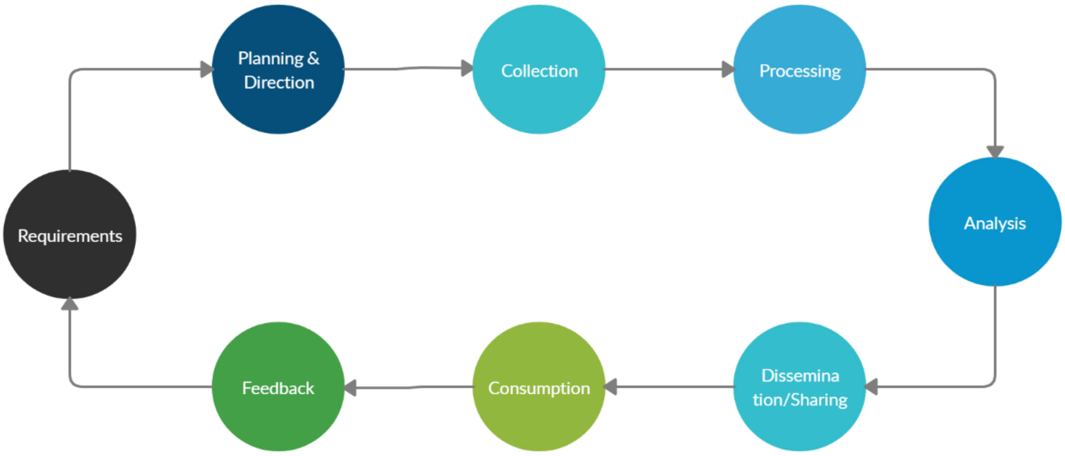


Figure 8: Initial proposal of 7-stage cyber threat intelligence cycle

However, completing the cycle to 8 stages by adding the requirement and feedback stages and equally splitting the processing and analysis into 2 separate stages does not fulfil the factors that were discovered and enunciated at the end of the previous chapter. This is so because the other factors cannot be represented graphically. As previously stated a, this paper sees a cyber threat intelligence cycle or an intelligence cycle in general as having 2 aspects, a visual/graphical one and the explanatory aspect which gives the actual meaning/use of the stages in the cycle. As a reminder, the remaining points that need to be fulfilled are:

1. Allow for parallelism and flexibility (stages can go back and forth) across the necessary stages of the cycle. Facilitate the localisation of errors that occur within the cycle

2. Planning & direction and dissemination stages suffer from the customers having little to zero knowledge on intelligence. Recommend that every agent in the cycle is a domain specialist
3. Reduction of bias
4. Businesses focus too much on profit and see intelligence as a burden. This affects allocation of resources for the functioning of the cycle
5. Semi-automation of collection, processing, and analysis stages in conjunction with human guidance/effort.
6. Make use of the cyber kill chain and include counter intelligence operations

Taking these factors into account, this thesis proposes the model in figure 9 below (a larger image can be found at the appendix). Notice how the stages are grouped into similar colours. Here, the green designates the stages that are mostly 'in the hands of the customer'. The intelligence analyst has little influence to no influence over these stages. For example, in the dissemination stage, the analyst is in charge of producing and disseminating the intelligence report while the consumption, feedback, and requirements are heavily influenced by the customer. Next, the stages in sky blue represent stages in which the analyst is fully implemented. Note that the circles in orange are not extra stages. They represent processes/actions which are carried out simultaneously which then fulfils the parallelism requirement. The dark blue circle, the planning and direction, is a stage where this paper proposes that it be done by an intelligence officer/manager who has experience in managing and coordinating intelligence projects and allocation of resources.

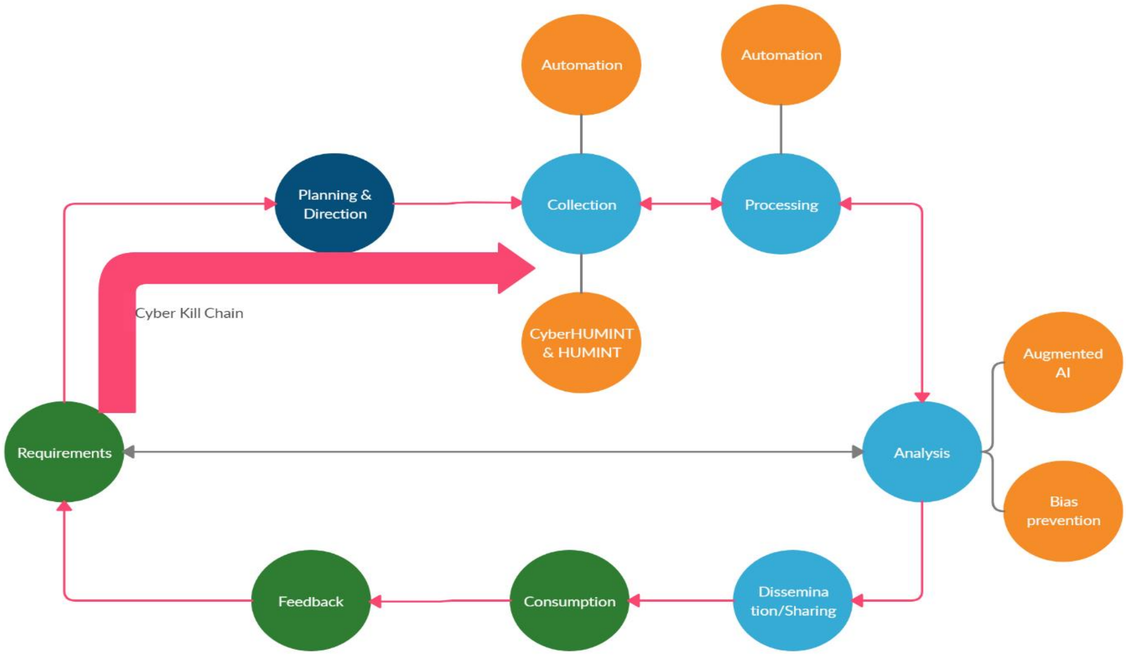


Figure 9: Final proposal of a cyber threat intelligence cycle.

Lastly, the pink bent arrow represents the cyber kill chain which stops at the collection stage because the cyber kill chain involves the collection of information on network intruders.

At first glance, one positive aspect of this proposed cycle is that it is understandable to someone who has little or no knowledge on cyber threat intelligence. This is so because as the colour coding shows, the cycle can be grouped into the traditional 4-stage cyber intelligence cycle to which people are easily familiar with. A 4-stage intelligence cycle comprises of direction, Collection, processing, and dissemination. These will be equivalent to: direction – requirements and planning & direction, Collection – collection, processing – processing and analysis, dissemination – dissemination, consumption, and feedback. Another positive aspect is that a head of security operations centre (SOC) in a company could edit this model to fit his/her organisation capabilities/resources.

The proposed cyber threat intelligence cycle in its entirety is an incorporation of best practices that aim to answer the 5W1H questions – the

Who, What, When, Where, Why, and How (by what means). Ultimately, the role of this cyber threat intelligence cycle is to produce threat intelligence that will help security operation centres and other business decision makers in protecting the businesses' assets and ensure the well-being of the company. As a result, the company should be careful of knowing what the threat intelligence will serve – will the threat intelligence support decision making or will it represent the decisions in itself? In order to be clear on this, this paper proposes that the company share common goals and be knowledgeable on the value and limits of intelligence.

4.1.1 Requirements

This stage entails getting the task from the client. The requirements is one of the, if not, the most important stage because if the instructions or task is misunderstood, then the product of the cyber threat intelligence cycle will be doomed to failure right from the start. This will also lead to wastage of time, money and resources. So it is vital that the requirements be clearly understood by the intelligence manager.

The intelligence manager gets in contact with the client to help the client define and understand what they want, how they wish the cyber threat intelligence report to be made. The manager can choose from the traditional requirement gathering techniques like brainstorming, interview, observation, reverse engineering, prototyping, amongst others. Pertaining to the proposed model in this paper, the prototyping methods works best. In this method, a preliminary requirement is gathered in order to produce an initial version of the solution. If this solution satisfies the requirement and the client, then the requirement and process is approved if not the requirement and process is adjusted accordingly. This is represented by the two-way grey arrow which connects the requirements and the analysis stage. The intelligence manager should be flexible in order to be able to pick up the nuances expressed by the client. Follow-up question are important however the manager should beware of not ending up speaking for the client instead, because it will look like the manager is defining the requirements by himself. Therefore, the best practice is to be flexible and ask questions in order to guide the requirements but also to listen. In addition, it is equally beneficial to obtain details of previous cyber attacks on the enterprise and on other enterprises both the same and different industry. The enterprise will then compare this information with its own security posture in order to identify gaps which can serve as a start for the formulation of requirements.

Also, at this stage, depending on the requirements, the cyber kill chain can be used from the requirements stage to the collection stage since the cyber threat intelligence cycle is primarily designed for APTs, as elaborated at the beginning of this paper. Some signs of APTs that should be looked out at the requirement stage are; information moved, data clumped and ready for export, spear phishing, Trojans, odd logins, and wide spread backdoor. The cyber kill chain will be activated because it is a tool that is used for gathering information on network intrusion. The cyber kill chain is important because businesses suffer lots of intrusion attacks leading to massive data breaches of confidential information like passwords, Personally Identifiable Information (PII), bank account information, amongst others.

The cyber kill chain can equally be used in normal times or when honey pots[126] are installed in the network in order to lure attackers and learn from their intrusion techniques. Once the stage at which the attacker is on the kill chain has been identified, it is up to the analyst to break the chain – and hence stop the continuation of attack – or wait to see how the attacker progresses in the chain and collect more information.

Finally, businesses cannot respond to every single threat they face, especially small and medium-sized enterprises which even have more budget

[126] Honey pots are ways in which cyber security defenders protect data or networks from unauthorised use by using false representation of the true data or fake copies of the true network/website. The goal is to allow the attack use all his/her techniques so the defender will learn from it and better adapt security measures on the real data or network/website.

constraints and resources. Therefore, it is necessary that they prioritise threats through the operational understanding of threats, vulnerabilities, and resource management.

4.1.2 Planning and Direction

In this phase, the intelligence manager plans how the cycle will work and will modify the cycle in order to adapt to the requirements, if necessary. What needs to be done, who is going to it, through what means and resources, and how the success will be measured is equally defined here. This stage also has to set out a strategy to monitor and ensure the effective flow of the cyber threat intelligence cycle.

While planning, it is good practice to compare the cyber threat intelligence process with leaving from known knowns to unknown unknowns via known unknowns. Known knowns are the things we know we know, therefore we have no doubts or uncertainties about them. These are generally factual information like the IP address of a website, the functioning of a worm, a virus, amongst others. Known unknowns on the other hand are the things we are aware that we do not know. Here, you have the knowledge and capability to measure the uncertainties around them. Unknown knowns are the things we do not know we are aware of. They represent intuition or tacit knowledge, that is, knowledge that is difficult to transmit by means of writing or verbalisation. Like Polanyi rightly said, they are things "we can know more than we can tell."[127]

[127] Polanyi, Michael, *The Tacit Dimension*, (Chicago: University of Chicago Press, 1966)

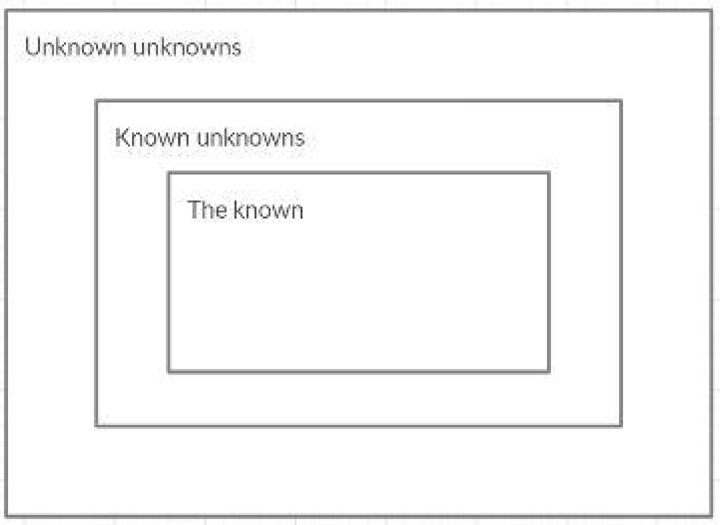


Figure 10: The unknown unknowns englobes all knowledge. Own work.

Finally, unknown unknowns are the things we do not know we are aware of. Uncertainty cannot be quantified because we do not even know what to measure in the first place. However, in some sense, it represents the absolute truth/knowledge because it is all the things that are to be known of an object but which we can cannot fully access because we are not aware they exist in the first place. So, the best we can do is to get a little closer to it by means of relentless exploration of knowledge. Therefore, during the planning process, the manager should strive to reach the unknown unknowns of the requirement.

After having clearly understood the intelligence requirements, the intelligence manager evaluates the requirements in order to ascertain that they are within the capabilities of the intelligence team. After this step, the requirements are then translated unto the proposed cyber threat intelligence cycle where the appropriate collection, processing, analysis and dissemination techniques and resources are allocated. It also beneficial that previous failures and success of the threat cycle be taken into account as it may help either not to repeat the same mistakes or it may help in solving problems that have been encountered before.

4.1.3 Collection

Based on the requirements, the areas and collection methods are set out. Collection often takes the largest part of the budget due to the time and energy used in collecting data from different sources. Collection is the exploitation of sources for the gathering of data and the delivery of this data to the analysts for the production of intelligence. Collecting the correct information with the appropriate methods is vital as it may lead to downstream errors if the data collected is not compatible with the intelligence requirements.

In the threat cycle model proposed, data can come from a variety of sources through automation by the use of artificial intelligence. These sources are; cyber human intelligence (cyberHUMINT), and HUMINT in addition to other conventional collection methods like Signal intelligence (SIGINT), imagery intelligence (IMINT), open-source intelligence (OSINT). Recall that in the definition of cyber space that was given at the introduction, the cyber space exists both in the space, air, land & sea realms and so cyber threat intelligence collection can occur across all these realms. This multi-discipline collection strategy should be coupled with a collection strategy that prioritises the intelligence requirement, takes in to account the capabilities and limitations of the resources of the company, and is flexible and dynamic.

With the increasing amount of information from diverse sources on the internet, the automation of collection in the intelligence cycle has been recommended and praised as earlier seen. More specifically, the RUSI recommended the automation of collection in parallel with other conventional methods. This thesis proposes the automation of collection from news feeds, MRTI data feeds,[128] large databases of text files, and the tons of threat information reports falsely labelled as threat intelligence by some cyber security companies. The remaining data collection methods – cyberHUMINT and HUMINT – are there to capture a type of data that reflect the behavioural

[128] MRTI stands for Machine Readable Threat Intelligence

dimension of cyber security. Semi-automation is equally necessary at this step due to the immense amount of open-source information available on the internet nowadays which makes looking for the right information akin to searching for a needle in a haystack. There are AI algorithms that can enable the targeted search and collection of information based on specific keywords.

Finally, this paper proposes that intelligence collection must also occur in the dark web. The dark web is the nucleus of the malicious hacking world and contains forums and websites where hackers gather to share their ideas, techniques and buy and sell hacking tools. This therefore represents a gold mine for gathering information on hacker's capabilities, intensions and possible plan of action. J. Robertson et al. have written an excellent paper on how to browse the dark web and integrate hacker forums for information collection.[129]

The Behavioural Dimension of Cyber Threat Intelligence

The majority of cyber security approaches are focused on the computer or the state of the computer network and the important documents that are saved inside. The behavioural dimension of cyber threat intelligence additionally focuses on the person and not just on computer or the internet because behind every computer is a human being. Therefore, striving to know who is he, what are his intentions, how does he think, what are his connections (to other people, organisations), what are his beliefs, aspirations, amongst others suddenly becomes important. Combining this intelligence from 'the person' with that from 'the machine' will help optimise the cyber defence strategy. CyberHUMINT collection help integrate other sources of information outside of computer network/internet because network activity only represents part of what influences the attackers' cyber operations. CyberHUMINT data collection serves to facilitate the narrative of the attacker's intent. Therefore,

[129] John Robertson et al. *Darkweb Threat Intelligence Mining*, (Cambridge University press, 2017)

real life behavioural data and technical data is what gives an edge to this proposed cyber intelligence threat cycle.

For most attackers, what generally precedes the launching of a cyber-attack are well planned human activities to decide the action, the selection of an appropriate target and finally launching of the attack based on their own intelligence and their strategic goals. These are called the operational levels of a cyber-attack and CyberHUMINT & HUMINT will help collect data on this. Therefore, by correlating say data from geopolitical and social events with technical data, the estimation of the timeframe of an attack may be possible.

CyberHUMINT refers to the methods and tactics that are generally used by cyber attackers in order to obtain private information while attacking the human factor of their prey. It was first coined by an Ed Alcantara, a pioneer in cyber intelligence in the dark net, in 2010.[130] CyberHUMINT includes the use of online psychological deception tactics like social engineering as well as the use of conventional human espionage such as agent recruitment. Indeed, behind every computer/machine is a human being, therefore, by attacking the human factor and gathering intelligence on the human, it helps give more insight on the cyber-attack and can facilitate attribution.

Because cyber attacks, especially on businesses, are the result of wilful and well organised intelligence gathering, incorporating cyberHUMINT as a collection method in the proposed cyber threat intelligence cycle will permit intelligence analysts explore the real aims and potential capabilities of the attackers. This provides the organisation with a clear picture and more sober understanding of the threats they face. In order to achieve this, the business will need qualified computer engineers or IT professionals who are well skilled in behavioural patterns, language analysis, dark net jargon and culture, amongst others as well as HUMINT agents. As a result, computer

[130] Jeff Williams, C., *Interview: Ed Alcantara, CSO Of Darknet Blackops Intelligence*. Contrastsecurity.com. (2015). https://www.contrastsecurity.com/security-influencers/episode-28-ed-alcantara (Accessed: 9 June 2020)

experts work in tandem with intelligence specialists in order to uncover potential future cyber attacks long before they develop into actual attacks. This gives organisations the luxury to decide how, when and where to incapacitate potential threats.

It is equally important that businesses accompany the collection process with a collection strategy. This thesis recommends that companies consider the breadth versus depth dilemma. In some situations, it might be beneficial to collect data over a wide range without going into details (large breadth, small depth) while other times collecting highly detailed data over a small range is preferable (small breadth, big depth). Collecting data over a large breadth and big depth is equally possible however, it will lead to huge amounts of data and the difficulty lies in processing the data for what is actually needed. It is true that the automation of processing in the intelligence cycle could make it less painful therefore it is at the discretion of the intelligence manager to see whether or not the intelligence team has the adequate resources for such collection.

4.1.4 Processing

Once the appropriate collection methods has been chosen based on a correct and clear understanding of the requirements and all the data collected, it is time to process the data. This phase involves the collation of data, that is, the grouping together of related items by different data processing methods like filtering, parsing, aggregating, de-duplicating, amongst other. Also involves the identification of significant facts and the evaluation of the reliability of the source and the credibility of information.

As this thesis has proposed, the processing can be semi-automated in addition or in parallel with human processing. If during the filtering process the AI is unable to make a decision on a set of data for example, it can flag the data and call for further review. At this point an intelligence analyst may now intervene and finish the filtering process based on his/her own skills and judgement.

Evaluation of the reliability of a source and the credibility of an information.

A reliable source is one which consistently provides credible information while credibility addresses both the objective and subjective component of the believability of the data or information. A credible source or information should be truthful, logic, and most of the times considered to come from experts.

In short, the reliability of a source is checked over time and the credibility of an information can be evaluated by cross-checking the information with other sources (when available) or by evaluating if the information makes sense by the use common sense, if other sources are not available. The table below can be used to evaluate or quantify credibility and reliability.

Reliability of Source		*Credibility of information*	
Completely reliable	A	Confirmed by other sources	1
Usually reliable	B	Probably true	2
Fairly reliable	C	Possibly true	3
Unreliable	D	Doubtful	4
Cannot be judged	E	Cannot be judged	5

Table 2: Evaluation of reliability and credibility

Source and information reliability and credibility are so crucial not just in cyber threat intelligence but in intelligence in general. Rafid Ahmed Alwan al-Janabi currently a German citizen of Iraqi origin, claimed he had worked in a mobile plant that produced biological weapons as part of the Iraqi government's weapon of mass destruction program. Even though the German Federal Intelligence Service and the British Secret Intelligence Service strongly doubted and verified the credibility of al-Janabi's allegations to be false, the US and British governments still used them as a basis for the invasion Iraq. Al-Janabi later revealed in 2011 to The Guardian that his allegations were false. This rather extreme example serves as proof that the evaluation of a source's and information reliability and credibility should not be neglected.

4.1.5 Analysis

This is the stage where actual cyber threat intelligence is produced. When data is turned into information that can help understand and thwart a cyber threat, then it is termed cyber threat intelligence.

As argued before, the collection and analysis should be partly automated since as the RUSI institute found in their research, all attempts to make AI fully mimic the role of humans is doomed to fail. Therefore, this paper proposes that the collection and analysis stage should be partly automated in conjunction with human skills.

Although it is true that automation can bring about the exclusion of human skills, it should instead be seen as a way to enhance human skills and capabilities. This can only be achieved by deeply understanding the capabilities that automation via artificial intelligence can provide from a human-centric perspective. Indeed, by automating monotonous tasks in the collection and analysis stages such as sorting data, collecting information from news feeds, amongst other, it provides more time to the analysts to focus on more intellectually demanding activities like critical thinking, problem solving, and creativity which are essential in intelligence analysis. This will permit analysts in the enterprise to transform AI findings into actionable information.

However, this does not mean artificial intelligence will support human skills only but rather they will work alongside each other. AI and human skills will work alongside each other such that their actions will be complementary. In such a way, it will bring about a sum of skills which will be greater than the individual parts. Therefore, this combination will be able to solve analysis tasks that humans alone or artificial intelligence alone cannot do by themselves. The biggest challenges in implementing this will be for organisations to stop viewing cyber threat intelligence as a burden and rather as an asset and hence invest in novel artificial intelligence technologies. Also, enterprises should be willing to re-skill their employees.

More specifically, machines will transform the data into patterns, trends, clusters, and sequences thereby turning the data into more manageable subsets with low SNR (signal-to-noise ratio). Humans then apply imagination, intuition, curiosity, to try to 'link the dots'. The end result of analysis is to produce intelligence that is either descriptive – describe the problem at hand, prognostic (predict), or decisive/actionable – for decision making or planning cyber security actions.

Augmented AI

The general expectation of AI is what it can do on its own without human interaction. However, augmented artificial intelligence is another conceptualisation of artificial intelligence with the concept that artificial intelligence serves to enhance human skills rather than replace it. The word augmented only serves to denote the role human intelligence plays in conjunction with machine learning/deep learning. Humans are still better at exercising common sense, versatility, intuition, and creativity, which are lacking in machines. However machines are rapidly learning 'prediction skills' and are on their way to truly emulate human skills. Therefore, augmented AI is used in this cycle for the collection of machine-readable threat intelligence online, from information from data feeds, to identify suspicious actions in a network, and other tasks which were previously accomplished by humans. All of these will help expedite the processing and analysis stages.

Bias

Biases are inevitable during intelligence analysis but this is not a call for it to be ignored. Rather, they should be accepted and properly handled. Cultural bias, cognitive bias, pattern bias, and self-interest bias are the biases that plague intelligence analysts the most.

The analyst should strive to understand that every threat actor is born into a culture and the practices of one another's cultures are neither right nor wrong – they are simply the expressions of these respective cultures. Therefore, if an analyst can identify the region from which his hacker is from, it is necessary that the analyst acknowledges his/her cultural bias when trying to understand for example the incentives of the attacker.

Self-interest bias arises as a result of analysts interpreting reality in their own way based on individual experiences, expertise, hobbies, amongst others. This bias may be reduced by explicitly elaborating the analysis decision making process/criteria from the beginning and revisiting them frequently throughout the process.

Cognitive biases is widely accepted as the most difficult to recognize and mitigate and has even been recognised as the major cause of failure at the CIA. This is because they are rooted in the way our brains function/think – they form an integral part of us and the awareness of the bias does not suffice to solve it. Cognitive bias be recognised in the following ways:[131]

- When analysts stick to first impressions even when the evidence later clearly shows that the first impression was wrong. This is not just stubbornness – if the data comes from a reliable and credible source, the analyst is highly prone to trust it even when it is disproved later on

[131] Richard J. Heuer, *Psychology of Intelligence Analysis*, Centre for the Studies of Intelligence, (1999): Chapter 9. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-andmonographs/psychology-of-intelligence-analysis. (Accessed: June 10, 2020)

- Basing too much on best guess. This happens when analysts have a hard time dealing with information they deem too complex. Breaking the information into separate bits may help in such situation.
- When there is difficulty in finding evidence on an issue, it means the issue does not exist
- The things we hear or experience by ourselves always seem truer than reported information.

This paper recommends the use of structured analytic techniques in order to reduce bias. Structured analytic techniques in addition to helping reduce bias, help deal with incomplete and ambiguous information. ‘Reduce’ because this paper argues that bias cannot equally be eliminated in cyber threat intelligence because behind every analyst is human being and as long as human beings are involved there will always be a form of bias in the analysis. Therefore, the best way is to acknowledge it and try to tone it down. Structured analysis works by breaking down a specific problem into its components and solving each component step by step. This method equally provides transparency for intra-office and inter-agency collaboration.

Analysts should beware not to think of analytic techniques are a ‘cure’ to cognitive biases. Cognitive biases simply question the bias by providing a wider range of options for analysis. They help reduce the frequency and severity of error. Techniques such as the key assumption’s check method – helps explain the logic and understand the key factors, signposts of change method – helps in tracking events, monitor targets, spot emerging trend. Can be of great help in the cyber kill chain. The devil’s advocacy method – helps in challenging the main assumption, What if method – helps deal with limited information, a situation very common in cyber security, Red teaming method – makes the analyst think how the adversary would have thought. All these will greatly help curb bias during the analysis stage.

Lastly, this paper argues that in addition to the use of structured analytic techniques in reducing bias, implementing diversity can also help in curbing bias. Indeed, a diverse team of intelligence analysts and cyber security experts of male, female and different backgrounds can help reduce bias because there is an interconnection between the shaping of society and technology. This stems from the argument that an algorithm reflects a social realm and that even technological developments and analyses reflect our cultural and social backgrounds and therefore, the bias they come along with.[132] Since cyber threat intelligence deals with technical data and experts, it will be beneficial to implement a diverse team.

4.1.6 Dissemination/Sharing

Once the analysis is over, the intelligence product is now distributed to the consumers. The final product should be reviewed by the intelligence manage in order to assure that it meets the requirements set at the beginning. In businesses, these consumers are often heads of IT security or risk departments at strategic, operational, and tactical levels. The dissemination phase often overlooked however, it is vital that intelligence be presented the right way and at the right time.

These factors are vital because even the best intelligence in the world would be worthless if it were not understood by their consumer or did not arrive on time. To achieve this, intelligence analysts, must strive to present intelligence in an understandable jargon-free form which matches the language of the recipient. Also care should be made to assure that intelligence is delivered in a timely manner that allows the consumers to make proactive decisions.

The cyber threat intelligence report may be disseminated through simple alerts, secure online portals, machine-readable data feeds, or custom designed. For businesses, this thesis recommends that threat intelligence reports be custom made because they are often equally given to high executives who will

[132] Striphas T., "Algorithmic culture*", European Journal of Cultural Studies*, Vol. 18 Nos 4-5. (2015): p. 395; Claude Draude, Goda Klumbyte and Phillip Lücking, "Situated algorithms: a sociotechnical systemic approach to bias", *Emerald Insight*, (September 2019)

be in charge of allocating cyber security budgets and have little know of intelligence jargon. Therefore, it is essential that the report be customised in a way that will soot the executives and other important senior staff. The burden is then left on the intelligence analyst to translate highly technical data into simpler terms without impacting the sense and tone that the threat intelligence is meant to convey.

Intelligence sharing amongst businesses is recommended especially when a small number of companies are targeted by a larger number of attackers. This thesis recommends that businesses share intelligence as a means of getting up-to-date with new cyber threats.

4.1.7 Consumption/Implementation of findings in cyber threat intelligence report

Once the intelligence report has been briefed to the consumers, it is left for them to implement it. This takes place at this stage. The consumers should be able clearly understand the threat intelligence such that they can translate it into actions. For this to happen, the intelligence must be tailored to the key interests of the enterprise.

Given the rapid increase in the number and virulence of APTs and other cyber threats,[133] most experts have agreed that successful intelligence actors cannot act by themselves.[134] Therefore, an effective cyber security management could also encompass the sharing of cyber threat intelligence amongst companies through Information Sharing and Analysis Centres (ISACs). The threat intelligence shared should be inclusive, actionable, trusted, and transparent.

In order to improve efficiency and effectiveness in the threat intelligence sharing, the companies should agree on some prerequisites like:

[133] Rudner, M, "Cyber-threats to critical national infrastructure: An intelligence challenge". *International Journal of Intelligence and CounterIntelligence,* 26(3), (2013): 453–481

[134] Parkes, A. "Lessons through reform: Australia's security intelligence." *The International Journal of Intelligence, Security, and Public Affairs*, 19(3), (2017): 157–170.

- Adopting a common cyber threat intelligence vocabulary
- A protocol for sending, receiving, and storing threat intelligence
- A common way of understanding and classifying threats

4.1.8 Feedback.

Consumer feedback helps to adjust future planning and direction. This equally helps in the continuous improvement of the cycle. Therefore, it is imperative that feedback be given through effective communication.

The feedback will either terminate the cycle or re-active it depending on whether the cyber threat intelligence attained its goal of understanding or mitigating a cyber threat.

4.2 Counter-Intelligence

Counter-intelligence intelligence are the measures taken to identify, deter, counter, exploit, degrade, and protect against adversarial intelligence activities that have been judged as potentially harmful to one's interests and intelligence practices.[135] The aim then is the countering of hostile activities. Espionage is the most pervasive form of adversarial activity.[136]

Cyber counter-intelligence is the design of deception tactics to lure the attacker in order to collect information or cause damage to the attacker with the use of cyber means as the primary technology. The ultimate goal is to out think and outwit adversaries. Cyber counter-intelligence goes by the saying 'the best defence is good offense'. Just as the military track terrorists and monitor them in for their security, businesses should do same when it comes to cyber threat intelligence with hackers.

Defensive cyber counter-intelligence aims at denying adversary's access to critical assets through physical defence of network assets. This may

[135] Duvenage, PC, and SH Von Solms. "Cyber Counterintelligence: Back to the Future." *Journal of Information Warfare* 13, no. 4 (2014): 42-56www.jstor.org/stable/26487466. (Accessed June 14, 2020)

[136] Ibid. p. 45

prevent issues like unauthorised access of computers, physical destruction, and introduction of malware. Another defensive measure that should accompany the proposed model is penetration testing. Penetration testing is crucial as it helps test the businesses' network with attack tactics that hackers use thereby shedding light on possible vulnerabilities.

Offensive cyber counter-intelligence uses means like deception, manipulation in order to neutralise adversarial intelligence activities. In the context of the proposed cyber threat cycle model, this occurs by the use of hardware and software tools like honeypots, intrusion detection systems, and counter-HUMINT espionage. Steps of counter-intelligence

- Indication of assets that may be of interest to attackers
- Asses the consequences of a possible compromise of these assets
- Identify current and potential threat agents and collect information on them
- Develop and implement counter-intelligence procedures – offensive and defensive. This can be through the identification, prioritisation, and investigation of espionage adversaries in that order. Next is the engagement and exploitation of counter-espionage targets. One this has been the done, the target may now be neutralised.

All the procedures and recommendations presented in this section must be applied with care in order not to fall in illegality.

4.3 Advantages and Limitations of the Proposed Cyber Threat Model

In addition to filling a gap in literature, this paper equally proposed a model with novel practices which represents the newness the model brings and its advantages as well. The proposed cyber threat intelligence cycle contains tools and techniques that are absent from the cyber threat intelligence cycles that were analysed in the literature review. While these concepts/tools are not new, their application in cyber threat intelligence are new. These are;

- The use of counter-intelligence to protect against adversarial intelligence because cyber attacks, especially on businesses, are the result of wilful and well organised intelligence gathering.
- The cyber kill chain to break network intrusion attacks
- Cyber human intelligence (CyberHUMINT) which takes into account the behavioural dimension of cyber attacks by collecting intelligence on the hackers
- Use of Augmented AI to consolidate human skills
- Even though the proposed model is designed specifically to work best on combatting APTs, it could also be used to business intelligence, or gathering intelligence on competitors in the industry.
- Use of a diverse team to curb biases
- Multi-discipline collection strategy that occurs across land, air, sea, space domains, and intelligence collection in dark web
- 8-stage model makes it easy to pin-point errors in during the process.
- Lastly, the fact that it is easy to follow and based off of traditional intelligence cycle. Therefore it will be easy to get acquainted with.

The model equally contains some practical limitations which are;

- The proposed model is costly to implement. While it is not necessarily an issue for large organisations, government agencies, or any other business that is dedicated to go the extra mile for its cyber security, it is not the case for small and medium-sized enterprises. Small and medium-sized enterprises are the most vulnerable to APTs and they could face some difficulties - financial or infrastructural - to incorporate this model in their business. Financial difficulties can arise as a result of the inability to afford the material (servers, AI tools, amongst others), paying expert intelligence analysts, HUMINT agents, counter-HUMINT, and cyber security experts. This point becomes more pertinent if one considers the fact that there is shortage of specialist cyber security skills which will make the current ones available on the market to be hired for high wages.

- The cyber kill chain asserts that the attacker will always follow the same steps as in the kill chain while believing that a disruption in one of those steps will disrupt the entire cyber attack. Therefore, the whole principle, kind of, rests on the fact that all attackers will follow the same chain of attack. In case the attacker does not – like amateurs, newbies, or teenagers with little technical knowledge who buy hacking tools on the dark net and 'hack for fun' – the approach will highly likely fail.
- Lastly, as the behavioural dimension of cyber threat intelligence was elaborated, it will require human agents in order to perform HUMINT. Without attribution of cyber-attacks, it will be difficult to know on what who/what entity exactly to gather HUMINT. Attribution of cyber attacks is a very strenuous and daunting task in cyber security in which attackers are often not identified with one-hundred percent accuracy. Such uncertainties can undermine HUMINT collection which can have a spill over effect on the threat cycle.

In conclusion, this section has fulfilled the objective of designing a cyber threat intelligence cycle within the context of enterprise cyber security with novice tools. This is not only important as it will contribute to academic literature in the field but it will also help companies have a clearer picture of cyber threat intelligence and its creation process.

Chapter 5: CONCLUSION

The previous section presented a model of a cyber threat intelligence cycle. Unfortunately due to research constraints imposed by the Coronavirus pandemic, this model could not be tested in real life. Before jumping to the conclusion, this section will first present ways in which the proposed model could have been tested to assure its feasibility and robustness. This will be followed by possible future research directions and finally and all-round conclusion.

5.1 Validation/Testing of Proposed Model

The validation or testing of a model is an integral part of a design process. Indeed, the efficacy and utility of a model should be demonstrated using rigorous evaluation methods which also provides a better understanding of a model.[137] Analogically, because this paper has proposed a model, a validation or testing method is therefore required. This section provides the factors and requirements for the validation of the proposed cyber threat intelligence cycle.

The style of the beauty is one of the aspects that Arnould E. et al. consider when evaluating designs. However, as the popular saying goes, there is no accounting for taste, meaning the 'stylishness' of a design is subjective. Therefore, this factor was not taken into account during the design of the model as the dominant goal was to find a cyber threat intelligence model that will efficiently combat APTs from enterprise perspective. Nevertheless, one cannot ignore the fact that stylish designs are easier, more pleasant, and more inviting to use. Therefore, this paper settles for style be considered as an evaluation criteria, albeit being a loose factor.

Another way to validate the proposed model is to carry out an observational case study. This will work in two ways. The first way will be validating the model in an enterprise environment in order to determine if the

[137] Arnould E., Hevner A., S. T. March, & J. Park, "Design Science in Information Systems," *MIS Quarterly, vol. 28, no. 1, (2004)* pp. 75–105 p. 86

goal of the model – clarifying the cyber threat intelligence concept and modelling a cyber threat intelligence cycle from an enterprise perspective – has been achieved. This will give insight to the real world application of the proposed model. The second way is evaluating the proposed model with an expert in the field/industry through an interview or a discussion. This will help evaluate the analysis, conclusions, and general construction of ideas in the proposed model. Troy Mattern and Michael Cloppert are good examples of specialists in the field due to their position as chairman of the Intelligence and National Security Alliance (INSA) & former executive of the US Cyber Command, and SANS institute specialist in cyber threat intelligence, respectively. This gives them a deep view in the subject field in aspects like feasibility, resources, operationalisation, management, and cost, amongst others thereby making their opinion credible and valuable. Another party or organisation that could equally give a credible opinion on the proposed model is the CREST a leading intelligence-led cyber security service and research company whose services are recognised by the Bank of England as they are working alongside.

The aim of the interview is to grasp what their understanding of cyber threat intelligence is. This is important because as argued in this paper, the foundation of every concept or model is based on how it is defined. This will help understand in what perspective they understand cyber threat intelligence and what themes, tone, and scope they have. These initial questions will then be used as a basis to understand their concept of the cyber threat intelligence creation process. Once the proposed threat cycle is presented to the experts, the aim is to get a feedback so as to understand if the proposed model is practicable in the real world. This will require very specific but open questions on what the proposed model conceives as an added values and questions on missing or incorrect factors and viability. If the outcome is positive, then the model can then be used in an enterprise setting for the second phase of the test otherwise the critiques will be used to refine the model.

During the implementation of the model in the real world, the aim is to know how the model has been incorporated into the organisation's practises, the issues encountered and why. Note that in case of failure, the business should be asked if it is as a result of the cyber threat intelligence cycle failure or failure to properly implement the cyber threat intelligence recommendations. This question arises because:

- The failure could have been as a result of the poor or misunderstanding of cyber threat intelligence by the client/customer in the consumption stage. OR
- The unfamiliarity of the client with the cyber threat intelligence realm thereby affecting his/her ability to properly communicate the intelligence requirements

Errors might also occur as a result of organisational failure, that is, the business was unable to implement the cycle in their organisational practices as a whole. What should also be considered during the real-world implementation of the proposed design is how the enterprise defines successes. A poor definition can affect allocation of resources, communication between analysts, thereby even affecting how success itself at the end of the cycle.

5.2 Future Research Direction

Promoting academic research, allocating funds for research in the industry, enabling decision makers and company executives to fully understand the potential of cyber threat intelligence, and educating on the importance of consensus in the field represents the future challenges to face for the improvement of cyber threat intelligence in companies. Talking about the future, further researches may focus on cyber threat intelligence and how it could help protect against cyber attacks in the context of working from home.

Indeed, due to the Coronavirus pandemic that has imposed a lockdown which led to working from home and a shift to virtual collaboration, future research in cyber threat intelligence within the context of enterprise cyber security could focus on the new types of cyber threats that these could cause to a company. Because most employees have little to no experience on working from home, it may bring about new forms of employee behaviours. We should also not forget that working from home involves having family or close relatives around which can equally be another potential form of threat. Since technical vulnerabilities are well known and documented, this future research may focus on the behavioural aspects of the employees towards virtual working spaces and how working from home may bring about new behavioural aspects coupled with new work-from-home technologies that may favour social engineering attacks, all of which could favour hackers. Since this paper equally takes into account the behavioural nature of cyber attacks, future research will benefit from using this paper as a base/starting point. Even though the lockdown will not be forever, it has raised questions on the necessity to work on-site and some companies have even considered letting their employees work from home indefinitely,[138] thereby highlighting the importance of such a research.

5.3 Conclusion

Cyber attacks have gradually become more targeted and sophisticated leading to a new type of cyber attacks called advanced persistent threats. While cyber threat intelligence has been recognised by experts and some academics as the most effective tool to combat these, its implementation has been very slow in addition to reports showing that lots of companies still do not spend enough on cyber security and suffer from the 'security poverty line'. In addition to the fact that the concept of cyber threat intelligence is recent, the slow implementation of cyber threat intelligence is largely owing to a shortage of academic research & literature and quality grey literature on the implications

[138] Rob, McLean. "These Companies Plan to Make Working from Home the New Normal. As in Forever," CNN Business, (June 25, 2020). https://edition.cnn.com/2020/05/22/tech/work-from-home-companies/index.html. (Accessed: July 7th, 2020)

of cyber threat intelligence in relation to enterprise cyber security. Indeed, cyber threat intelligence or even just intelligence was long seen as a military or government tool. Furthermore, there is non-consensus on the definition and principles of cyber threat intelligence, which has further made cyber threat intelligence become a marketing term in which companies use the definition that will attract the most clients, regardless of its inefficiency.

With regards to these gaps, this paper has helped clarify the concept of cyber threat intelligence by providing a definition and a cyber threat intelligence cycle within the context of enterprises in order to contribute to the academic literature and help companies better understand cyber threat intelligence. This was achieved through a qualitative comparative literature analysis of the thematic components of these literatures. Through the lens of comparative analysis, this paper challenged the stability of currently existing cyber threat intelligence cycles and definitions by a thematic analysis of various cyber security white papers and academic literature. Qualitative analysis equally permitted to have an insider view of the field and forge subjective opinions which allowed for ambiguity, contradiction, and the generation of new ideas. Moreover, drawing conclusions on such a wide variety of renowned academic and grey literature encompassing all fields added to the strength of the research.

The first sections of this paper demonstrated how clearly defining a concept is a big step towards the creation of a cyber threat intelligence model as it lays solid theoretical foundations. This paper has provided a concise definition of cyber threat intelligence and identified factors/points that would help design an efficient cyber threat intelligence cycle from the perspective of the enterprise. This innovative model saw the use of known concepts/tools, which had not been incorporated altogether in an enterprise cyber threat cycle before, such as the cyber kill chain, cyber human intelligence (cyberHUMINT) collection which depicts the behavioural dimension of cyber attacks, multi-discipline collection strategy that occurs across land, air, sea, space domains and in the dark web, counter-intelligence - because cyber attacks especially on businesses are the result of wilful and well organised intelligence gathering, and the use of a diverse intelligence team in order to help reduce bias. This was followed by a clear method that can be used to validate or test the proposed threat cycle.

All in all, this paper was aimed at improving the understanding of cyber threat intelligence by providing a definition of cyber threat intelligence and a model for its creation process in the context of enterprise cyber security. By addressing the lack of consensus, clarity, and academic literature, this paper will not only stimulate the academic debate in the field but equally help in supporting businesses that are willing to use cyber threat intelligence in their organisation in order to improve their defensive posture thereby partly contributing to the general safety of the cyber domain, by ricochet. Even if there is no consensus on the definition of cyber threat intelligence, like other forms of intelligence, nevertheless this paper will help companies understand cyber threat intelligence in a way that is specific/relevant to them.

References

"CIA Observes 50th Anniversary of Original Headquarters Building Cornerstone Laying". *Central Intelligence Agency*, https://www.cia.gov/news-information/featured-story-archive/ohb-50th-anniversary.html (Accessed: May 24, 2020).

451 Research, "Threat intelligence", *451 Research*, LLC. (2014)

A. Frini and A.-C. Boury-Brisset, "An intelligence process model based on a collaborative approach" *Defence Research & Development Canada, no. Paper 113*, (2011): 1–49

Ackoff, Russell L. *The design of social research*. (Chicago: University of Chicago Press, 1953)

Alexander Babuta, Marion Oswald, and Ardi Janjeva, "Artificial Intelligence and UK National Security", *Royal United Services Institute for Defence and Security Studies (RUSI)*, (April 2020)

Arenas, Edilson, "Cyber Threat Intelligence Information Sharing", *Conference Paper, Central Queensland University*, (2017)

Arnould E., Hevner A., S. T. March, & J. Park, "Design Science in Information Systems," *MIS Quarterly, vol. 28, no. 1, (2004)* pp. 75–105

Barnum, S., "Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIXTM*)*", *MITRE Corp*. (July 2014): pp. 1–20

Bimfort, Martin T. "A Definition of Intelligence." *CIA*, May 8, 2007. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm. (Accessed: May 27, 2020)

Brett van Niekerk et al. “An analysis of selected cyber intelligence texts”, *18th European Conference on Cyber Warfare and Security, At Coimbra, Portuga*l, (2019)

Bryman, Alan, & Emma Bell, *Business research methods*, (Cambridge: Oxford University Press, 2011)

Burnham, Peter et al. *Research Methods in Politics*, (United Kingdom: MacMillan Education UK, 01 August 2008)

Cabinet Office, ‘The UK cyber security strategy: protecting and promoting the UK in a digital world’. Crown Copyright, (2011)

Cambridge Dictionary, “Definition of Intelligence”, https://dictionary.cambridge.org/dictionary/english/intelligence, (Accessed: May 23, 2020)

Checkpoint, “Threat Intelligence,” (2019). https://www.checkpoint.com/products-solutions/threat-intelligence/ (Accessed: June 10, 2020)

CISCO, “The Security Bottom Line: How much security is enough?”, October 2019.

Claude Draude, Goda Klumbyte and Phillip Lücking, “Situated algorithms: a sociotechnical systemic approach to bias”, *Emerald Insight*, (September 2019)

Control Risks, “Cyber Threat Intelligence; Actionable insights to help you understand the cyber threat.” https://www.controlrisks.com/our-services/creating-a-secure-organisation/cyber-security (Accessed: June 10, 2020)

CREST, “Cyber security incident response guide”, *CREST (GB), Version 1,* (2013) CREST, “Understanding Cyber Threat Intelligence Operations”, *CREST Intelligence-Led Testing, Bank of England, version 2,* (2016)

Daniil Davydoff, “Rethinking the Intelligence Cycle”, *ASIS International*, (2017)

David Emm, “APT Review: what the world’s threat actors got up to in 2019”, *Kaspersky*, (2019). https://securelist.com/ksb-2019-review-of-the-year/95394/ (Accessed: June 10, 2020)

David, Chismon & Martin Ruks, “Threat Intelligence: Collecting, Analysing, Evaluating,” *MWR Infosecurity*, (2015)

Denscombe, M. *The Good Research Guide: for small-scale social research*. (McGraw Hill, 2010)

Duvenage, PC, and SH Von Solms. "Cyber Counterintelligence: Back to the Future." *Journal of Information Warfare 13*, no. 4 (2014): 42-56www.jstor.org/stable/26487466. (Accessed June 14, 2020)

Eric M. Hutchins et al., “Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains” *Lockheed Martin Corporation*, (2011)

European Cybercrime Centre, “Internet Organised Crime Threat Assessment”, *EUROPOL, (2018)*

Eurostat, “Power from Statistics: data, information and knowledge”, *Eurostat statistical report* (2018)

Federation of American Scientists, “The Intelligence Cycle”. Fas.org, https://fas.org/irp/cia/product/facttell/intcycle.htm, (Accessed: June 2, 2020)

Geoff Hancock, Christian Anthony, and Lincoln Kaffenberger, “Tactical Cyber Intelligence”, *Intelligence and National Security Alliance (INSA)*, (December 2015)

Gerring, John. *Social Science Methodology: A Unified Framework*, (Cambridge University Press, 2nd ed. 2012)

Gibbs, S., "Shadow Brokers Threaten To Unleash More Hacking Tools." *The Guardian, May 2017.* https://www.theguardian.com/technology/2017/may/17/hackers-shadow-brokers-threatens-issue-more-leaks-hacking-tools-ransomware. (Accessed: June 10, 2020)

Gibson S.D. "Exploring the Role and Value of Open Source Intelligence" In *Open Source Intelligence in the Twenty-First Century. New Security Challenges*, Hobbs C., Moran M., Salisbury D. (Eds). (London: Palgrave Macmillan, 2014)

Glass, Robert, Philip Davidson, *Intelligence is for Commanders*, Harrisburg, Pennsylvania: Military Service Publishing Company, 1948

Hakim, Catherine, *Research design: successful designs for social and economic research*, (London: Social research today. (2nd Re). Routledge, 2000)

Hantrais, Linda. *International comparative research: theory, methods and practice*, (Basingstoke (England): Palgrave Macmillan, 2009)

Hewling Moniphia, "Cyber Intelligence: A Framework for the Sharing of Data" *International Conference on Cyber Warfare and Security*, (2018)

InfoArmor, "Threat Intelligence vs. Threat Information", (2019) https://www.infosecurityeurope.com/__novadocuments/362143?v=636312780187970000 (Accessed: June 10, 2020)

INSA, "Operational levels of cyber intelligence". *Intelligence and National Security Alliance*, (2013)

Intelligence as a Science," Studies in Intelligence", Vol. 2, No. 2 (Spring 1958)

J. Richards, “Pedalling hard,” in *Understanding the Intelligence Cycle*, 1st ed., M. Pythian, Ed. Oxfordshire: Routledge, 2013.

James A. Lewis, ‘‘Raising the Bar for Cybersecurity,*’’ Centre for Strategic and International Studies, Washington, DC,* (2013)

Jeff Williams, C.*, Interview: Ed Alcantara, CSO Of Darknet Blackops Intelligence*. Contrastsecurity.com. (2015). https://www.contrastsecurity.com/security-influencers/episode-28-ed-alcantara (Accessed: 9 June 2020)

Jellenc, E, “Unpublished research materials”, *VeriSign-iDefense, Inc*. (2013)

John Robertson et al. *Darkweb Threat Intelligence Mining*, (Cambridge University press, 2017)

Jorl Kalkman, Lotte Wieskamp, “Cyber Intelligence Network: A Typology”, *The International Journal of Intelligence, Security, and Public Affairs, 21:1, 4-24,* (April 2019)

Kapuria, S, “IT threat intelligence to anticipate, stop and counteract targeted attacks”, *Symantec Corporation*, (2011)

Kathleen Kuczma, Briana Manalo, “Criminal Underground Continues to Target Microsoft Products”, *Recorded Future*, (2019).

Kelly, Gail P., Altbach, Philip G. & Arnove, Robert F. “Trends in comparative education: a critical analysis.” In *Comparative education*, edited by Altbach, Philip G., Arnove, Robert F. & Kelly, Gail P, 505-535, New York: Macmillan; London: Collier Macmillan, 1982

KENT, SHERMAN. *Strategic Intelligence for American World Policy,* (PRINCETON, NEW JERSEY: Princeton University Press, 1966) doi:10.2307/j.ctt183q0qt. (Accessed May 24, 2020)

Knightley, Phillip, *The Second Oldest Profession. Spies and Spying in the Twentieth Century*, (W. W. Norton & Company, 1986).

Lijphart, Arend. *Comparative politics and the comparative method*, (American political science review 65(3), 1971), 682-693

Lor, Peter Johan, *International and Comparative Librarianship*, (Berlin, Boston: De Gruyter Saur, 2019)

Lowenthal, Mark, *Intelligence: from Secrets to Policy*, Washington, D.C.: CQ Press, 4th Edition, 2009.

M. Warner, "The past and future of the Intelligence Cycle," in *Understanding the Intelligence Cycle*, 1st ed., M. Pythian, Ed. Oxfordshire: Routledge, 2013.

Maria Henriquez, "The Top 12 Data Breaches of 2019", Security Magazine, (December 2019). https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019 (Accessed: June 10, 2020)

McIntyre, Donald, "Bridging the gap between research and practice", *Cambridge Journal of Education*, 35:3, (2005): 357-382

McLean, Rob, "These Companies Plan to Make Working from Home the New Normal. As in Forever," CNN Business, (June 25, 2020). https://edition.cnn.com/2020/05/22/tech/work-from-home-companies/index.html. (Accessed: July 7th, 2020)

McLeod, Saul. "Qualitative vs Quantitative Research: Simply Psychology." *Qualitative vs Quantitative Research | Simply Psychology*. https://www.simplypsychology.org/qualitative-quantitative.html. (Accessed: May 16, 2020.)

Merriam-Webster Dictionary, "Definition of Intelligence", https://www.merriam-webster.com/dictionary/intelligence, (Accessed: May 23, 2020)

Michael Warner, "Wanted: A definition of Intelligence", *CIA*, (April 2007) https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html#author1 (Accessed: May 26, 2020)

N. Quarmby and L. J. Young, *Managing Intelligence: The Art of Influence*, (Federation Press, 2010)

National Cyber Security Centre (NCSC), *Annual Review 2019*, UK Government, (2019)

NATO, "AAP-06; NATO Glossary of Terms and Definitions," *Allied Joint Publication*, (2014)

Nussbaum, H. Brian, "Communicating Cyber Intelligence to Non-Technical Customers?" *International Journal of Intelligence and CounterIntelligence*, 30:4, (2017): 734-764

Oxford dictionary, "Definition of Intelligence",   Lexcio dictionary for free English, https://www.lexico.com/definition/intelligence, (Accessed: May 23, 2020)

Parkes, A. "Lessons through reform: Australia's security intelligence." *The International Journal of Intelligence, Security, and Public Affairs*, 19(3), (2017): 157–170.

Pennings, Paul, Keman, Hans, & Kleinnijenhuis, *Doing research in political science*, (London; Thousand Oaks (CA): Sage Publications, Jan. 1999)

Peter Gill, Mark Phythian, *Intelligence in an insecure world*, (Polity, 2nd Edition, 2012)

Pickard, Alison J. *Research methods in information*, (London: Facet Publishing, 2007)

Polanyi, Michael, *The Tacit Dimension*, (Chicago: University of Chicago Press, 1966)

Punch, K. *Introduction to Social Research: Quantitative and Qualitative Approaches*, (London: Sage, 1998)

Ragin, Charles C. *The comparative method: moving beyond qualitative and quantitative strategies,* (Berkeley (CA): University of California Press, 1987)

Richard J. Heuer, *Psychology of Intelligence Analysis*, Centre for the Studies of Intelligence, (1999): Chapter 9. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-andmonographs/psychology-of-intelligence-analysis. (Accessed: June 10, 2020)

Robert M. Clark, *Intelligence Analysis a Target Centric Approach,* (London: CQ Press, 4th Ed. 2013)

Robert M. Clark. "Intelligence Collection", (Washington D.C.: CQ Press, 2014)

Rudner, M, "Cyber-threats to critical national infrastructure: An intelligence challenge". *International Journal of Intelligence and CounterIntelligence,* 26(3), (2013): 453–481

Sara Qamar et al. "Data-driven analytics for cyber threat Intelligence", *Elsevier*, (2017)

Sartori, Giovanni. "Comparing and miscomparing." *Journal of theoretical politics* 3(3), (1991): 243-357

Shackleford, "Who's using Cyber Threat Intelligence and How?" SANS Survey, no. 1, (2015).

Sid Snitkin, "*Critical Industries Need Active Defence and Intelligence-driven Cybersecurity*" https://dragos.com/wp-content/uploads/ARCViewDragos-01.pdf (Accessed: 30th Oct. 2019)

Steele, Robert, “Human Intelligence(HUMINT): All Humans, All minds, All the Time”, Strategic studies institute, June 2010, https://phibetaiota.net/2011/11/reference-human-intelligence-humint-all-humans-all-minds-all-the-time-full-text-online-for-google-translate/ (Accessed: May 28th, 2020)

Striphas T., “Algorithmic culture*”, European Journal of Cultural Studies*, Vol. 18 Nos 4-5. (2015): p. 395

Tounsi, Wiem, “What is Cyber Threat Intelligence and How is it Evolving?”, *Institut Mines-Telecom*, (April 2019)

Troy Mattern, John Felker, Randy Borum & George Bamford, “Operational Levels of Cyber Intelligence” *International Journal of Intelligence and CounterIntelligence*, 27:4, (2014)

UK Ministry of Defence, “Understanding and Intelligence Support to Joint Operations (JDP 2-00),” *Joint Doctrine. Publication*, (2011)

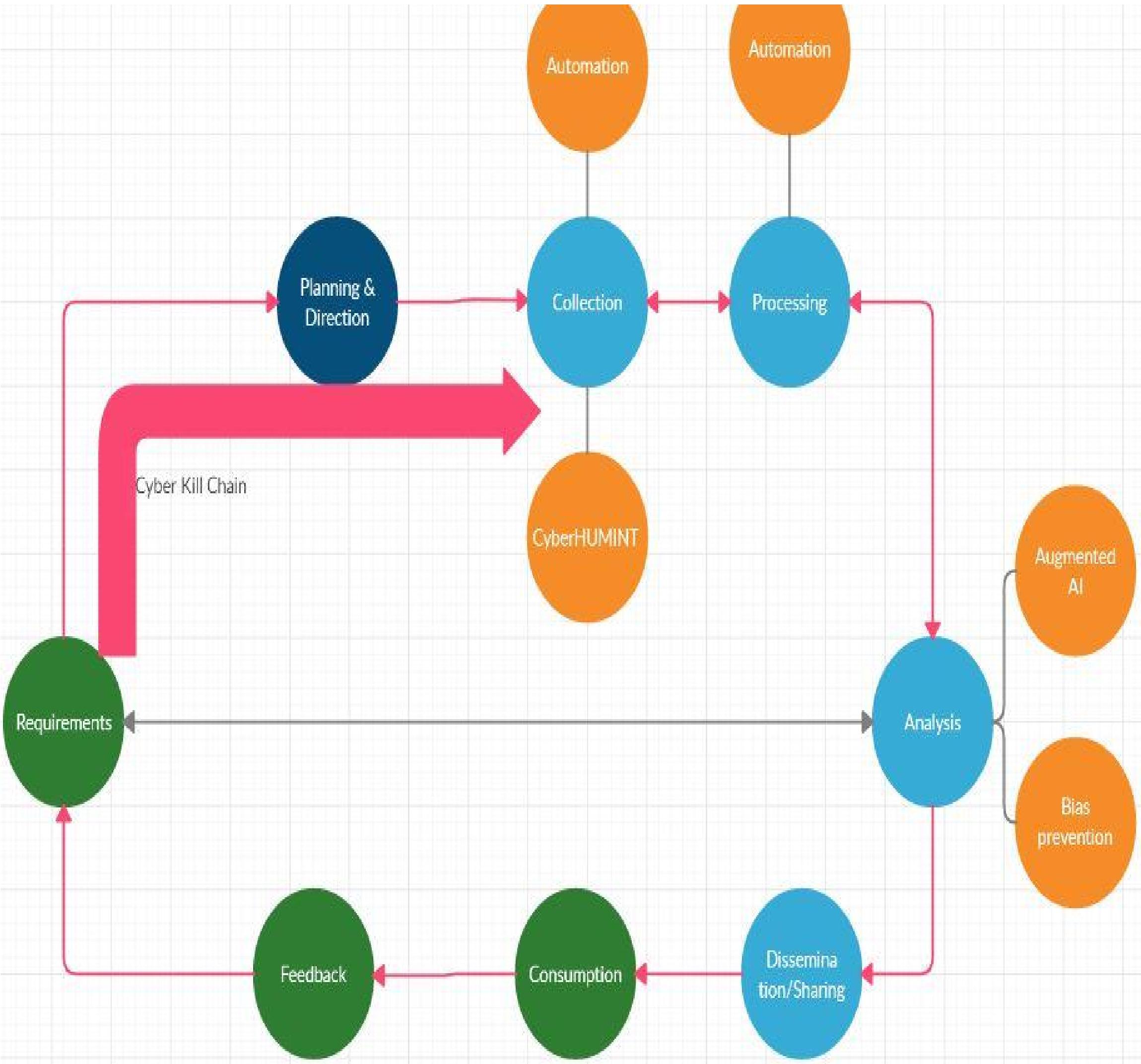
US Army, ‘Field Manual 3–38: cyber electromagnetic activities’. Department of the Army, (2014)

US DoD, “Department of Defence Dictionary of Military and Associated Terms,” *US DoD*, (June 2015): 1–513

V. Goel and N. Perlroth, “Yahoo Says 1 Billion User Accounts Were Hacked,” *Washington Post, 2016*. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0. (Accessed: June 10, 2020)

Zane Pokorny, *The Threat Intelligence Handbook*, (Annapolis: CyberEdge Group, LLC, 2019), https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/ (Accessed: May 31st, 2020)

APPENDIX A – Proposed cyber threat intelligence cycle


Automation
Automation
Planning & Direction
Collection
Processing
Cyber Kill Chain
CyberHUMINT
Augmented AI
Requirements
Analysis
Bias prevention
Feedback
Consumption
Dissemina tion/Sharing