Cyber Threat Intelligence

From confusion to clarity; An investigation into Cyber Threat Intelligence

Daan Planqué

Date:	20th of January 2017
First supervisor:	Sergei Boeke
Second supervisor:	Jan van de Berg
Student number:	660591

Abstract

As the number of threats originating from the cyber domain grows it helps to have a clear understanding on what these threats precisely are and how one could defend against them. A concept often lauded to provide these insights is Cyber Threat Intelligence (CTI) were it not that it lacks a clear definition. This fact, in combination with an absence of academic literature clarifying the concept, and companies using the term to distinguish their products, leads to confusion for the companies wanting to use it. To take a first step in clarifying the concept and reducing the confusion, this thesis proposes a definition of the term and a model of how it could be used.

Table of Contents

Abbreviations

Abbreviation	Description
AIVD	Algemene Inlichtingen- en VeiligheidsDienst
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CISO	Chief Information Security Officer
C-Level	Management level of CEOs, CFO, CTO, etc
CND	Computer Network Defense
CPNI	Center for the Protection of National Infrastructure
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DNC	Democratic National Comittee
DNS	Domain Name System
FBI	Federal Bureau of Investigation
FIRST	Forum for Incident Response and Security Teams
GCHQ	Governmental Communications HeadQuarters
HUMINT	Human Intelligence
JDP	Joint Doctrine Publication
MI5	Military Intelligence Section 5
MI6	Military Intelligence Section 6
MoD	Ministry of Defense
NATO	North Atlantic Treaty Organization
NCSC	Nationale Cyber Security Centrum
NDN	Nationale Detectie Netwerk
NSA	National Security Agency
RFI	Request for Information
SIGINT	Signal Intelligence
STIX	Structured Threat Information Expression
TTP	Tactics, Techniques, and Procedures
U.S.A.	United Stated of America
UK	United Kingdom
UN	United Nations

1. Introduction

In the last couple of years, and especially the last couple of months, Cyber security has gained increasing amount of media attention. One only needs to look back a couple of months to find some of the largest stories. In September there was the 655 Gbps[1] Distributed Denial of Service attack against the website of Brian Krebs, a freelance journalist specialized in cyber security[1]. Or, two days later, the 1Tbps[2] Distributed Denial of Service attack against OVH hosting[2]. Then there was the hack of the Democratic National Committee (DNC)[3] in June, Yahoo announcing in December that 1 Billion user accounts were compromised in an attack in 2013[4], and the release of multiple NSA hacking tools by the Shadow brokers team in August of 2016 and January of 2017 [5], [6]. This attention has not only spooked governments[7], [8] but also companies who are suddenly faced with the growing threats emanating from the cyber domain.

The countermeasures required to defend against these threats will vary depending on the company and its specific situation. A regional bank in Ghana faces different threats than a company building cars in the U.S. To help companies respond to their specific threats and make an informed decision on which countermeasures to deploy first, a new concept called Cyber Threat Intelligence (CTI) is often heralded as the ultimate solution. CTI is often sold as a service that, once you use it, will allow you to "Gain a deep understanding of cyber threats" and to "understand the cyber threats to your company"[9]. Furthermore, no matter who's service you adopt it will provide an 'unsurpassed visibility into global threats' and other golden mountains[10]. The idea being that it will help in making an informed decision and, eventually, improve a company's defense against threats emanating from the cyber domain.

To give some sense of scale: A 2015, global, cross-sectoral survey from the SANS Institute stated that, of the 326 respondents, 85% already are using or are planning to start using CTI for detection and response[11, p. 9]. However, what is never explained is if a dedicated team is required to do CTI, and if so, how do you use it? Neither is clear what exactly the scope of that CTI team should be: do they also mitigate the threats they find or do they only provide intelligence? This lack of clarity regarding what constitutes as CTI and how it should be used is not only seen within the companies that want to utilize CTI, but also when comparing the vendors selling it. A quick Google search on the term "Cyber Threat Intelligence" will provide you with more than 270.000 hits and a long list of companies that sell it as a service. These companies, however, do not all sell the same products even though they use the same terminology. For example, Fireeye provides 'relevant, actionable intelligence tailored to your security mission' which translates into six different intelligence products such as tactical, executive, operational, vulnerability, fusion, or motivation-based intelligence. All six of these products are based on processed and classified data that allow the customer to prioritize which actions need to be taken based on the threat profile of your company[12]. Checkpoint, on the other hand, is a company that also sells a CTI product. However this product only consists of a data feed which the customers themselves need to turn into intelligence[13]. LookingGlass Cyber Solutions also provides these data feeds but instead of calling it a CTI feed they have called it 'Machine Readable Threat Intelligence'. The company also provides a Threat Intelligence service but instead of producing a report, as Fireeye does, it delivers personnel that 'fill in the gaps in your threat

[1] Gigabit per second
[2] Terrabit per second

intelligence operations'. This product is the aptly named 'Cyber Threat Intelligence Group'[14]. Besides these companies there are also CTI products offered by Crowdstrike, Kaspersky, Verisign, Microsoft, Cisco, Surfwatch, and other smaller parties, who all have their own version of what constitutes as CTI and what a CTI product should look like. These different variations make it difficult for those companies who do not know which CTI services they need and frustrating for those trying to find what they want.

Unfortunately, the confusion does not end there as buying a product is only part of the work. The company will need to figure out what goal they want to achieve with the intelligence they receive. Does the company only buy a product that delivers reports to the C-Levels who in turn can act upon the given information or does it want to set up its own department to create intelligence for the entire company? If so, this leads to other questions such as how many people do you need and how should this intelligence creation process work?

In an effort to answer these questions, on what constitutes as CTI and how it should be operationalized, a logical step for these companies would be to look into the literature already present. The problem being that this literature has either been written by commercial parties who want to sell their products or are personal opinions on blogs [15]–[17]. A second logical avenue for these companies to follow would be to look at organizations that have been creating intelligence for years; i.e. the national intelligence agencies such as: CIA, FBI, Mossad, AIVD, MI5, MI6, etc. Because nation-state intelligence has been around for decades, if not longer, and their processes and definitions have been publicized and studied by the academic world, one might expect a certain level of quality. An example of such literature is a book by Robert M. Clark[3] on intelligence analysis which not only discusses the techniques and procedures but also personnel considerations and how to manage an intelligence department[18]. However, what becomes clear from Clark's work is that even in such a seemingly established domain there is no consensus regarding the definition of the term intelligence. This is not only illustrated by the website of the CIA, where on two different occasions the discussion on the term intelligence is summarized and a new definition proposed[12],[13] but also in work from Sherman Kent[21] and Mark Pythian[22], who are both specialists on the field of intelligence.

This lack of consensus can also be seen in a quote from the secretary general of the United Nations, Kofi Annan. When in 2000 he tried to improve the intelligence capabilities of the UN it was the lack of clarity about what constitutes intelligence which launched a controversial and complex debate: "*What some viewed as information-collection was considered intelligence-gathering by others, and what was called "strategic intelligence" by some was labeled "espionage" by others*"[23]. Additionally, this lack of consensus also extends to the model that describes the process of intelligence creation, referred to as 'the intelligence cycle'. This debate has even gone so far that multiple authors have worked together and written a book that explains what is wrong with the cycle and proposes multiple solutions for the problems they identify[24].

The end result is that for a company trying to understand how CTI works and how to operationalize it, these discussions only add to the initial confusion that the companies selling the service have created. Moreover, this lack of clarity not only hinders the adoption of CTI, but also benefits the adversaries due to the investment in time and money required to properly

[3] Robert M. Clark was previously a senior CIA analyst and now teaches graduate courses on intelligence at Johns Hopkins University and the University of Maryland.

design, build, and use the process. Money that could be used to buy and implement other defensive countermeasures. Lastly, for the companies that do use CTI, cooperation is made difficult due to the different definitions and interpretations each company uses when talking about the subject. If CTI is ever to be a security measure that even the smallest companies can benefit from will require a clear and concisely specified concept.

1.1.1. Research Question

In solving these problems there is a role for academia to provide clarity and stimulate innovation. As prof. John Gerring, an expert in the field of social sciences regarding methodology and comparative politics, states in his book on Social Science Methodology:

"Concepts are integral to every argument for they address the most basic question of social science research: what are we talking about"[25, p. 112]*?*

Therefore, the goal of this thesis is to help companies integrate CTI into their defensive cyber security portfolio by clarifying the concept of CTI and how it might be used. To do this this thesis will answer the following research question:

How could the CTI process be modelled from the perspective of an enterprise?

However, before it is possible to create a model of the process a definition is required as defines the context of the term CTI. To do this the following research sub-question will be addressed:

How could the term CTI be defined from the perspective of an enterprise?

1.1.2. Structure of Thesis

The previous chapters have already given an introduction into the subject at hand, the relevance, and the scope of the research being done in this thesis. This thesis is structured as follows: the next chapter will explain on which assumptions the research is based, which method is used, and how this method was executed within the analysis. The following chapters will present a literature analysis in order to come to a definition of CTI. Furthermore, this analysis will be the basis on which this thesis presents its own proposal of how the process for intelligence creation should be modelled. This is followed by a chapter on the validation of the proposed model. Closing off the document is the answer to the research question, a conclusion, and advice for the next steps.

2. Methodology

2.1.1. Assumptions

The author of this thesis has a technical background in telecommunications and electrical engineering, and is currently employed at the Dutch telecommunications company, Koninklijke KPN NV. (KPN), as a member of the threat intelligence team within the CISO[4]. While a potential bias might be present in how the author approaches the research aim of this thesis, this professional expertise also allows for a better understanding of the perspective of an enterprise and a stronger grasp of the operation, complexities, requirements, and problems.

An important aspect that should be considered when addressing the research questions of this thesis is that every enterprise is not only different both in size and internal hierarchy but also in the products they deliver, their long and short term goals, and the sector they are part of. Each of these factors will influence the scope of the company and therefore their requirements for a CTI team. For example, a 50-man company producing a highly-specialized product has different requirements for the focus of the team but also on what resources are available to support them. When comparing this to a multi-national with many different products in different sectors and a multi-billion-dollar profit margin the scope of the CTI team can be considerably larger as the resources available are higher. For example, KPN is a telecommunications company that not only sells telecommunications and cloud services to customers in The Netherlands but also provides (tele)communication services to most, if not all, parties who are part of the critical infrastructure of The Netherlands. This means that the CTI team not only protects the financial status of the company but also has an important role in the safety and continuity of the country itself.

Lastly it must be mentioned that the author is only fluent in Dutch and English meaning that any sources not written in these languages have been excluded from the research.

2.1.2. Execution

As stated in the previous chapters, the goal of this thesis is to reduce the confusion about CTI for it to be of use for an enterprise. The cause of this confusion seems to be due to the lack of clarity on the concept of what CTI is and what it entails. Therefore, as mentioned in the research question, this thesis will look at how the concept can be defined, and how the intelligence creation process of CTI be modelled. To achieve this, each research question has been split into two parts, where the first is a comparative literature analysis and the second presents a proposal for either a definition or a model.

Both comparative literature analyses are based on academic literature originating from the field of intelligence, and so-called 'grey' literature on CTI such as white papers and blogs. While the chosen types of literature have certain limitations pertaining to their applicability to the field of CTI, their teachings can, with these limitations in mind, be translated to the domain of CTI. To be able to distil these teachings into a usable artifact, attributes will be used to generalize the document. To help identify which attributes are required for a clear and concise definition of CTI, two factors will be used in a comparative analysis. The first parameter is that of

[4] The CISO within KPN department is where all parties responsible for corporate IT security, such as the CERT and redteam, are located.

context: who wrote the definition and with what reasoning the term should be interpreted and the context in which it should be used. The second parameter identifies the key attributes of the different definitions. These attributes, in combination with the context, will be analyzed in order to determine which of these attributes a definition of CTI needs to cover. Based on this analysis, the chapter will propose a definition.

To help define the factors required for a model the literature analysis will not, as with the definition, define the context and its attributes. Instead, the discussion on the failures of the intelligence cycle, and the current model for intelligence creation in the intelligence sector, will be used to define which factors a model the intelligence creation process for CTI requires. These factors are distilled by analyzing different pieces of academic literature that discusses the flaws on the intelligence cycle. This identified flaws will be used to design a proposal of an intelligence creation process that can fulfill the need of a company. Due to the limitations regarding time and scope, this thesis cannot validate the proposed model. However, it will elaborate on which factors must be included when validating the model at that later moment in time.

3. Literature analysis as basis for a definition

By clarifying the definition of CTI, this thesis not only gives an insight into the nuts and bolts of the CTI domain but also sets the scope for the model investigated later in this thesis. As current academic literature on the subject is scarce and grey literature doesn't provide a consensus on what it might be an investigation is required. To help in this, this thesis will investigate a set of documents that all provide a definition of intelligence. The selected documents were chosen on how often the documents and authors were referenced in regards to this discussion, the experience and knowledge of the authors, and insofar they were unique in what they added to the discussion. This means that there might be a brilliant definition of intelligence but if it, or its author, was not referenced in other documents it would not be used. This was also done in regards to uniqueness as it makes no sense to analyze fifteen definitions that do not bring anything new to the analyses. The resulting documents will be analyzed for context and which key attributes they exhume. Based on these two factors a proposal for CTI will be built in the following chapter. To start off this investigation five English dictionaries have been analyzed for their interpretation of the term intelligence.

3.1. Dictionaries

When one does not know what a particular word means, a logical place to start is a dictionary. One might expect that every language has only one dictionary, and there might be countries where this is the case, but for UK English, there are many. Then there are also the sector specific dictionaries that provide a context specific definition. Due to its focus on the intelligence sector and due to it being internationally accepted, one of these dictionaries is included in this analysis. Note that only the definitions pertaining to intelligence in the scope of this thesis are presented and that others pertaining to other subjects such as human intelligence or artificial intelligence are excluded.

The first definition is from the Merriam-Webster dictionary who defines intelligence as two things namely[26]:

"information concerning an enemy or possible enemy or an area;"

and

"*an agency engaged in obtaining such information".*

The Cambridge dictionary defines intelligence as[27]:

"a government department or other group that gathers information about other countries or enemies, or the information that is gathered".

The Collins dictionary[28] defines intelligence as two things namely:

"*military information about enemies, spies, etc*"

and

"*a group or department that gathers or deals with such information*"

And lastly the Oxford dictionary[29] defines intelligence in three parts as:

"The collection of information of military or political value"

and

"People employed in the collection of military or political information"

and

"Military or political information"

The context of these definitions are a reflection of what the term means in this day and age. They reflect what 'the people' think what the term intelligence entails. How this has come to be is a study for another time and another field and could influence the context but here it is assumed that dictionaries are, in principle, not biased and therefore contextually neutral.
However, when one studies the different definitions a pattern arises. Every definition makes a reference to intelligence being either political or military in nature. This can be seen in the definitions that use the words 'political' or 'military' in the definition, but also in the references to 'spies' or 'other countries'. Also, relations to physical locations such as 'an area', or the use of 'enemies' is, in this context, nation-state based and not normally used when describing an attacking party in the cyber domain. An example of this is can be seen in how actors in cyberspace are described by the STIX[5] notation; *"actors are a group of people with tactics, techniques, and procedures, physical location is not part of the equation*"[30]. Here, the attackers are described as adversaries or actors, and not as enemies which has a much more physical and warlike connotation.

To summarize, due to the choice of words all dictionaries stated above present a definition of either military or national intelligence that cannot easily be taken out of context and used to describe CTI. For the proposed definition, the choice of words that do not have this military or political connotation will be important.

The NATO[31] definition of intelligence, as documented in their 'Glossary of Definitions and Terms', which is also used by the United States' Department of Defense[32] and the Dutch Department of Defense[33][6], is sector specific and consists of three parts:

> *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.*
>
> *The activities that result in the product.*
>
> *The organizations engaged in such activities. See also acoustic intelligence; all-source intelligence; communications intelligence; critical intelligence; domestic intelligence; electronic intelligence; foreign intelligence; foreign instrumentation signals intelligence; general military intelligence; imagery intelligence; joint intelligence; measurement and*

[5] STIX is a syntax for documenting (cyber) threat intelligence indicators which describe an attacker such as IPs or Hashes. For more information, see the reference at the end of the quote.

[6] The UKs Ministry of Defense states, in their Joint Doctrine Publication on Intelligence: JDP 2-00v3, that they following NATOs doctrine. However, JDP 2-00v3 does not contain a singular definition of 'intelligence'. Instead each different discipline, category, or level of intelligence has its own definition – an example of this is medical intelligence.[34]

signature intelligence; medical intelligence; national intelligence; open-source intelligence; operational intelligence; scientific and technical intelligence; strategic intelligence; tactical intelligence; target intelligence; technical intelligence; terrain intelligence.

That these definitions area clearly written within a military context is not surprising and can also be seen in the introduction of the document:

"[..] supplements standard English-language dictionaries and standardizes military and associated terminology to improve communication and mutual understanding within DOD, with other federal agencies, and among the United States and its allies"[32, p. 3].

Furthermore, this can also be seen in the definition as a reference is made to "*areas of actual or potential operations".*

Of note is that the definition is more a description of the intelligence creation process where the output of the process "*the product resulting from.."* has as scope the military domain. This can be seen in the final part of the definition:

"*concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations".*

This scope differentiation can also be seen in the definitions of the different types of intelligence mentioned in the third part of the definition. There are types of intelligence which can be clustered based on the attribute of time. For example, when analyzing the term strategic intelligence, as noted in the third part of the definition, a reference is made to *"the formation of policy and military plans*" stating a long-term view. Whereas operational intelligence has a much short view on time due to its reference to *"[..] accomplish strategic objectives within theaters or operational areas*". Then there are also definitions which have as attribute that they are a description of the result of analyzing that specific type of information. An example of this is acoustic intelligence: *"Intelligence derived from the collection and processing of acoustic phenomena."* Interestingly this scope setting was already done by the UKs Joint Doctrine Publication on intelligence, JDP 2-00, where a split was made in levels of intelligence (i.e. time-based: strategic, operational, tactical), intelligence disciplines (result focused: acoustic), and one that cannot be found in the NATO dictionary – counter-intelligence[34, p. 41]. This thesis argues that scope is an attribute that must be included when setting a definition for CTI.

3.2. Definitions from the intelligence domain

When you analyze a specific subject and its domain it is not surprising that the work done in that field will use language specific to that domain. This is illustrated when analyzing the definition of intelligence from the perspective of authors experienced and focused on that field. Take, for example, the definition that was written, most likely under a pseudonym, by R.A. Random for the CIA magazine 'Studies in Intelligence':

"Intelligence is 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" [7], [28].

In this definition one can identify a couple of factors that reveal that this definition has a strong governmental scope. The first being the fact that intelligence is used to "*aid in formulating*

and implementing foreign policies", and that information being processed is collected "*on foreign countries"*. This leads to a somewhat similar attribute as with the previously discussed NATO definition, in that it is governmental in nature. The choice of words in this definition only describe the role of a governmental organization and its extraterritorial focus. Due to this, the definition cannot be used for anything else. The same can be said about the definition by M. Warner:

"Intelligence is secret, state activity to understand or influence foreign entities."

Here intelligence is made out to be an activity that only nation states use to be able to understand or influence foreign entities. There is also the fact that both definitions have another descriptive attribute namely that of secrecy. Both definitions state that intelligence is a secret activity; M. Warner call is a *"secret, state activity"*; and R.A. Random not only argues that it is "*secret collection and processing*" but also the "*conduct of covert activities abroad"*. One could argue about whether the intelligence function of a company should or should not be secret. But most companies will not use covert actions to help them defend themselves against attackers in the physical or cyber domain. That being said, there is something important to consider when analyzing these definitions and that is the bias of the authors. M. Warner was an analyst at the FBI's Directorate of Intelligence and wrote his definition in 2002 when he was part of the CIA History Staff[35], [36]. And R.A. Random is, most likely, an employee at the CIA, however this cannot be confirmed[37]. This gives both authors a possible bias as their definitions have been written from the perspective of the CIA. As the CIA is a US intelligence agency and has different roles and responsibilities than, for example the FBI or GCHQ, the definition cannot be used for all national intelligence agencies.

M. Lowenthal, who is currently an adjunct professor at John Hopkins University and has written 6 books and more than 100 articles on intelligence and national security, presents a more generalist definition. In the introduction of his college textbook states that, while not part of the CIA or, as far as can be found, tied to that organization, "*intelligence is a normal function of government"* [38]. This statement is only a precursor for his complete definition:

"Information is anything that can be known, regardless of how it is discovered. Intelligence refers to information 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 analyzed responds to the needs of policy makers, all intelligence is information not all information is intelligence"[38, p. 2].

In this definition one can, again, see that intelligence is a function that supports the functioning of a nation state. This is visible not only in M. Lowenthal's introductory statement, but also by stating that intelligence is processed information to meet the needs of policy makers. However, if one were to replace policy makers with customers the definition loses its governmental focus and clarifies that intelligence is simply analyzed information to meet the needs of that person. This streak of high-level thinking also effects the attribute of secrecy where M. Lowenthal clarifies why secrecy is required:

"[..]Intelligence exists because governments seek to hide some information from other governments, who, in turn, seek to discover hidden information by means that they wish to keep secret."

When explained in such a manner, secrecy can also be part of the definition used by an organization. A CTI team would never want the adversaries to know which intelligence they have about them as that might mean that the adversaries will alter their behavior. This alteration would require the company to reinvest time and money to track these changes and re-gain the initial advantage needed to defend itself against these adversaries.

Having analyzed definitions from both well-known dictionaries and the professional intelligence field, one can identify two key attributes that need to be taken into account when trying to define the term CTI; The first being scope, in that the term intelligence has a governmental connotation and is used to support the creation and execution of foreign policy. The second attribute being that secrecy is an important part of the definition as it is required to keep the advantage that intelligence provides.

3.3. Cyber Threat Intelligence

After finding the attributes of secrecy and scope in the previously discussed literature on the definition of intelligence, a look into what has been written about CTI is warranted. As said before the field is not as well founded as that of governmental or military intelligence meaning that there is a lack of academic literature on the subject. To feed this part of the analysis four definitions were chosen from literature where the author was deemed to be a specialist in the field.

First off is a whitepaper written by MWR, a cyber security consultancy bureau specialized in research, CERT-UK, and the Center for the Protection of National Infrastructure (CPNI)[39], [40]. The goal of the paper was to clarify the terminology, upsides, downsides, and what companies should and shouldn't do if they want to start using threat intelligence. Naturally this requires a definition of what threat intelligence is. The paper presents three definitions of intelligence where each definition builds upon the previous. The first definition is: *"information that can be acted upon to change outcomes."* This definition is very general but explains what intelligence is in a manner that anyone can understand. In the accompanying definition they also refer to the fact that intelligence can be as simple as picking a garage to get your car repaired after reading the specific section in the telephone book. The second definition is more an explanation of what intelligence tries to achieve namely: *"process of moving topics from 'unknown unknowns' to 'known unknowns' by discovering the existence of threats, and then shifting 'known unknowns' to 'known knowns', where the threat is well understood and mitigated"*[41]. And for the third definition they give a definition of threat intelligence:

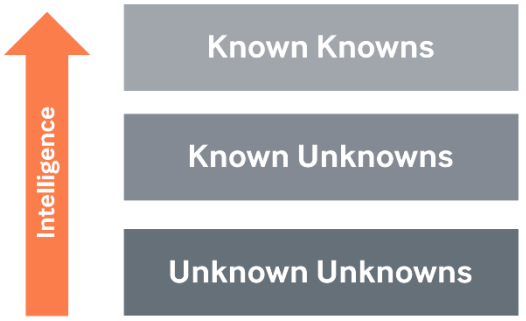

Figure 1 - Process of moving from unknown unknowns to known knowns - MWR report[42]

"*As with traditional intelligence, a core definition is that threat intelligence is 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"*[42].

What it comes down to is that the third definition is an expanded version of their first definition – information that can inform or aid in making decisions however the definition lacks focus and detail of the domain it tries to define. Previously discussed definitions, such as that of

M. Lowenthal or R.A. Random, contain the same concepts but scope it to a specific domain. So, while this definition does not provide any more insight into what threat intelligence entails it does illustrate the argument that a definition should be attributable to a certain domain.
Mr. S. Caltagirone, head of Microsoft Threat Intelligence Analysis team, follows a similar line as document by MWR, with a definition proposed on his blog:

"*Intelligence is the collecting and processing of that information about threats and their agents which is needed by an organization for its policy and for security, the conduct of non-attributable activities outside the organization's boundaries to facilitate the implementation of policy, and the protection of both process and product, as well as persons and organizations concerned with these, against unauthorized disclosure"* [16].

An issue with this definition is that it is meant to define CTI however S. Caltagirone has taken the definition by Martin T. Bimfort of the CIA[19] and translated it to fit the scope of a company. There are, however, a number of problems with the result. The 'conduct of non-attributable activities' is one. Where here 'non-attributable activities' are defined as the type of actions where stealth is used with the goal being physical harm e.g. drones strikes or covert navy seal actions. As said before, there are most likely few, if there are any, companies that will undertake such physically motivated actions to 'facilitate the implementation of policy'. One could also read the definition to be the analyst collecting data which supports the company security policy but that is not inherently clear. The other is the choice of words – the use of 'policy', 'non-attributable actions', and 'agents' give the definition a very governmental connotation. This leads back to the domain attribute – the context in which the definition applies needs to be crystal clear or possibly be misinterpreted to mean something else. Another attribute that this definition also considers is that threat intelligence should be a secret process and is therefore in-line with the previously discussed governmental definitions.
In contrast, the following two sources see things somewhat differently and do not include secrecy in their definition. Robert M. Lee, trainer at the SANS institute on the subject of CTI and specialized in digital forensics and threat intelligence research, proposes the following definition for threat intelligence:

"The process and product resulting from the interpretation of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity and capability to do harm"[15].

In the first half of this definition one can again identify the general definition of intelligence with the processing of raw data into information step being added. The second half of the definition is where the scoping to the domain of CTI can be seen. This can be seen in the fact that the definition is adversary focused where an adversary is described as a party that has *"intent, opportunity and capability to do harm"*.
Michael Cloppert[7] states much of the same in his blog where he proposes his three-part definition of CTI:

[7] Michael Cloppert is of interest here as he now works as Security Advisor at Price Waterhouse Coopers, worked at the Lockheed Martin Computer Incident Response team for 11 years, Is the author of the SANS FOR578 training on CTI together with Robert M. Lee, is one of the authors of the Lockheed Martin paper on the kill chain[55], and has been co-chair of the SANS CTI summit since 2013.

1. “I define Cyber Threat Intelligence Operations as *actions taken in cyberspace to compromise and defend protected information and capabilities available in that domain*”
2. “I define Cyber Threat Intelligence Analysis as *the analysis of those actions and the actors, tools, and techniques behind them so as to support Operations*”
3. “and I define the Cyber Threat Intelligence domain *as the union of Cyber Threat Intelligence Operations and Analysis*..”[17]

The main difference with the definition of Robert M. Lee being that the definition not only considers CTI being used to gain an advantage over the adversary, but that the adversary also uses it to gain an advantage over the defender. This an interesting attribute to consider due to companies normally only being defensive players in cyberspace whereas military and governmental intelligence is done by a party that is also offensive in nature. Another unique attribute that both Cloppert and the previous two authors link to CTI is to gather intelligence and describe the adversary at a high-level. Robert M. Lee does this by defining intent, opportunity, and capability to do harm whereas Michael Cloppert does this by defining more technical aspects such as tools and techniques. While both work to describe an adversary the definition of Robert M. Lee does not work when describing the data gathered of a defender as a defender does not have intent to do harm. Either way, it is an attribute that needs to be considered when defining CTI.

Now that all the different definitions of the three different domains (dictionaries, intelligence, and CTI) have been analyzed, a number of attributes are identified which need to be considered when one wants to define CTI.

- The first being context: one needs to choose terms that clearly and concisely describe the context one is operating in. If this is not done one gets definitions like that of Sergio Caltagirone which can be interpreted in multiple ways and do not clearly define the scope it operates in.
- The second attribute is secrecy: that the intelligence creation process is one where the data created needs to be kept secret to not lose a possible advantage to one’s adversary.
- And finally, to consider the attribute that CTI is not only used by defenders but also by attackers.

4. Setting a definition for CTI

One of the attributes that was identified multiple times during the literature analysis on intelligence definitions is that of context. This was most clearly seen when looking at the definitions from a militaristic or governmental perspective but was also identified in the definitions on CTI. While each definition presented its own perspective of what intelligence is, the different contexts wherein these were generated could be clearly seen. The NATO definition had a focus on the physical domain whereas the intelligence agencies were mostly looking at foreign policy. The problem being that every domain tried to define the same term. This thesis therefore proposes that the discussion on the term intelligence is flawed as each definition is unique in its own context and that therefore each domain should have its own definition. This thesis therefore proposes the following six domains of intelligence:

- Military Intelligence
- Nation-State Intelligence
- Business Intelligence
- Threat Intelligence
- Psychological Intelligence
- Artificial Intelligence.

Between these six domains, another split needs to be made between psychological and artificial intelligence on the one hand, and the other four on the other hand due to not only their scope being different but also area the they focus on. Psychological and Artificial intelligence focuses on a form of intelligence that looks at problem solving by humans or computer systems[8]. The other four options all consider intelligence in the sense that they try to answer one or more question(s) for a specific situation. Therefore, this thesis proposes to cluster them under the term Actionable intelligence which this thesis defines as:

"The result of the process that combines information[9] to answer a specific question."

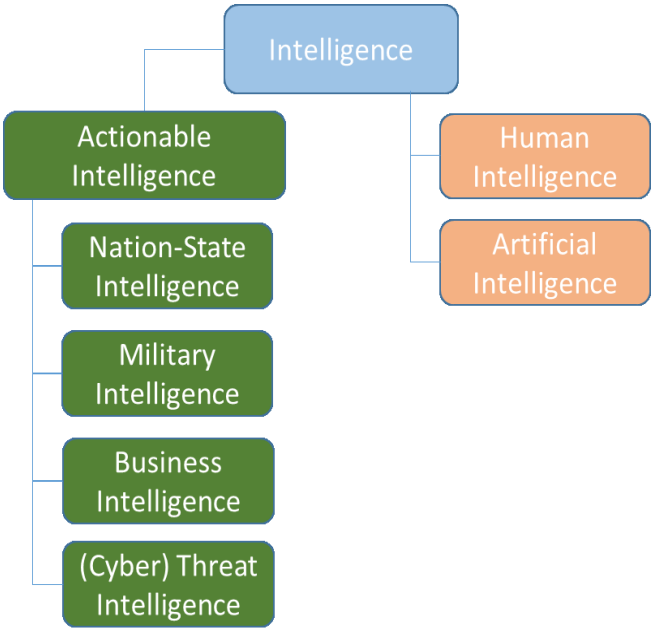

Figure 2 - A definition of intelligence; model of own design

While these four domains try and answer a specific question they share other facets as well. The first being that every domain generates intelligence on the same timelines, namely strategic (long term), tactical (mid-long term), operational (short term), and technical (very short term). These timelines are set by the party requesting the intelligence. However, the only difference between the domains is, again, the context of the answer. An example of this might be Threat Intelligence where, for example, the question is to determine the evolution of

[8] Both artificial and human intelligence will be out of scope for the rest of this thesis as they were only added for completion when discussing the term intelligence.

[9] In this definition, the term information also needs some clarification due to it not always being used in the same way. This thesis follows the principles of data analysis in that information is the result of processed raw data. Where raw data is that which is collected, and stored before being filtered, processed, and structured into a singular format.

attack tools on point-of-sale[10] systems to help a company set priorities when creating its strategic priority. For Military Intelligence the timelines could translate to evaluating the evolution of weapon design to help prioritize the research budget for counter-measures. While both domains want 'intelligence' to help set their long-term goals, the context wherein this is done, physical vs cyber, is different.

A second reason for grouping these domains is that they all make use of open or closed sources to get the information required. Open sources could be patents, news articles, twitter messages, videos on YouTube, or Pastebin pastes. But they could also come from closed sources such as network sensors, logs, or for nation-states and military – espionage. Here again, the principle of data collection is the same but the sources used are specific to the context.

While on the subject of context some clarification is required of what is meant with the definition of each domain. As there are others more knowledgeable about the domains of military, nation-state, and business intelligence, a precise definition for these domains shall not be proposed. Instead what needs to be know is that each domain is separate due to its specific focus. In the third part of NATOs definition it is stated that military intelligence has a strong focus on collecting information which allows the respective party to be superior on the battlefield. This information might entail geological (lay of the land), medical (status of their own or opposing troops), technical (weaponry), etc. Nation-state intelligence, on the other hand, is focused on creating intelligence that makes the nation superior in all other fields of government such as economics, or politics. There might be cases where these two types mix, as with the CIA also doing covert operations such as drone strikes, however this seems to be an exception and not a rule. The context of nation-state intelligence could, in theory, also be compared to enterprise intelligence were it not that an enterprise is only focused on the financial bottom line while a nation is focused on survival of the state. Then there is business intelligence which focusses on gaining the upper hand of other businesses from an economic perspective whereas the goal of (cyber) threat intelligence is to determine physical or cyber threats from internal or external actors against the organization. To be more precise on what is precisely meant, this thesis proposes the following definition for the term CTI:

"The result of the process that combines information to create an overview of an adversary and their intent, tactics, techniques, and procedures"

To come to this definition a combination was made of a definition of intelligence and threat. As seen earlier in this thesis intelligence is the result of processed information. This principle can not only be seen in the definition as discussed earlier in this thesis but is also seen in the following chapters on models for intelligence creation. For the definition of the term 'Threat' the definitions from Michael Cloppert and Robert M. Lee were selectively combined. For example, the terms opportunity and capability were excluded as these are the result of the analysis of an attackers TTP[11] on a specific situation. Additionally, it is this authors view that a threat intelligence team only catalogues threats to the organization. Whereas other teams, such as CERT or Security Strategy, can put this information into context, thereby defining the

[10] Point-of-Sale systems are systems used for financial transactions. An example of such a system is the credit or debit card terminal used for payments at a supermarket.

[11] TTP is an abbreviation for Tactics, Techniques and Procedures which are three terms used to define the different attributes of an attacker.[30]

opportunity and capability of the adversary, due to their situational awareness of the security level of the company and its computer systems. The CERT and Strategy teams are also aware of the changes and projects taking place within the company and can, if required, act to change their scope. Therefore, this thesis argues that threat intelligence teams should not be burdened with this task and let the people who already fulfill this task to act upon the intelligence the threat intel team delivers. An exception could be made for technical intelligence which might, in theory, be directly imported from the intelligence platform into network sensors and blacklists, however this should always be done together with the CERT. A situation where this might be applicable is when tracking a botnet using a fast-flux DNS environment. Meaning that the combination of a domain name and IP address is only valid for a limited time and therefore automation supports the quick response required for implementation and reduces the strain on human engineers for removal/implementation.

The end result is that by giving defining intelligence as a general subject and grouping the actionable intelligence domains will allow the discussion on the definition to be more clearly scoped. This might, for example, help the debate on nation-state intelligence by scoping it to support foreign policy and removing the physical, or military, aspect from the discussion. Additionally, it also helps to clarify that Cyber Threat Intelligence is its own domain with its own scope and therefore requires, and now has, a different definition of the concept.

5. Literature analysis for a model

While a definition tries to explain a phenomenon in language, a model tries to do the same for a process. This model could be an algorithm or, in this case, a graphical representation to show the interworking between different people. For the intelligence process the 'intelligence cycle', as shown in Figure 3**Error! Reference source not found.**, is often used as a description. However, many authors such as Mark Pythian, David Omand, and Arthur S. Hulnick all state that it is either a) not an accurate depiction of reality, or b) it has several flaws that make it ineffective in use[24]. These discussions have led to the creation of a multitude of different models that all try to explain the 'intelligence process'. The goal of this chapter is identify what commentary there is on the classic intelligence cycle to help in setting the requirements for the model of CTI creation.

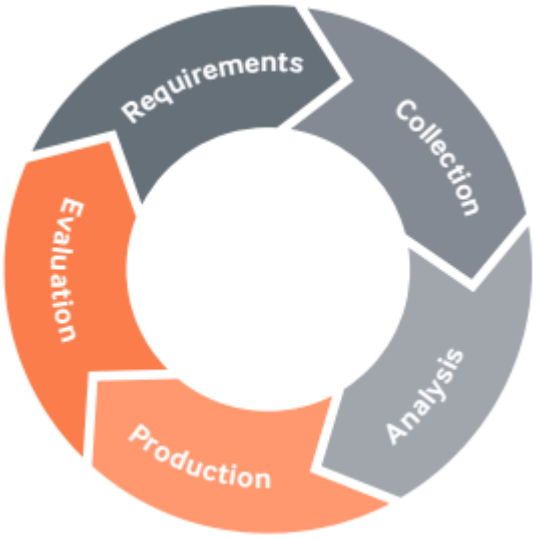

Figure 3 - The 'classic' intelligence cycle; source: MWR report [42]

The author(s) of the classical intelligence cycle[12], as shown in Figure 3, are unknown but Michael Warner, a historian at the CIA[16][21], wrote an article wherein he gives an indication of where it might have originated from. In this analysis, he refers to a document by a Prussian general Carl von Clausewitz who reflected on the task of a general. In this book, called "On War", Clausewitz gives his view on intelligence and argues that a better general would be one that improves the information he receives so as to make better decisions[44, p. 10]. This seems to be the first written indication on the use of intelligence within the military. Dr. Warner also focusses on research done by Kristan Wheaton of Mercyhurst College who, via Google NGrams, found that the first use of the phrase 'intelligence cycle' is mentioned in a book from 1948. This book 'Intelligence is for Commanders' is authored by two US Army lieutenants, Robert R. Glass and Philip B. Davidson, who were, at that time, teaching at the US Army Command and General Staff College at Fort Leavenworth[45]. In this book, Warner argues, the authors present their version of the intelligence cycle consisting of four phases namely "Direction of collection effort, Collection of information, processing of information, and use of intelligence"[45, p. 5]. According to Mr. Wheaton, the explanation presented by Lt. Glass and Davidson indicated that the model was already in use during training of officers in the Second World War.

Another source was found by Dr. Julian Richards in a book by Quarmby and Young who found a reference in a document of the United States[46]. Regrettably Dr. Richards doesn't indicate if this version of the model is any different of that presented by Lt. Glass and Davidson. And as it was not possible to get access to the book by Quarmby and Young it was not possible to verify for ourselves. This thesis therefore presumes, based on a statement by Dr. Richards, that the model is close to identical due to his explanation: "transactional process from a requirement being levied by a policy-maker or intelligence "customer", through the processes of

[12] There are different variations of the classic intelligence cycle containing either 4, 5, or 6 different phases. Here the choice was made to use the five phase variant as an example. The principle behind the model does not change with more or less phases – it is purely for clarity's sake.

collection, processing, and analysis of resultant intelligence data, and back around to the dissemination of the finished intelligence product to the original requestor [47, p. 43].
Whoever first designed the intelligence cycle, it is now the go-to model to explain the process of intelligence creation. Robert M. Clark even goes so far to say that "the intelligence cycle has become almost a theological concept: no one questions its validity."[18, p. 5]. Depending on the author, the model contains either four[48, p. 4], five[49, p. 2] as seen in Figure 3, or even six[18, p. 5] phases. The difference between these different versions is purely visual as the explanation behind what each phase does is almost always the same for both the four-phase model and the six-phase variety.

Each model, as shown in figure 4 through 8, starts off with a process that clarifies the question of the customer, i.e. sets the requirements of the process. These requirements are then translated to a plan on how this question will be answered and who needs to do what. For example, the analyst needs to research the problem and determine what data is already known and what needs to be collected. These two parts are combined in a single step in the four- and five-phase model, whereas the six-phase model has two separate steps. Most likely this is due to the different activities being executed by other parties[48, p. 6]. Next follows the process for the collection of the required data from closed or public sources which is followed by the processing phase. This phase is used as a "pre-analytical stage in which raw information is filtered and readied for analysis via range of techniques including decryption, language translation, and data reduction"[49, p. 3]. The four-phase, as shown in Figure 4, model combines processing with the next phase of analysis. Analysis is where the collected and processed information is combined, including already known information, and turned into intelligence. The resulting intelligence is then vetted by other analysts to prevent the result being skewed due to, for example, bias[34, p. 73] and eventually written into a report during the 'production' phase. The resulting report is afterwards shared with the customer during the 'dissemination' phase in a format that fits the customer's requirements. This could be an email detailing the highlights with the report attached or a special briefing going into the details[18, p. 5]. While not always described, the idea is that the customer will then return with new requirements and complete the intelligence cycle[50].

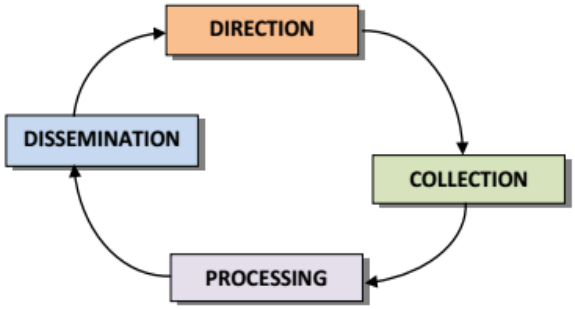

Figure 4 - The Canadian Intelligence Cycle[48]

Although the 'classic' intelligence cycle is the generally accepted model there is a discussion ongoing on its correct and completeness. This discussion has resulted in several models which all propose a way to re-model the classical intelligence cycle in a manner that gives a *"a more complete and accurate representation of all elements of the process as well as the factors that influence them"*[48, p. 9]. The feedback that these models provide will be used as the requirements that the model for CTI creation needs to adhere to.

Dr. Gill and Dr. Pythian propose the model of the 'intelligence web' as shown in Figure 5. In their proposal, they address several items that they find are flawed in the intelligence cycle. First of these is the fact that the intelligence cycle is presented as a closed loop where feedback from the customer is not incorporated. They posit that the model is closed and that therefore interaction with the environment is lacking, and that the intelligence process is not always sequential in nature. A second quality that, they argue, is lacking is the aspect of internal politics such as 'who determines if a threat is still a threat' and 'who determines priorities'. Third, they state that the sequential nature, that analysis follows collection, is incorrect in that analysis could lead to more collection and that collection and analysis might occur in parallel i.e. the model lacks interactivity. The fourth and fifth challenge they found are more nation-state based in that the model does not cover the aspect of covert action, which an intelligence agency is prone to execute, and the varying nature of political regimes. And finally, the last challenge Dr. Gill and Dr. Pythian identify is that of technological development in that nation-states are moving towards a method of working where they collect everything instead of only collecting that what is necessary. The result being that Dr. Gill and Dr. Pythian propose the 'web of intelligence' as a solution which should counteract these findings.

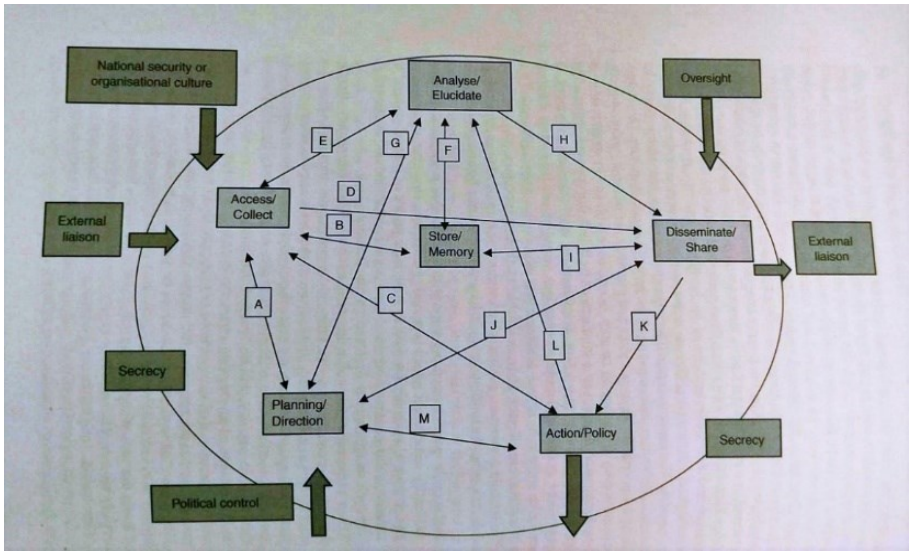

Figure 5 - The web of intelligence - Dr. Gill & Dr. Pythian

The two researchers from the Canadian R&D Defence labs, Ms. Frini and Ms. Boury-Brisset highlight the same points that Dr. Gill and Dr. Pythian have and expand upon them[48, p. 7]. However, they propose a different model based more around the collection and processing of intelligence. From their analysis of the papers of nine different authors they identify the following list of criticisms:

1. Intelligence collection process is not only driven by the decision makers
2. Intelligence support decision maker rather than inform him
3. Collection and analysis actually work in parallel
4. The traditional intelligence cycle is not iterative
5. The traditional intelligence cycle does not include consumption and feedback
6. The traditional intelligence cycle assumes the same process whatever the objective
7. Stovepiping
    a. Different collection disciplines are organizationally separated preventing cross-checking
8. The traditional intelligence cycle complicates the tasks of recognizing from where errors can occur

9. The traditional intelligence cycle lack in representing evaluation activities
10. The traditional intelligence cycle fits with the industrial mindset of the mid-twentieth century
11. The intelligence cycle does not represent the all-source intelligence perspective.

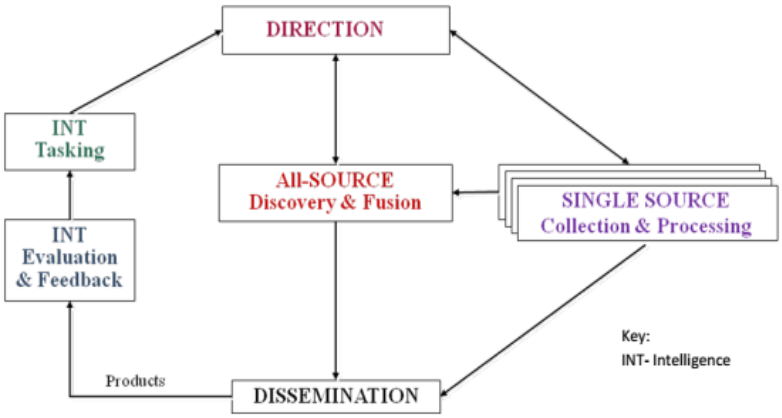

Figure 6 - An all-source intelligence model - Ms. Frini & Ms. Boury-Bisset

With this list of criticisms in mind Ms. Frini and Ms. Boury-Brisset propose a model that highlights the "all-source intelligence activities". This model groups these activities to the involved resources, reinforces continuous dissemination and feedback, promotes enhanced evaluation, favors the exchange of intelligence between all parties to improve the quality of the products, and makes information accessible, available, and discoverable at the earliest point possible. The result of their work is the model shown in Figure 6.

Dr. Robert M. Clark, in his book Intelligence Analysis; a Target Centric Approach, proposes another model for the intelligence cycle. This book is written with a focus on the role of the nation state analyst and therefore starts with an overview of the intelligence cycle. In this overview, he brings forward a fact that is often mentioned:

"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".

In his commentary on the model Clark mentions many of the points already previously mentioned such as linearity, interactivity between stakeholders, and the lack of a defined feedback loop from the customer to the intelligence team. To counter these comments, Dr. Clark proposes a target-centric, or objective-oriented, model that includes all stakeholders (collectors, processors, analysists, and customers) and is designed to be used for military, governmental, or criminal intelligence. The result of his work is seen in Figure 7. The idea behind this logic is, as Dr. Clark explains, to

"construct a shared picture of the target, from which all participants can extract the elements they need to do their jobs and to which all can contribute from their resources or knowledge, so as to create a more accurate target picture"

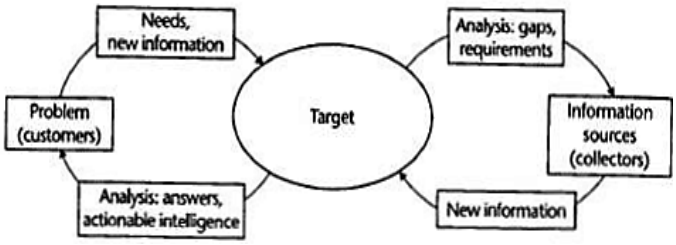

Figure 7 - A target centered view of the intelligence process Dr. Robert. M. Clark

The goal being that this model is not cyclical or linear but parallel as it allows all parties to input new goals, add new intelligence or insights, identify new knowledge gaps, and provide actionable intelligence at any time from a single point. Due to this interplay between all parties, one can share the same knowledge with many

customers at the same time and, due to each customers' different needs, all aspects of the same target will be covered in a single source.

The last model of this analysis is written by the UK Ministry of Defence in their Joint Doctrine Publication 2-00v3 on 'Understanding and Intelligence support to joint operations'. The model this document presents is shown in Figure 8**Error! Reference source not found.**. In the explanation of the model the MoD states that this model is an oversimplification of the intelligence process and that it "*is a continuous process comprising many cycles operating at different levels and speeds. [..] the tasks overlap and coincide so that they are often conducted concurrently, rather than sequentially*" [34, p. 53]. In short, it addresses some of the earlier defined shortcomings of the basic process via an extra explanation while not reducing the simplicity of the classical model. The explanation also discusses the subject of bias prevention where the other models do not. According to the author(s) of the document this was done because:

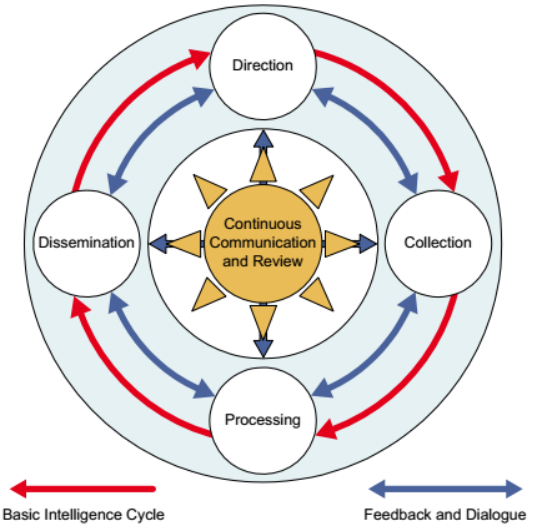

Figure 8 - The intelligence core functions and the intelligence cycle - JDP 2-00v3[34]

"[..] using structured analytical approaches can avoid analytical biases and provide a clear intellectual audit trail for judgements made".

They also state that each organization and participant might use different methods and could *"where appropriate [..] involve external experts, such as academics, who may have a different perspective" [41, p. 73].* The authors mention a few examples of how this might be done, such as by using a Key Assumption Check, testing the validity of made assumptions, playing the devil's advocate, using the same information to disprove the hypothesis, Red Teaming, re-analyzing the data while playing as the attacker, and Peer reviewing where seniors and peers review the judge the argumentation and possible alternative outcomes [41, p. 74].

Taking all previous findings into account, if one were to try to improve or create a new model based on the intelligence cycle then the list of requirements is quite extensive. Namely a better model should

A) consider that every actor within the intelligence creation process is a domain specialist;
B) include Parallelism which is not limited to the collection and analysis stages;
C) include Bias prevention and evaluation of whatever an analyst produces;
D) include a clear, complete, and concise explanation of the model to clarify the context it operates in;
E) should also fix the first nine findings that Frini and Bourriset found in their literature.

Some of these findings are duplicates of the four requirements previously mentioned and therefore the actual list to which the new CTI model needs to comply to is somewhat shorter. An example would be finding #3, from the paper of Frini et. al., regarding collection and analysis working in parallel which is a duplicate of requirement B, or #9 that evaluation of that which has been created is lacking. Then there are also a number of findings that cannot be solved in a new model. The end result is a list with seven extra requirements, that when combined with the

previous four requirements results in a total of eleven items which the new model will need to incorporate.

1. Intelligence collection process is not only driven by the decision makers
2. The traditional intelligence cycle is not iterative
3. The traditional intelligence cycle does not include consumption and feedback
4. The traditional intelligence cycle assumes the same process whatever the objective
5. Stove piping – the output of different collection systems is kept separate and prevent cross-checking by different disciplines.
6. The traditional intelligence cycle complicates the tasks of recognizing from where errors can occur
7. The traditional intelligence cycle fits with the industrial mindset of the mid-twentieth century

6. Proposal of the CTI model

Models are graphical explanations of how something works. The problem with this is that the more detail you want to put in, the more complex and therefore harder to understand the model becomes. For example – how does one graphically show that the new model does not embody the mindset of the mid-twentieth century in that it resembles an assembly line? As the intelligence cycle is circular in nature it quickly becomes an assembly line and the solution requires a high level of graphical detail to prove otherwise. To solve this, one needs to create a model that treads the fine line between easily understandable but detailed enough. Any extra information on how the different parts work and why is explained in a separate text. This is also the principle that this thesis used.

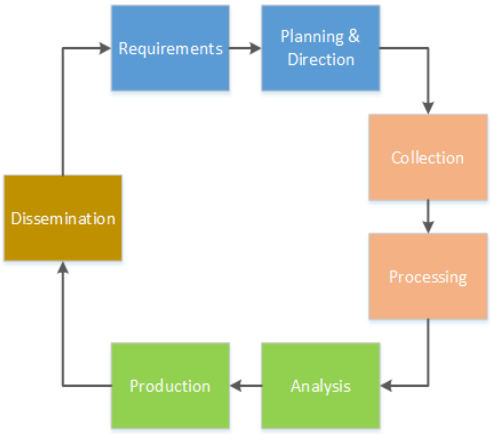

Figure 9 - The seven phases of the intelligence cycle; model of own design

Now, before the model for CTI will be presented a quick look back at the intelligence cycle and its different phases is required as it is the basis for the proposed model. While most models include four to six phases there are, when looking at the explanations, in reality, seven:

1. Requirements
2. Planning & direction
3. Collection
4. Processing
5. Analysis
6. Production
7. Dissemination

However, when looking at the list of requirements stated in the previous chapter, a couple of phases are missing namely:

1. Evaluation of the quality of the intelligence product — Finding C
2. Bias Prevention — Finding C
3. Consumption of the intelligence product — Finding #3
4. Feedback on the quality of the product — Finding #3

Taking these requirements into account, one comes to a model with eleven phases as shown in Figure 10. This figure is still readable and easy to follow, especially when using some colors to differentiate who does what when. Here blue is designated as the start of the intelligence cycle where customer, analyst, planner, and collection analyst come together to determine what the requirements are and what is required to answer the question. The light pink color indicates the process of data collection and processing whereas the green indicates the role of the analyst. The dark yellow is used to define the interaction with the customer and their role in closing and restarting the process. However, the oversight this model generates is counteracted when adding the requirement for parallelism and the possibility for the analyst to help set the next intelligence requirements.

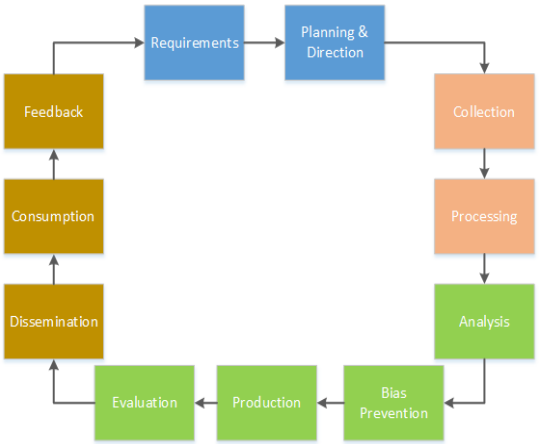

Figure 10 - The eleven phases of the 'new' intelligence cycle; model of own design

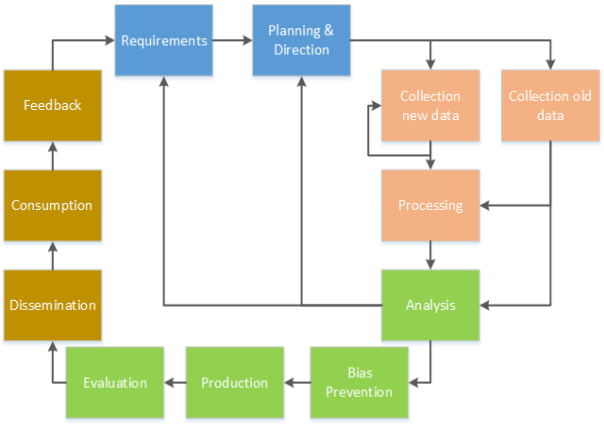

Figure 11 - The 'new' intelligence cycle with parallelism; model of own design

The new model, as shown in Figure 11, that these changes create give an indication that the singular, circular loop is not sufficient. This conclusion is entirely not new as the intelligence cycle in JDP 2-00, or the example models from the US MoD[48, p. 5] as previously shown in Figure 8, also use a multi-ring circular model. However, instead of changing the model to include the requirements the problems are solved in text, meaning that study is required and that the model itself remains unclear. For example, the JDP 2-00 solves the problem of parallelism with a two-headed arrow between collection and processing, a general statement at the beginning of the chapter[13], and in the chapter on processing or collection completely omits any reference to parallelism being a fact. This, again, makes the model hard to understand without having read the 30 pages that clarify the intricacies of the model.

With this conclusion in mind, this thesis proposes the following model for the intelligence cycle of CTI as shown in Figure 12 and a larger version can be found in Appendix A – Proposed model for CTI creation.

The core principle behind this model is that it has to be understandable with a minimal amount of knowledge of what CTI entails. The goal is that one could, within a company, build a CTI process on the model alone and that it is only necessary to study the literature to understand the details of the different phases. To do so, the model keeps the essence of the classic intelligence cycle in that it is A) a continuous process, and B) that it contains the, in this case six, different phases of the intelligence cycle. These different phases are made visible with colors: the light pink tones are used for the planning & direction phase, yellow for collection, green for analysis, brown for dissemination, and blue for evaluation.

Another new addition to the model is that who does what when is defined. The reasoning being that it clarifies who does what while also indicating that an analyst doesn't directly interact with a customer but goes via the intermediary. Additionally, it also describes the role of the intermediary as the point of translation between the analyst and the customer.

The process starts with the customer who has a question that requires an intelligence analyst. The intermediary will, together with the customer, clarify what the question entails, find an analyst who can answer the question in the requested timeframe, and determine the

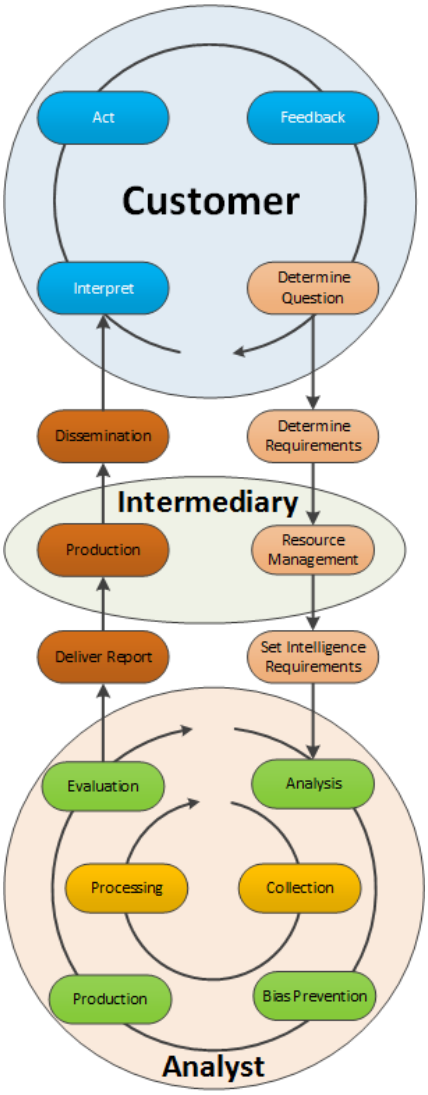

Figure 12 - Intelligence cycle of CTI; model of own design

[13] It is a continuous process comprising many cycles operating at different levels and speeds. Although the 4 individual tasks are discrete, as information flows and is processed and disseminated as intelligence, the tasks overlap and coincide so that they are often conducted concurrently, rather than sequentially.[34, p. 54]

intelligence requirements. The analyst will then start the intelligence creation process by collecting the data required, new or already known, processing it to fit the question, analyzing it and, if necessary, restarting the collection and analysis process until an answer the customers question is created. At this point a bias prevention together with one or more other analysts will take place to make sure there are no holes or misinterpretation and, if none can be found, a report will be produced. This will be evaluated, again by other analysts, and if deemed to pass the quality and assurance standards is sent to the Intermediary who will translate the report into the format required by the customer. If at any point gaps are found the analyst will have to go back into the collection and analysis cycles until the problems are corrected. Eventually, the intermediary will disseminate the report, the customer will interpret the intelligence, act upon it, and upon request by the intermediary or Samaritan kindness will give feedback on the result. If necessary, the question will be tweaked or a new one created and the cycle restarted.

As one can see that, in comparison with the intelligence cycle, the number of steps has increased from four to sixteen. Specific phases have been assigned to specific people and a hard split has been made between the analyst and the customer. This split has resulted in the role of the intermediary. This person is, in essence, a consultant and a team lead. Meaning that the intermediary not only acts as translator between analyst and customer, but also manages which analyst does what when and keeps an overview of what is happening where. There are a couple of benefits to this. First off, due to the intermediary being the single point of contact towards a customer, he or she has a very good understanding of their needs and how best to communicate. Combine this with the fact that the intermediary has access to all previous intelligence reports and the analysts, gives him/her a good position to advise the customer on other subjects. An analyst might, for example, have stated that subject XYZ is not interesting for further investigation. However, due to new information, an analyst might advise the intermediary that this subject is suddenly of interest. The intermediary can then contact the respective customers whom it impacts, inform them of the fact, and possibly advise them to re-investigate previous questions. This process scales with the number of customers with similar situations. Customer X might receive a report on subject A but the results of this report also impacts customer Y and Z. This allows the intermediary to inform the customer of the fact, if possible, or at least inform them that an investigation into subject A might be wise. Secondly, the segmentation also protects the analyst from any possible bias by knowing the plans of the customer and telling the customer what they want to hear.

The implementation of the bias prevention requirement is also resolved in the role of the analyst. As insinuated before, the analyst has two different cycles he/she operates in. The first is the cycle for collection and processing of data to feed analysis. This is a continuous process that not only pulls data from internal and external data feeds but also processed in near real-time into a singular syntax ,such as STIX[30], for storage and classification. When the analyst has collected the required data the analysis cycle starts with the analyst analysing and combining the different parts of information to a possible answer. If the analyst finds that he/she is missing data, the collection cycle is restarted to add more/extra data to the database. Eventually, the answer is checked for holes or misinterpretation by other analysts. If none are found the analyst can write the report, if there are problems the analyst will have to continue with the analysis process. The report, when finished, is again checked for problems by other analysts and the same rule exists

– if problems, then re-write or restart analysis. The end result being a report that is complete and, in theory, free of any bias.

Bias prevention is not the only requirement that has been implemented in the graphical model. Stovepiping, meaning that data collected and analyzed by team A is not shared with Team B, is also resolved due to the new role distribution. The theory behind the role distribution is that a CTI analyst will be a generalist instead of a specialist due to enterprises having smaller analyst teams due to budgetary limitations. For example, looking at the definitions of intelligence the NATO definition gave a long list of different types of intelligence such as HUMINT (human intelligence) or SIGINT (signals intelligence). Within a nation-state intelligence agency these will be different people or even teams due to the amount of data needing to be processed requiring specialists. Meaning that data from a HUMINT analyst will not quickly be used to evaluate a SIGINT report, which leads to stovepiping[14]. In the CTI model proposed here this is not possible as the analyst is a generalist instead of a specialist. Even if collection is split off in a different team, the analyst should still use the data from all of the sources due to him/her a) knowing that it exists and b) having access to the data.

Domain specialism is also solved graphically due to the actor-based grouping of the different phases. Customers are specialized in being customers, the intermediary is specialized in talking with analysts and customers, and analysts are specialized in the intelligence creation process. However, this is where the specialism ends due to the analysts having to be generalists to prevent stovepiping. Additionally, it might be possible to split the collection and analysis cycle and improve the specialization of these roles.

Finally, the requirement of the consumption and feedback phases not being included in the classic intelligence cycle can be found resolved in the end of the cycle within the domain of the customer. The idea being that the customer will receive the report, interpret it to his/her situation, act upon the intelligence received, and based on the result, provide feedback themselves or when asked by the intermediary. Based on this feedback, and the wish of the customer, the question will be corrected or a new one created. While this closes off the intelligence cycle, the explanation provided does not yet include all of the requirements as these are sometimes simply not something one can fix/include in a graphical model. Requirement #8 is an example of this. The requirement states that 'the traditional intelligence cycle fits with the industrial mindset of the mid-twentieth century' meaning that is resembles an assembly line "where specialization and a division of labor are supposed to improve efficiency". In the proposed CTI model an explanation has been given to favor generalists over specialists due to possible limitations in team size and to prevent stovepiping. However, when a CTI team becomes larger a natural tendency is that certain people will be become specialists in certain fields. Furthermore, at a certain point in time it might also become logical to split analysis and collection due to time constraints. These are all choices that need to be made by that department: a case can be made for specialized analysts working in an assembly line structure whereas a pure generalist structure also has its benefits. A solution might be to have a hybrid design of these two departmental structures but this will depend on the organization and their vision and goals they want to achieve with their CTI team. This conclusion also extends to requirements finding #7 which states that " that assessment of the intelligence product is not considered in the cycle"[48, p. 10].

[14] This was also the reason for Frini & Bourriset creating the all-source model.

According to this finding (#7) this is not possible due to intelligence being “fundamentally predictive in nature and there is no statement of objectives”. This seems to be a problem of defining a set of criteria whereupon an evaluation can be done. In the model proposed by this thesis this could be done by the intermediary asking for specific feedback which would answer a pre-set number of criteria. What these criteria are and when the best time to evaluate them is a subject for further investigation.

Requirements #2 and 3 also cannot easily be solved. Requirement #2 states that a customer already has a confirmation bias and only wants the intelligence to confirm his/her/their choice. This seems to be a problem of human psychology and it is up to the recipient of the intelligence report on how to handle it. It does not seem strange that a third party is already thinking ahead on which next steps to make. However, that party will need to be open to the results of the intelligence report and if it goes against the pre-determined choice, the customer will need to determine what to do with it. This will probably be the case in many cases but that is a subject of human psychology. Robert M. Clark also makes a point on this subject. He states that an intelligence team will need to gain the trust of the customer based on “the analysts reputation and the persuasiveness of the arguments”[18, p. 307]. For this model the customer will not be aware of the specific analyst but the same statement holds true for a CTI team only if quality control is implemented and executed thoroughly.

Requirement #3, which states that the intelligence process is not an iterative process, is also solved by keeping the human factor in mind and making a choice. The problem stated by in requirement three is that the entire model is iterative and that changes to a phase that has already been executed should force the process to adapt and take the changes into account. To implement such a change is something that needs to be centralized by a singular authority. In the model of JDP 2-00 there is a singular authority that determines the priorities and requirements of the intelligence creation process. In the proposed CTI model the choice was made to have the intelligence requirements set by the analyst working together with the intermediary. Therefore, if there is a reason for the intelligence creation process to be restarted then this will have to be decided on a case by case basis by those two parties.

In conclusion: Figure 12 shows a proposal for the intelligence cycle of CTI. While it tackles many of the requirements found during the analysis, some are situation specific. These will have to be tackled on a case by case or company per company basis and answered to fit the needs and situation of that company.

7. Validating the proposed definition and model

In their paper on Design science in Information Systems research, Hevner et al. states that *"The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well executed evaluation methods"*[51, p. 86]. Where, as Hevner et al explain, an artifact is the product or result of a design process within the field of Information System research; and that evaluating the artifact "provides feedback […] and a better understanding of the problem in order to improve both the quality of the product and the design process"[51, p. 78]. As this thesis proposes an artifact in the shape of a model, validation of its efficacy is required. To facilitate this process of validation a method is required which is described below. Due to the scope and time limitations, this thesis will not execute the validation. However, the following chapter will elaborate and which factors needs to be considered if the validation were to take place.

One of the criteria that Hevner et al. state which should be used is "the artifact's style"[51, p. 86] as "*Good designers bring an element of style to their work"*. In other words, the aspect of style gives an indication of the quality of the model. However, as Margaret Wolfe Hungerford stated in her 1878 novel 'Molly Bawn', "*Beauty is in the eye of the beholder*"[39, p. 143] meaning that beauty is a subjective fact that varies from person to person. This thesis has tried to present an effective solution to the problem about how CTI should be defined and beauty was not a factor that played any part in the design process of either the definition or the model. One could also make the case that, due to beauty being subjective, it might influence the party doing the validation to judge it on facts that have no influence on its utility. On the other hand, there is something to be said for judging this factor simply because if an artifact is nice to look at its more pleasant to use. Due to this reason, this thesis posits the first validation criteria of this thesis's artifacts to be 'style'. How this is determined is left up to the person or team doing the validation but an expected method would be to poll the opinion of a statistically relevant group of people. If this group should be knowledgeable about the subject or not is an item of discussion left for further investigation.

A second step in validating both the definition and the model, is to do an observational case study. This implies that both the model and the definition are studied in-depth in a business environment based on a pre-defined set of criteria. These criteria are split into two groups, each for a different phase of the validation process. The first grouping, or phase, is to test the model based on interviews with experts in the field of CTI. Reason being that one first wants to verify if the analysis and, the conclusions it presents, are correct when reviewed by a subject matter specialist. Additionally, the subject matter specialist can provide an insight into the real world validity of both artifacts. The second phase, or grouping, is to validate the model within one or multiple business environments to determine if the goal of this thesis has been reached in that the proposed model and definition help to clarify the concept of CTI to parties who have little to no experience with the subject. Additionally, this will provide insight into the real world validity of both artifacts. It is the idea of the thesis to validate both model and definition at the same time as they are, in this scenario where clarity is lacking, intertwined and there is no benefit to gain when validating them separately.

As stated, the first phase of the validation will consist of one or multiple interviews with subject matter specialists. The goal of these interviews is to determine their opinion on the proposed artifacts. Specialists one might want to contact are Michael Cloppert and Robert M.

Lee due to their specialism in the field of threat intelligence. Additionally, due to them authoring the SANS course on CTI and writing their views on the definition of CTI, they have proven to have a deeper understanding of the field. This gives them a broader and deeper view on the subject matter, giving more value to their opinion. Other authors are also welcome and one might consider also talking to the threat intelligence team at the ING Bank, or one could also get in contact with the Dutch NCSC who facilitate the Dutch 'Nationale Detectie Netwerk (NDN)'[53]. Both parties already have practical experience with the subject but, from personal experience, have differing views on what CTI is. TNO is another party that might be interesting to discuss the artifacts with. TNO is a research organization who's focus is on many subjects of which CTI is one[54]. Their in-depth knowledge of the subject and their interaction with other enterprises on these subjects might also provide valid insights. There are, of course, other parties one could contact and the previous parties are only presented as a starting point. The party who does the validation is free to choose as long as the specialism and experience of the chosen parties is a key factor of the decision.

During the interview there are several subjects that need to be discussed. The first being to document what their current understanding of the definition of CTI is. This will clarify with what kind of lens they are looking at the subject matter and what aspects are in scope and/or out of scope. What this means is that if the scope or what definition their opinion is based on is not clear, follow-up questions are required to help with clarifying the scope. The second subject to discuss is identical in the types of questions, however they should be focused on their understanding of the intelligence creation process of CTI – i.e. the CTI intelligence cycle. Here again the idea is to clarify their experience and view on the matter. When clarified, an explanation of the proposed model and definition is given after which the second phase of the interview starts.

The goal of the second phase is to determine if the experts find any fault with the proposed artifacts and if, in their opinion, it can be used in a real world scenario. To achieve this a set of very specific but open questions need to be defined. These questions would be on matters of perceived added value, factors missing or incorrect, real world viability, and if there are possible implications when used in an enterprise. If these questions are answered in a manner that finds the artifacts to be correct and usable then one can move on to testing them in an enterprise. If deemed incorrect the reasoning behind this opinion needs to be collected and used to propose a new model. Other options might also be a round-table discussion where multiple experts are brought in to discuss the pros and cons of the model, and discuss any possible refinements that might be required.

During the second phase of validation, the goal is to see insofar the artifacts are applicable in a real world enterprise CTI teams of different sectors. The manner wherein this thesis proposes to do this is by settings a zero level baseline, explaining the artifacts, having the artifacts implemented within the company and then using them for a set time[15]. The idea being that the measurement of the zero level baseline identifies current understanding of CTI. Whereas the second measurement, after the explanation, determines the delta and new understanding of what CTI entails while also giving an indication of with what kind of perspective they used. Additionally, it might also be used to determine if any problems are already foreseen. These

[15] This implementation might take a significant amount of time and should not be part of the evaluation period.

possible problems can be used in the later measurements to see if they have come true and why. The following measurement, after the artifacts have been implemented, will identify how the artifacts have been embedded into the organization and if they encountered any issues and why. Later on, when the artifacts have been used for a while, multiple measurements are done to identify the viability of the model and definition and to see what changes are made and why. These models are spread out on an ever increasing timeframe, e.g. 1 month, 3 months, 6 months, with a maximum duration of measurements being three years. This maximum of 3 years will help the implementation of the model mature and give the team the opportunity to identify problems. It will also give the team the opportunity to innovate, discuss with peers, and let the proposed model and process evolve naturally without the measurements guiding the process. At the end of the three years a final evaluation is done where the final input is gathered to help determine if any changes to the definition or the model are required and if so, what those are. With these steps it should become clear if the proposed artifacts are representative of an enterprise implementation of CTI and, if not, what needs to be changed and why.

When executing the evaluations two sets of questions are required. The first set is used when determining the baseline and after the model is explained. This set of questions has to determine the level of knowledge present within the team on the subject to determine any possible biases. An example of this might be an employee who was employed at a national intelligence agency or military intelligence agency. This means that this person has a certain training and possibly a mindset that changes his/her perception on the subject. This bias, if deemed to possibly be present, will have to be further investigated when evaluating the model and definition. The second set of questions is used to evaluate the validity of the artifacts when and/or after they have been used. Meaning that the questions asked should be focused on determining how the processes designed around the model are being used and, if changes occur, why they have taken place. Based on this information, combined with a possible bias, and a final evaluation will allow the validating party to determine what changes are organization specific and which are errors in the model. And after both validation checks have taken place can one say if the model and definition are a valid description of CTI within an enterprise.

8. Conclusion

In the closing lines of the introduction it was stated that a clearly defined concept is required if CTI is ever to be a security measure that even the smallest companies can benefit from. Currently, this is not the case due to different vendors using the same term to sell services that are barely related. For one vendor this is a data feed that the customer needs to convert to intelligence. Whereas a different vendor also sells CTI but instead sells processed and classified reports specific for the customer. This problem, which makes it hard for their customer to figure out what to buy, also extends to how a company who buys such a service should use it. As the literature on CTI is scarce, and the academic literature on nation state intelligence lacks a generally agreed upon definition or model, a first step was required to define what the concept entails.

To achieve the clarity required this thesis focusses on, from the perspective of an enterprise, defining what CTI is and modelling the intelligence creation process. To achieve this a comparative literature analysis was employed to answer both questions. The conducted analyses resulted in two proposals. The first proposal consisted of two parts; Intelligence as a term consists of six domains which all use the term intelligence but in their own way. Four of these six domains can be aggregated due to them using the term in a similar manner but with a different scope. This aggregation, under the term 'Actionable Intelligence' can be seen in Figure 13 and is defined as: *"The result of the process that combines information to answer a specific question."* This similarity in what each domain tries to achieve is balanced by its difference in its scope; the type of questions that it tries to answer. For nation-state intelligence, for example, this is survival of the state whereas military intelligence is focused on gaining battlefield superiority, or business intelligence which is focused on economic superiority of a company. For Cyber Threat Intelligence the scope was defined as wanting to determine the physical or cyber threat from internal or external actors against the company. This resulted in the second part of the proposal namely an official definition of the term CTI: "*"The result of the process that combines information to create an overview of an adversary and their intent, tactics, techniques, procedures"*.

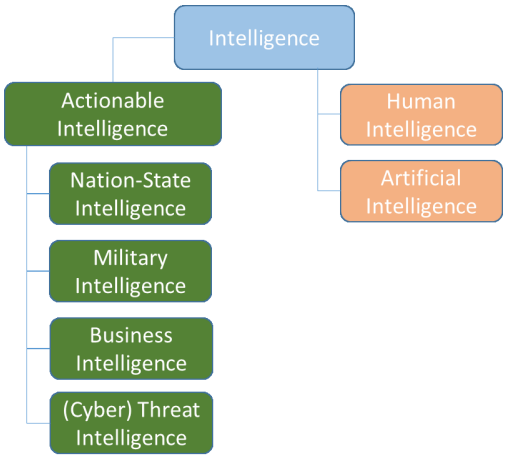

Figure 13 - A definition of intelligence; model of own design

The second proposal is the model of intelligence creation for a CTI team. This model was created by combining the 'classical intelligence cycle' with the commentary on the model by other authors. This commentary was aggregated into a set of requirements which was then translated into a model that describes the intelligence creation process for a company's CTI team. Part of this translation was done by expanding the 'classical intelligence cycle' graphically by clearly binding certain processes to certain actors, and by defining the required extra processes, while keeping the cyclical and six-phase nature of the original model. Other requirements were explained textually during the explanation of the model as they couldn't be explained graphically; and some requirements were disregarded entirely due to them not being solvable in a model. An example of this being the pre-determined bias of a customer who only wants the intelligence he/she/they receive to confirm his/her/their strategy. This is human nature and cannot be solved

in a model but can partially be solved by gaining the trust of the customer. Other requirements are more company or situation specific and need to be considered and/or solved by the party using the model.

While the proposed model and the definition will, on their own, reduce the lack of clarity that enterprises feel on the subject of CTI, it does require them to find this thesis and any research done on validating both artifacts. To help spread the knowledge of both artifacts and reduce the possibility of a misunderstanding in the communication between companies, a next step could be to publicize this thesis in a journal or present the model at selected events. An example of such an event might be an ETIS or FIRST meeting where security teams from all over the globe come together to share knowledge. These events could also provide valuable feedback due to the broad scala of security professionals present.

As Hevner et al. state in their paper on design science*: "Design is essentially a search process to discover an effective solution to a problem"*[51, p. 88]. This thesis is only a first important step in the design process to define the domain of Cyber Threat Intelligence and to take away to the lack of clarity that surrounds the subject. As CTI is a new field of study and is only starting to be used, a lot might change, meaning that any work created now might require drastic changes. It could be that CTI simply does not work for small and medium enterprise (due to financial limitations for instance) or that it does not provide the results required. If so, this could lead require changes to the model and definition due to a new understanding of what CTI should do and how it should work.

Furthermore, in the chapter on assumptions it was stated that the author of this thesis is employed as a member of the CISO team of KPN thereby possibly providing a better insight into the needs and complexities of an enterprise. However, due to this teams' position in the organization gives tremendous possibilities and insight into the company, it is also not a typical place for such a department. When looking at the situation at other telecommunication companies, these teams are often placed much lower in the organization and have less mandate thereby providing less chances and funding. Additionally, KPN has also been the authors only place of employment in such a large enterprise, and only for five years, meaning that any understanding of the enterprise environment is not from an extremely broad palette of experience. To compensate for this possible bias, this thesis advises that the second phase of validation should test the model in different sectors.

Nonetheless, this thesis has aimed to advance the understanding around the concept of CTI by presenting a much needed definition of CTI and by creating a model of the intelligence creation process. By addressing the lack of clarity it not only stimulates the academic debate on the subject but also supports the companies trying to operationalize it in their organization. Thereby not only improving communication between different intelligence teams, but also the defensive posture of the company and the general safety of the cyber domain.

9. References

[1] B. Krebs, "KresbsOnSecurity hit with record DDOS," 2016. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. [Accessed: 20-Jan-2017].

[2] O. Klaba, "OVH 1Tbps DDOS," *Twitter*, 2017. [Online]. Available: https://twitter.com/olesovhcom/status/778830571677978624/photo/1. [Accessed: 20-Jan-2017].

[3] E. Nakashima, "Russian government hackers penetrated DNC, stole opposition research on Trump," *Washington Post*, 2016. [Online]. Available: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?utm_term=.69c2a2d57b27. [Accessed: 20-Jan-2017].

[4] V. Goel and N. Perlroth, "Yahoo Says 1 Billion User Accounts Were Hacked," *Washington Post*, 2016. [Online]. Available: https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0. [Accessed: 20-Jan-2017].

[5] D. Goodin, "NSA-leaking Shadow Brokers lob Molotov cocktail before exiting world stage," *Ars Technica*, 2017. [Online]. Available: http://arstechnica.com/security/2017/01/nsa-leaking-shadow-brokers-lob-molotov-cocktail-before-exiting-world-stage/. [Accessed: 20-Jan-2017].

[6] A. Greenberg, "Hackers claim to auction data they store from NSA-linked spies," *Wired Magazine*, 2016. [Online]. Available: https://www.wired.com/2016/08/hackers-claim-auction-data-stolen-nsa-linked-spies/. [Accessed: 20-Jan-2017].

[7] M. Eddy, "After a cyberattack, Germany fears election disruption," *The New York Times*, 2016. [Online]. Available: https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html. [Accessed: 20-Jan-2017].

[8] G. Corera, "Bulgaria warns of Russian attempts to divide europe," *BBC News*, 2016. [Online]. Available: http://www.bbc.com/news/world-europe-37867591. [Accessed: 20-Jan-2017].

[9] Control Risks, "Cyber Threat Intelligence; Actionable insights to help you understand the cyber threat." [Online]. Available: https://www.controlrisks.com/en/services/security-risk/cyber-security-services/cyber-threat-intelligence. [Accessed: 09-Jan-2017].

[10] Symantec, "DeepSight™ Intelligence," *Website*, 2017. [Online]. Available: https://www.symantec.com/services/cyber-security-services/deepsight-intelligence. [Accessed: 09-Jan-2017].

[11] D. Shackleford, "Who's using Cyberthreat Intelligence and How?," *SANS Surv.*, no. 1st, p. 26, 2015.

[12] Fireeye, "Threat Intelligence," *iSight Threat Intell. Prod.*, p. 2, 2016.

[13] Checkpoint, "Threatcloud intellistore," 2016. [Online]. Available: https://www.checkpoint.com/products/threatcloud-intellistore/. [Accessed: 03-Dec-2016].

[14] L. C. S. Inc., "Threat Intelligence Services," 2016. [Online]. Available:

https://www.lookingglasscyber.com/products/threat-intelligence-services/. [Accessed: 03-Dec-2016].
[15] R. M. Lee, “Intelligence Defined and its Impact on Cyber Threat Intelligence,” 2016. [Online]. Available: http://www.robertmlee.org/tag/intelligence/. [Accessed: 29-Oct-2016].
[16] S. Caltagirone, “Threat Intelligence Definition: What is Old is New Again,” 2016. [Online]. Available: http://www.activeresponse.org/threat-intelligence-definition-old-new/. [Accessed: 30-Oct-2016].
[17] M. Cloppert, “Defining Cyber Threat Intelligence,” 2016. [Online]. Available: https://ctianalys.is/2016/08/22/defining-cyber-threat-intelligence/. [Accessed: 30-Oct-2016].
[18] R. M. Clark, *Intelligence Analysis a Target Centric Approach*, 4th ed. London: CQ Press, 2013.
[19] M. T. Bimfort, “A Definition of Intelligence,” *Studies in Intelligence*, 1994. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm. [Accessed: 22-Oct-2016].
[20] M. Warner, “Wanted: A Definition of "Intelligence" — Central Intelligence Agency,” *Studies in Intelligence*, 2007. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html. [Accessed: 16-Oct-2016].
[21] S. Kent, *Strategic Intelligence for American World Policy*, vol. 43, no. 2. Princeton University Press}, 1966.
[22] P. Gill and M. Pythian, “From Cycle to web of intelligence,” in *Understanding the Intelligence Cycle*, 1st ed., M. Pythian, Ed. Oxfordshire: Routledge, 2013, p. 160.
[23] A. W. Dorn, “United Nations Peacekeeping Intelligence,” in *The Oxford Handbook of National Security Intelligence*, L. K. Johnson, Ed. Oxford University Press, 2010, pp. 275–295.
[24] M. Pythian *et al.*, *Understanding the Intelligence Cycle*, 1st ed. Taylor & Francis, 2013.
[25] J. Gerring, *Social Science Methodology: A Unified Framework*, 2nd ed. Cambridge University Press, 2012.
[26] Merriam-Webster, “Definition of Intelligence.” [Online]. Available: http://www.merriam-webster.com/dictionary/intelligence. [Accessed: 16-Oct-2016].
[27] Cambridge English Dictionary, “Definition of Intelligence.” [Online]. Available: https://dictionary.cambridge.org/us/dictionary/english/intelligence?q=Intelligence. [Accessed: 16-Oct-2016].
[28] Collins Dictionary, “Definition of Intelligence.” [Online]. Available: http://www.collinsdictionary.com/dictionary/english/intelligence. [Accessed: 16-Oct-2016].
[29] Oxford Dictionary, “Definition of intelligence.” [Online]. Available: https://en.oxforddictionaries.com/definition/intelligence. [Accessed: 16-Oct-2016].
[30] S. Barnum, “Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™),” *MITRE Corp. July*, pp. 1–20, 2014.
[31] NATO, “AAP-06; NATO Glossary of Terms and Definitions,” *Allied Jt. Publ.*, p. 443, 2014.
[32] US DoD, “Department of Defense Dictionary of Military and Associated Terms,” *US Dep.*

Def. Jt. Publ., vol. 2001, no. June, pp. 1–513, 2015.
[33] Ministerie van Defensie, P. A. Brouwer, and M. Scholten, "Inlichtingen Joint Doctrine Publicatie 2 - Inlichtingen," *Jt. Doctrin. Publ. 2*, no. 2, p. 50.
[34] UK Ministry of Defence, "Understanding and Intelligence Support to Joint Operations (JDP 2-00)," *Jt. Doctrin. Publ.*, p. 155, 2011.
[35] Unknown, "Overview of documents bij Michael Warner." [Online]. Available: http://intellit.muskingum.edu/alpha_folder/W_folder/warner_m_a-q.html. [Accessed: 22-Oct-2016].
[36] CIA, "Michael Warner - who is he," 2007. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol52no2. [Accessed: 22-Oct-2016].
[37] M. Warner, "Wanted: A Definition of "Intelligence"," *Studies in Intelligence*, 2002. [Online]. Available: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html. [Accessed: 22-Oct-2016].
[38] M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. Sage Publication, 2016.
[39] MWR, "About MWR." [Online]. Available: https://www.mwrinfosecurity.com/about-us/. [Accessed: 20-Jan-2017].
[40] CPNI, "About CPNI." [Online]. Available: https://www.cpni.gov.uk/about-cpni. [Accessed: 20-Jan-2017].
[41] Oxford Dictionaries, "Definition of Military." [Online]. Available: https://en.oxforddictionaries.com/definition/military. [Accessed: 16-Oct-2016].
[42] D. Chismon and M. Ruks, "Threat Intelligence: Collecting, Analysing, Evaluating," p. 36, 2015.
[43] M. Warner and J. K. Mcdonald, "US Intelligence Community Reform Studies Since 1947," 2005.
[44] 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.
[45] R. R. Glass and P. B. Davidson, *Intelligence is for commanders,*. Harrisburg, Pa.: Military Service Pub. Co., 1948.
[46] N. Quarmby and L. J. Young, *Managing Intelligence: The Art of Influence*. Federation Press, 2010.
[47] J. Richards, "Pedalling hard," in *Understanding the Intelligence Cycle*, 1st ed., M. Pythian, Ed. Oxfordshire: Routledge, 2013, p. 160.
[48] A. Frini and A.-C. Boury-Brisset, "An intelligence process model based on a collaborative approach," *Def. Res. Dev. Canada*, no. Paper 113, pp. 1–49, 2011.
[49] M. Pythian, "Beyond the Intelligence Cycle?," *Underst. Intell. Cycle2*, vol. 1, no. 1, p. 8, 2014.
[50] "The Intelligence Cycle." [Online]. Available: https://fas.org/irp/cia/product/facttell/intcycle.htm. [Accessed: 30-Dec-2016].
[51] E. J. Arnould, A. R. Hevner, S. T. March, and J. Park, "Design Science in Information Systems," *MIS Q.*, vol. 28, no. 08.09.2007, pp. 75–105, 2004.
[52] M. W. Hamilton, *Molly Bawn*. New York: Hurst and Company, 1878.
[53] NCSC, "Nationaal Detectie Netwerk," 2016. [Online]. Available:

https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/het-nationaal-detectie-netwerk.html. [Accessed: 08-Jul-2016].

[54] Haagse Security Delta, “TNO CTI event,” 2016. [Online]. Available: https://www.thehaguesecuritydelta.com/events/event/1254-tno-organiseert-cyber-threat-intelligence-event-2016-12-21. [Accessed: 07-Jan-2017].

[55] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” *6th Annu. Int. Conf. Inf. Warf. Secur.*, no. July 2005, pp. 1–14, 2011.

Appendix A – Proposed model for CTI creation