Juho Koivula

CYBER HUMINT IN CYBERSECURITY: A CONTENT ANALYSIS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Koivula, Juho
Cyber HUMINT In Cybersecurity: A Content Analysis
Jyväskylä: Jyväskylän yliopisto, 2024
Turvallisuus ja strateginen analyysi, pro gradu -tutkielma
Ohjaaja: Moilanen, Panu

Tutkimuksen aihe on englanninkielinen termi ”cyber HUMINT”. HUMINT tarkoittaa henkilötiedustelua, joka on ihmisten avulla ja/tai ihmisiltä kerättyä tietoa. Kyber-etuliite termissä ”cyber HUMINT” tarkoittaa, että sitä toteutetaan kyberavaruudessa, joka on keinotekoinen ympäristö. Sen mahdollistavat toisiinsa kytketyt järjestelmät ja verkot. Tutkimuksessa tarkasteltiin analysoimalla yksityisten kyberturvallisuusorganisaatioiden verkkosisältöä vastaamalla kysymykseen: ”mitä on cyber HUMINT kyberturvallisuudessa?” Tutkimuksessa käytetään sisällönanalyysiä ja hyödynnetään erilaisia akateemisia lähteitä sen selvittämiseksi, miten henkilötiedustelu toimii perinteisesti ja digitaalisella aikakaudella. Tutkimusmenetelmäksi on valittu laadullinen sisällönanalyysi, joka on systemaattinen lähestymistapa analysoida ja tulkita eri verkkosisällön tarjoajien sisältöä ”cyber HUMINT” -toiminnasta kyberturvallisuudessa. Lähestymistapa noudattaa amerikkalaista perinnettä, ja siinä ryhmitellään samankaltaista ja osiin purettua sisältöä ja luodaan siten hierarkkinen rakenne, jossa suuremmat samankaltaiset ryhmät muodostavat kokonaisuuden. Ensimmäinen alakäsiteluokka kattaa tekniikat, joilla saadaan tietoa uhkatoimijoiden aikeista ja kehittyvästä uhkakuvasta. Toisessa kategoriassa korostetaan proaktiivisen kybertiedustelun keräämisen merkitystä mahdollisten kyberuhkien tunnistamisessa ennen kuin ne aiheuttavat vahinkoa. Jälkimmäisessä korostetaan ”cyber HUMINT” -toiminnan roolia kyberuhkatiedustelussa ja painotetaan sen merkitystä torjuntastrategioiden muodostamisessa kyberuhkakuvan avulla. Kokonaisuudessaan kyseessä on proaktiivinen lähestymistapa ihmiskeskeisessä kyberuhkatiedustelussa. Tutkimuksen johtopäätöksenä on, että ”cyber HUMINT” on merkittävässä asemassa uhkatietojen keräämisessä henkilölähteiltä kyberturvatoimien tehostamiseksi. Tutkimuksessa korostui kyberturvallisuuden, kybertiedustelun ja kyberavaruudessa ja digitaalisessa maailmassa tapahtuvan toiminnan inhimillinen osa-alue. Tutkimuksessa syvennyttiin siihen, miten teknologia muuttaa henkilötiedustelumenetelmää kyberturvallisuuden viitekehyksestä. Tärkeinä näkökulmina nousivat esiin automatisaatio operaatioiden skaalaamiseksi, toiminnan eettisyys ja lain noudattaminen ihmiskeskeisyyden vuoksi.

Avainsanat: cyber HUMINT, henkilötiedustelu, HUMINT, kyberturvallisuus, kyberuhkatiedustelu

ABSTRACT

Koivula, Juho
Cyber HUMINT In Cybersecurity: A Content Analysis
Jyväskylä: University of Jyväskylä, 2024
Security and Strategic Analysis, Master's Thesis
Supervisor: Moilanen, Panu

The subject of the study is "cyber HUMINT." HUMINT means human intelligence collected by humans and/or from humans. The cyber prefix in the term "cyber HUMINT" means that it is conducted in cyberspace, an artificial environment. Interconnected systems and networks enable it. The study analyzed the online content of private cybersecurity organizations by answering the question, "What is cyber HUMINT in cybersecurity?" The study uses content analysis and draws on various academic sources to explore how human intelligence works in the traditional and digital era. The research method chosen is qualitative content analysis, a systematic approach to analyzing and interpreting the content of various online content providers' "cyber HUMINT" on cybersecurity. The approach follows the American tradition of grouping similar and disaggregated content to create a hierarchical structure where larger similar groups form a whole. The first subcategory covers techniques to gain insight into the intentions of threat actors and the evolving threat landscape. The second category highlights the importance of proactive cyber intelligence gathering to identify potential cyber threats before they cause damage. The latter highlights the role of "cyber HUMINT" in cyber threat intelligence and emphasizes its importance in forming preventive strategies based on the cyber threat landscape. Overall, this is a proactive approach to human-centered cyber threat intelligence. The study concludes that cyber HUMINT plays a significant role in gathering threat information from human sources to enhance cyber security measures. The study highlighted the human dimension of cybersecurity, cyber intelligence, and operations in cyberspace and the digital world. The study delved into how technology is transforming the method of human intelligence from a cybersecurity perspective. Automation to scale up operations, the ethics of operations, and compliance with the law due to human-centricity emerged as important perspectives.

Keywords: Cyber HUMINT, Cyber Threat Intelligence, Human Intelligence Collection, HUMINT, cybersecurity

TABLES

INDEX

1 INTRODUCTION

This study is called "Cyber HUMINT in Cybersecurity: A Content Analysis." HUMINT means human intelligence collection. Human intelligence is processed information gathered by humans and/or from humans. Cyber-prefix indicates HUMINT being conducted in cyberspace, an artificial environment made possible by interconnected systems and networks. The context of cyber HUMINT in this study is cybersecurity. Content analysis is the chosen research method. The content comprises private cybersecurity and security companies and organizations providing consultancy and/or learning courses on cyber HUMINT.

This study aims to examine the digitization of human activities related to security. The focus is understanding how human intelligence collection and espionage operate in a digitalized world. While cyber espionage heavily relies on technology, it is important to remember that humans are the primary users of the internet and other interconnected networks. *Espionage* is considered the "second oldest profession" (Lowenthal, 2020, p. 125). Spying methods have adapted through the ages (Musco, 2017). Lucas Kello (2017) thinks we are in a cyber revolution that cuts through the whole human domain.

> In Kello's estimation, we are in an age of cyber revolution, as evidenced by the rapid expansion of cyberspace into nearly every facet of human activity and the disruptive rebalancing of actors and their activities in the international order,[...]. (Kello 2017, Gioe *et al.,* 2020)

Kenneth Geers (2015) emphasizes the growing significance of cyber espionage as more individuals, devices, and networks interconnect. Cyber espionage has become a highly organized and intensified activity. Various means of cyber influence can be utilized for different purposes, which are the spy's tools for gathering information. (Lehto & Neittaanmäki, 2015, pp. 73–83). Cyber advances intelligence collection and, at the same time, adversarial espionage. Emergent technologies have enabled the field of intelligence collection to have a vast global reach from a distance.

Gioe (2018) suggests enabling intelligence collection types with another type and gives "HUMINT-enabled cyber-operations" and "cyber-enabled

human intelligence" as examples in the literature (Gioe, 2018). The term "HUMINT" means human intelligence, which is a type of intelligence-gathering discipline involving human sources. Merriam-Webster defines the word *enable* as follows (Merriam-Webster, 21.3.2023):

- "to provide with the means or opportunity"
- "to make possible, practical, or easy"
- "to cause to operate"
- "to give legal power, capacity, or sanction to."

Cyber technology and digitalization enable traditional human intelligence collection to work with digital technology and in cyber environments. Digitalization and cyber affect intelligence collection across the field. Lowenthal asks whether cyber espionage is, for example, a form of human intelligence or a new form of intelligence collection (Lowenthal, 2017, p. 153). Lowenthal (2020) gives the following perspective on a methodology (refers to INT as a collection discipline) and technology:

> The view here is that cyber in and of itself is not an INT. It is a technology that makes various types of intelligence, just as satellites do, for example. The types of intelligence provided by cyber may fall into several different categories, but cyber itself does not define an INT. (Lowenthal, 2020)

Information on human intelligence is obtained from human sources (Lowenthal, 2017, p. 143). Through cyber, one can conduct all the so-called "INTs." Cyber cuts through all collection disciplines as a technology. Every collection discipline works interconnectedly through networks. This research was motivated by how human intelligence collection adapts in a cyber age.

1.1 Research Purpose

Next, I will explain the purpose of the research. The research is exploratory because the topic has yet to be defined under one concept. It elaborates on technology adoption in conventional human activity, which is a particular example of a general digitalization trend. The research also highlights the gap between two research frameworks: intelligence and cybersecurity.

As the research's approach is exploratory, it examines human activity in a new emerging environment. The motivation is to explore the phenomenon of cyber HUMINT in cyber security. Devanny and others (2021) state that there is a need for further research in the field of cyber-related human intelligence (Devanny *et al.,* 2021). Amit Steinhart (2014) explains why research literature on HUMINT and cyber HUMINT is scarce as follows:

> Many HUMINT success stories are understandably classified, and even those that are public are regularly censored, omitting key details regarding the modus operandi,

> technologies, and precise strategies used. It is hard to locate credible literature dealing with HUMINT, both academic and popular literature [18]. Often, HUMINT literature is touched with disinformation for the obvious reason of safeguarding "secrets of the trade". (Steinhart, 2014)

Researching this topic helps us to understand how technology enables human activity on a more conceptual level. On a more practical level, this research would help recognize new threats to organizational security (state, corporate, etc.) and new ways to counter those threats. Gioe (2017) weights the future of technology-enabled HUMINT as follows:

> In the cyber era, HUMINT will become even more complex, and case officers, their managers, and their political masters will need to understand the significant role of technology in their operations, the creative and persistent counterintelligence threats, and how intelligence collection is evolving faster than ever before. (Gioe, 2017).

The research is focused on a topic that involves two different frameworks. If cybersecurity and intelligence operations are not studied together, an unseeable gap could exist. As an intelligence collection discipline, HUMINT has a framework that is different from that of cybersecurity. Cyber security is technically oriented, while human intelligence is process-oriented. This research focuses on the human side of cyber security through human intelligence collection.

1.2 Research Problem and Question

Next, I will introduce the research problem and the research question. The research problem concerns digitalization and traditional human activity in the realm of security. The research question is a specific query about how the more general research problem is solved, particularly regarding cyber HUMINT in the context of cybersecurity.

The research problem is how human intelligence collection as a traditional human activity instantiates in a digitalized world. According to Merriam-Webster, digitalization means "the process of converting something to digital form" (Merriam-Webster, no date). When information is increasingly available digitally, know-how and means should adapt to meet contemporary demands if one aims to acquire the required information in the digitalized world. Without digital information-gathering methods, much data remains out of reach. One of the problems was that there was no consensus on definitions of digitalized human intelligence collection. There are differing views on whether it is a new discipline in total, a subcategory, or an expansion.

The research problem and the research literature guided the forming of the research questions. The frameworks behind the research question were the methodology of human intelligence collection (HUMINT) and cyberspace as a milieu of cyber espionage. Multiple concepts denote human intelligence collection and human-targeting espionage in cyberspace or other digital milieus. Here, cyber

HUMINT denoted the preconception of human intelligence collection conducted in cyberspace to guide the formation of the research question. Reflecting on this, the research question is: What is cyber HUMINT in cybersecurity?

1.3 Research Structure

The research structure consists of literature reviews on traditional and cyber HUMINT (chapter 2), the research method with the data and process, the research results, a discussion of the research, and the conclusion of the research.

Content analysis was chosen as the research method to answer the following question: What is cyber HUMINT in cybersecurity? Jouni Tuomi and Anneli Sarajärvi wrote the chosen source for the content analysis, which is called *Qualitative research and content analysis* (Tuomi & Sarajärvi, 2009, 2018). This methodological book explains the method of content analysis. The new version from 2018 showed how to proceed from data collection to the analysis of the content analysis.

The primary focus of this study is to analyze the written content produced by private cybersecurity and security organizations. Specifically, the research material centers around content that aims to educate the target audience on the topic of cyber HUMINT. This audience includes individuals seeking consultation, learning, and services to reduce their exposure to security and cybersecurity risks. The audience includes cybersecurity and security specialists who do not have cyber HUMINT in their operational portfolio. The data utilized in this study was collected via Bing's search engine, while the content was carefully selected to align with the research objectives and subsequently analyzed through content analysis.

In their book on content analysis, Tuomi and Sarajärvi (2009) cited Timo Laine's recommended steps for content analysis as follows (Laine; Tuomi & Sarajärvi, 2009, p. 92):

- Limit the content that can be analyzed.
- Review and take note of the included content.
- Exclude any irrelevant content.
- Combine the selected content.
- Encode the content.
- Report the analysis.

The content analysis was inductive and driven by the data. This method helps researchers break down the selected content, categorize data, and better understand the phenomenon being studied (Tuomi & Sarajärvi, 2009, pp. 96–97). Data references were managed using Mendeley. Sources were imported into it during the web search for research data.

This content analysis is driven by data. The concrete process of data-driven content analysis uses tables (Table 1). Following this process, research results are

reported based on data. Content analysis is a tool that simplifies web content by condensing information, grouping it into categories, and summarizing it. This process helps analyze data comprehensively and systematically, enabling meaningful insights, pattern recognition, and conclusions. Content analysis was done using Atlas.ti – a data analysis software – and Excel. I used Grammarly – an AI-enabled grammar and writing assistance software – to ensure my written English language is correct and readable.

The research results are reviewed in the discussion regarding the research purpose, problem, question, and literature review (Chapter 5). The reliability is discussed regarding whether this method was an appropriate option and whether it answered the research question. Further research from a technological perspective is also needed.

1.4 Research Concepts

Next, I will introduce the research concepts. Intelligence and cybersecurity research and methodology disciplines provide the research concepts. Human intelligence collection is a term used in the field of intelligence and international security. It is an intelligence collection type. I will explain what intelligence is in the context of international security and what an intelligence collection type is. Cyber espionage is a concept relative to intelligence but in the context of cybersecurity. Later, I will also present what cyber espionage means.

1.4.1 What is intelligence?

Intelligence can mean a "process," a "product," and an "organization" (Lowenthal, 2017, p. 11), whereas process means that information is processed through different stages. A four-part intelligence process includes *direction*, *collection*, *analysis,* and *dissemination* (Lowenthal, 2017, p. 11). Information needed indicates what information is going to be collected. The information collected is assessed and analyzed. The result is an intelligence product ready for dissemination (Lowenthal, 2017, p. 11), which contains the processed information corresponding to the information needed. An intelligence organization consists of different sections with their own duties in the process (Lowenthal, 2017, p. 11). The intelligence organization may be governmental or non-governmental. Intelligence operations have been conducted by government agencies, private actors, and criminal organizations (Lowenthal & Clark, 2016, pp. 45-46). The intelligence organization runs the process. Such an organization, guided by the intelligence need, turns information into an intelligence product through the intelligence process.

According to Lowenthal (2017), intelligence is needed because not all information is public, as some information is restricted and confidential. There is a desire to keep all information about intelligence goals, sources, and methods of information gathering secured (Lowenthal, 2017, p. 1). Without intelligence, a

state or a non-state actor lacks information about its opponents' intentions. The state or other actor also wants to secure critical information from its opponents. The criticality of information guides both intelligence gathering and concealment of information. Lowenthal (2017) justifies the need for intelligence as follows: to identify strategic-level threats to the state, to respond to decision-makers' requests for information, to assist decision-making, and to keep the objectives, means, and sources secret (Lowenthal, 2017, pp. 2-5). Intelligence must mask the ways of intelligence gathering to protect sources and intelligence capabilities (Lowenthal, 2017, pp. 99-102). This is called denial and deception (Lowenthal, 2017, p. 105). One's activities are concealed to maintain the quality of information and avoid countermeasures.

Lowenthal (2017) distinguishes intelligence from general knowledge and information. Intelligence is sought to support decision-making, and it has gone through an information refinement process. Having gone through this process, it is "identified," "acquired," "analyzed," and "disseminated" as driven by information needs (Lowenthal, 2017, p. 2). Intelligence is pursued, *collected*, verified, and collated. Raw information is not disseminated as such but is processed to meet the information needs.

Lowenthal (2017) refers to Alan Breakspear's definition of intelligence as the "ability" to identify "changes" that create opportunities and threats in sufficient time to enable action. (Breakspear; Lowenthal, 2017, p. 10) Without change, the status quo will continue its current trajectory. Time is essential to prepare for change. Hence, Lowenthal's description of intelligence as "approximate reality" indicates the nature of intelligence as a provider of foresight.

1.4.2 What is an intelligence collection discipline?

In this thesis, the intelligence is delimited to the *collection*. The types of collection include mission, methods, objectives, and technical expertise. The type of collection is activated according to the need for information. The need for information drives the collection. The objectives of the collection determine which type of intelligence *collection discipline* should be used.

Many different types of collection methods and techniques can be included as intelligence collection types. For this study, Lowenthal's and Clark's framework of intelligence collection types has been selected. Lowenthal and Clark (2016) list *collection disciplines* as follows: Open-Source Intelligence (OSINT), Human Intelligence (HUMINT), Signal Intelligence (SIGINT), Geospatial Intelligence (GEOINT), and Measure and Signature Intelligence (MASINT) as *collection disciplines* (Lowenthal & Clark, 2016, p. 1). Each type of *collection discipline* can be implemented independently or in combination. Multi-INT is the combination of multiple *collection disciplines,* and All-Source is the use of every *collection discipline* for intelligence (Lowenthal & Clark, 2016, p. 1). The information collected from multiple *collection disciplines* is called " collection synergy " (Lowenthal, 2017, p. 95). Synergy refers to the fact that different types of collection disciplines complement each other. Each type of collection has its own methodology and

research area. For example, knowledge gaps left by open-source intelligence (OSINT) can be filled by signals intelligence, whereas OSINT could be used to gather a list of targets for HUMINT or SIGINT.

The collection is generally departmentalized into multiple organizational sections. Intelligence officers in one collection category are unaware of what their colleagues in other collection categories are collecting. This problem is known as *The Stovepipes Problem* (Lowenthal, 2017, p. 103)—one can think metaphorically that the left hand does not know what the right hand is doing, but the brain knows the movements of both. Traditionally, the two collection types follow their paths, but in the final product of intelligence gathering, they eventually merge.

1.4.3 What is cyber espionage?

As a framework, cyber espionage is a cyber security threat and thus differs from intelligence collection frameworks. One can make this interpretation based on the choice of the word *espionage* based on adversarial activities instead of the word *intelligence*, which refers to one's own activities. Lehto (2015) uses the definition of cyber espionage used by Liaropoulos (2010), that cyber espionage is the pursuit of self-interest in various dimensions (e.g., politics and economics) by providing non-public and proprietary information to a competitor through the cyber influence (Lehto & Neittaanmäki, 2015). Kenneth Geers (2015) sees the importance of cyber espionage increasing as more and more users, devices, and networks become interconnected. Cyber espionage has evolved into a highly organized and intensified activity. Means of cyber influence can be used for different purposes, which in this sense are the spy's tools for information gathering (Lehto & Neittaanmäki, 2015, pp. 73–83). What does cyber mean?

Lehto (2015) considers the meaning of the word to be derived from the Greek word *kybereo*, which means 'to direct', 'to guide', and 'to control'. In cybernetics, the word refers to the steering of a system towards a goal state in an information technology context, where steering takes place through the medium of information (Lehto & Neittaanmäki, 2015, pp. 3–4). The term "cyber" refers to the control of information systems, including all connected systems within a network, such as devices, programs, and networks. A device consists of several programs, making it a system with multiple subsystems. In turn, devices are linked to other systems in a network, which creates a cyberspace that comprises interconnected systems. Cyberspace is an entity formed by interconnected information networks, facilitating the exchange of digital information between systems. (Lehto & Neittaanmäki, 2015, p. v). An emergent property is more in quality than the sum of its constituent parts. Lehto (2015) uses Kuusisto's (2012) definitions for spaces of cyber, according to which a cyber domain is "a well-defined space controlled by someone". A cyber ecosystem is "the systems of cyber communities and their environment", whereas a cyber environment is "the built environments that provide a framework for human cyber activity". Cyberculture is "the totality of the mental and physical cyberspace-related achievements of humanity or

communities" (Lehto & Neittaanmäki, 2015, pp. 4–5). Cyber HUMINT could then hypothetically be conducted in these spaces and environments.

1.5 Research Literature

Next, the research literature will be presented. The literature under review includes methodological books and academic articles on human intelligence. The literature was searched from Finna, Semantic Scholar, Bing, and ProQuest Military Database.

Mark M. Lowenthal's book *Intelligence: From Secrets to Policy* is an introduction to intelligence overall and to collection disciplines, including human intelligence (Lowenthal, 2020). Intelligence literature often references it (Giannetakis *et al.,* 2020; Gioe *et al.,* 2020; Johnson, 2010; Steinhart, 2014; Stottlemyre, 2015). In addition to that, Lowenthal and Clark have a methodology book on collection disciplines called *The Five Disciplines of Intelligence Collection*, in which Michael Althoff writes on human intelligence as a collection discipline (Althoff; Lowenthal & Clark, 2016). These books guide the basics of how human intelligence collection is conducted, in addition to journal articles that saturate and provide depth for review. Loch K. Johnson in *Evaluating "Humint": The role of foreign agents in U.S. Security* weighs on surpluses and deficits in human intelligence operations and concludes on the necessity of HUMINT in addition to technical collection disciplines (Johnson, 2010). Aden C. Magee, in Countering Nontraditional HUMINT Collection Threats, studies human intelligence activities of adversarial non-governmental organizations that often operate in a more aggressive and hastened fashion while targeting lower-tier personnel than it is being used in governmental intelligence organizations (Magee, 2010). Stefano Musco in *The Art of Meddling: A theoretical, strategic and historical analysis of non-official covers for clandestine humint* studies creating and maintaining cover roles to gather intelligence throughout history (Musco, 2017). Kyle S. Cunliffe in *Hard target espionage in the information era: New challenges for the second oldest profession* observes difficulties in conducting strategic level human intelligence operations with traditional methods in countries with technologically enhanced surveillance (Cunliffe, 2021).

The literature for review on cyber HUMINT shows that the research topic is yet to be expanded. Steinhart (2014) holds *social engineering* as a cyber methodology to conduct a human intelligence operation in cyberspace (Steinhart, 2014). Brian Mitchell, in *Corporate Cyberespionage: Identification and Prevention Part 2*, argues that cyber means shares the purpose of traditional human intelligence methods but with less risk (Mitchell, 2020). David V. Gioe, Michael S. Goodman, and Tim Stevens in *Intelligence in the Cyber Era: Evolution or Revolution?* gives a concept of *cyber-enabled HUMINT* that describes traditional HUMINT with the possibility of infusing it with cyber means. (Gioe *et al.,* 2020). Gioe, in *'The More Things Change': HUMINT in the Cyber Age*, sees leaks done by cyberespionage as a threat to HUMINT (Gioe, 2017). Giannetakis, Iannilli, & Caravelli in *Cyber Humint. A*

Behavioral Analysis Perspective research possibilities of social media and the internet overall for HUMINT (Giannetakis *et al.,* 2020). Joe Devanny, Ciaran Martin, and Tim Stevens in *On the Strategic Consequences of Digital Espionage* state that digital espionage exposure does not lead to diplomatic crises as a human intelligence operation exposé does (Devanny *et al.,* 2021).

In the methodological chapter, the literature is following: a methodological book from Tuomi and Sarajärvi – *Laadullinen tutkimus ja sisällönanalyysi* (Eng. Qualitative research and content analysis) - on how to conduct research using a method of content analysis as well as *Tutki ja kirjoita* (Eng. Research and write) from Hirsjärvi, Remes, Sajavaara and Sinivuo (Hirsjärvi *et al.,* 2009; Tuomi & Sarajärvi, 2009, 2018). In addition to these, I will use *Cyber Security: Analytics, technology, and Automation* from Lehto and Neittaanmäki (2015) as an academic guidebook for defining cyberspace and cyber espionage. These theories will be explored more closely in the following chapter.

2 LITERATURE REVIEWS ON TRADITIONAL AND CYBER HUMINT

2.1 What is Human Intelligence (HUMINT)?

2.1.1 How is HUMINT defined?

Next, I will explain the definition of HUMINT as an intelligence collection discipline. Here, I will explain how it involves humans as intelligence operatives and agents as intelligence sources, including the recruiting process. I will also explain other measures in addition to the recruiting process.

Targeted sources in human intelligence are, by name, humans (ICD Stottlemyre, 2015). Human intelligence (HUMINT) is a *collection discipline*. Loch Johnson (2010) defines "narrowly" that HUMINT targets and recruits people with access to restricted, classified, or confidential information. Johnson (2010) adds that HUMINT includes any directly collected information by "human beings". He also includes "clandestine acquisition of documents and other secrets". Human intelligence also includes seeking information and planting spying devices. (Johnson, 2010). When a representative of a human intelligence organization exchanges information with a human intelligence colleague from another country, the human source is a foreign liaison (Johnson, 2010; Lowenthal, 2020, p. 129). HUMINT includes collecting information via interviewing and interrogating (Dando & Ormerod, 2020). Johnson (2010) calls the direct acquirement of information by intelligence operatives from targets "the James Bond Approach" (Johnson, 2010). Information can thus be obtained from individuals without agent acquisition. Robert D. Steele (2010) holds that *clandestine* and *covert* HUMINT are a small part of the whole of HUMINT, but they are the key activities when used correctly. When open sources are not enough, then *clandestine* and *covert* HUMINT sources should be activated (Steele, 2010). Acquiring information illegally means *espionage* (Johnson, 2010). Steele (2020) references Gen. (retired) Anthony Zinni that only a small minority of sources used to support his own decision-making are actually "classified" (Zinni; Steele, 2010). In this thesis, I will concentrate on clandestine and covert HUMINT. Acquiring information illegally means *espionage* (Johnson, 2010).

Even though HUMINT is a small part of the larger picture of intelligence collection, it has a key feature. That is obtaining an understanding of the opponent's intention (Johnson, 2010). Kyle Cunliffe (2021) names strategic-level sources as "hard targets". These are sources that have a very high level of access to information and to the inner circle of government or non-governmental organizations. Althoff (2016) includes military, economic, and political leaders, government officials, and decision-makers, as well as individuals involved in planning, implementing, and reporting on issues in various sectors that are of strategic value to the intelligence organization (Lowenthal & Clark 2016, p. 45-46).

Magee (2010) adds lower-tier targets of relevant organizations. They are being targeted, for example, by "terrorist" and "criminal" organizations to support their operational purposes (Magee, 2010). The targeted source is what fits the *request for information* (RFI).

Human intelligence is gathered either directly from targets or indirectly via technical devices or non-technically via recruited agents. Next in focus are human intelligence methods.

2.1.2 What is an agent-acquisition cycle?

Next, I will explain what an agent-acquisition cycle is. There are two perspectives on what an agent-acquisition cycle in human intelligence collection includes. Two different perspectives are given by Michael Althoff and Mark M. Lowenthal.

Althoff (2016) describes the process of human intelligence as an *agent-acquisition cycle* with the following stages:

- *targeting;*
- *evaluation;*
- *development;*
- *recruitment.*

Before acquiring agents, there is a need to target people who have access to the information they seek. Then, the *target's* suitableness is *evaluated* as a potential agent. Once the *target* has been approved, a recruiter begins *to develop* a "relationship" with the recruitable person. The duration of this phase varies greatly. The process can even last for years. The progression of the cycle does not mean, for example, that the assessment is finished. The recruiter must find out if the recruit is a so-called "dangle," which means a counter-espionage lure, to either catch HUMINT recruiters or leak false information to an adversary. The assessment is made to see if the person is even willing to give out information. Ways of recruiting a spy include bribery and blackmail. The best-case scenario is that the agent is spying willingly without coercion. After the recruitment process, information is acquired from recruited agents (Lowenthal & Clark 2016, p. 61-63). Magee (2010) adds that organizations – who are willing to take "risks" to acquire information - are more likely to use coercive and aggressive measures (Magee, 2010). Althoff's (2016) cycle ends with the actual decision to recruit. It is made by the personnel with the given authority when a sufficient assessment of the recruit is done. The decision is based on whether the recruiter will accept the so-called "offer" (Lowenthal & Clark, 2016, pp. 61-63).

Lowenthal (2020) proposes a five-stage *agent-acquisition cycle:*

- *targeting/spotting;*
- *assessment;*
- *recruitment;*
- *handling;*

- *termination.*

The first task is finding potential sources based on information needs. Next in line is an analysis of the target's knowledge and propensity to be recruited. When considered recruitable, the target is offered an incentive to become an *agent.* After the accepted offer, the agent will act and be guided as an intelligence source. The *agent* no longer acts as a *source* of human intelligence when the operation ends or is seen as disposable for intelligence purposes (Lowenthal, 2020, p. 138). Lowenthal's recruitment process includes *handling* and source *termination* compared to Althoff's recruitment process. Lowenthal (2020 holds continuous and long-term rapport between operative and informant as "developmental" in that he is not involved in the cycle as Althoff (2016) does but sees it as a tradecraft of an operative (Lowenthal, 2020, p. 126; Lowenthal & Clark, 2016).

Next, I conclude the process. The recruitment process involves targeting potential sources in relevant positions, analyzing the potentiality of the target as a source, offering the target a reason (either positive or negative incentive) for being a source, turning the target into a source, processing the source for information, and ending the source status if necessary. The acquisition cycle indicates that obtaining a viable source of information is a lengthy process that requires many steps. The source must be chosen correctly to avoid the process being pointless. The target must be known so that it is not misleading, unwilling to cooperate, or without access to relevant information. The target may be a counterintelligence agent looking for personal informants. The target may be completely unwilling to compromise and accept the offer. Then, the long process will be futile.

2.1.3 What are the covers for clandestine and covert HUMINT?

Next, I will explain the topic of cover in clandestine and covert HUMINT. Clandestine HUMINT is done in secrecy. HUMINT is covered and kept unknown for outsiders during covert operations. The cover is used to hide the activity of the HUMINT operation.

Lowenthal (2017) presents a formal and informal cover. In the former, a cover is an *official* position for the presence of an intelligence operative in the target country. A cover can be an *official* function in a foreign mission with diplomatic status. In this case, the disclosure of the intelligence operation leads the person to be a *persona non grata*, whereby the operative has a limited period to leave the country. Informal cover as a *non-official* one does not have the protection of diplomatic status. Exposure leads to immediate imprisonment (Lowenthal, 2017, pp. 139-140). Johnson (2010) involves *diversified cover officers* (DCO) in addition to *official* and *non-official*. DCO could be an intelligence officer with ethnic origins from the target country. Johnson holds that "closed societies" with "effective counterintelligence" demand high-quality covers. That is why *non-official covers* and DCOs are highly important for human intelligence (Johnson, 2010). A diplomatic cover has diplomatic consequences, while *non-official cover* and DCO

have more possibilities for cover than *official* cover. According to Lowenthal (2017), the duration of the cover varies. Either the mission is activated immediately upon entry into the country, or the recruiter remains as a sleeper. Sleepers are activated into the intelligence role after a certain period, making the mission long-standing and requiring assimilation into the target country (Lowenthal, 2017, pp. 139-140).

Stefano Musco (2017) analyses *non-official covers* (NOC) used throughout history. The intelligence operative has an incalculable number of cover options to choose from, and so demands good imagination. The essence is to understand the socio-cultural context of the target country to have a great *non-official cover*. A particular NOC should also fit the characteristics of the person gathering intelligence. The cover should also have features that let the spy carry certain objects (such as approval to carry a weapon) and travel to succeed in the task without having local officials alarmed by inconsistent behavior. The target sets the purpose for cover. Moreover, a cover without access to the targeted people is not convenient for the operation. Musco asserts that their NOC could be almost anything, which is why he notes there could be ethical problems when using NOC. One example is having "clergymen" and "patriarchs" as NOCs. The operative must make the cover believable and the NOC solid. That demands high acumen to keep the cover story intact and capable of spontaneously fabricating a story when needed. It is essential not to get caught (Musco, 2017). There are fewer options for cover based on regarding the country of operations and the zeitgeist. For example, in the case of economic change, covers that worked well in the 19th century in the Arabian Peninsula would require upgrades in the 21st century. An energy trader would have been a lousy cover for a 19th-century intelligence operative working in the Arabian Peninsula but a great one in the 20th and 21st centuries. Musco (2017) notes that "humanitarian" networks and other *non-government organizations* (NGOs) are the type of contemporary cover organizations that give access and cover for intelligence operations (Musco, 2017).

Next, I conclude on the topic of cover. There are two kinds of covers: informal and formal. The latter is a diplomatic position, therefore the person has diplomatic immunity. The immunity of a diplomat is held until becoming a *persona no grata* after the cover is exposed. Even then, there is time to escape the country. The former is not a governmental position and is without diplomatic security. There are unlimited options for the informal cover, namely *non-official covers* (NOC). Furthermore, a NOC must be personally and situationally consistent, and it does not abide by ethics. It needs to be a fit for the person, the purpose, and the current social and cultural milieu. The cover could be anything.

2.1.4 What are the costs and the benefits of HUMINT?

Next, I will explain the costs and benefits of clandestine and covert HUMINT. These consist of technical demands, human skills and knowledge, and time and money. Conventionally, HUMINT is less machine-technical and naturally

psychological and cultural in its human-centricity. The goal is to gain critical inside knowledge from adversaries and not get caught.

HUMINT is, at minimum, a low-tech and low-cost *collection discipline* (Lowenthal & Clark, 2016, p. 46). Human intelligence activities have high risks. According to Lowenthal (2017), the weakness of human intelligence has traditionally been the need for immediate proximity to the target. Therefore, getting caught in an act of espionage is a major threat (Lowenthal 2017, p. 143). The risks of human intelligence operations must be weighed against their benefits. Lowenthal (2017) suggests that human intelligence does not acquire information in the sense of high quantity but in high quality. Therefore, human intelligence targets high-level insiders with "access" to the information sought (Lowenthal 2017, p. 143). Johnson (2010) and Steele agree (2010) to target strategically relevant sources that are not within the reach of other collection methods and disciplines (Johnson, 2010; Steele, 2010). Magee (2010) holds that when information needs are met, the lower-tier target suits the purpose, but acquiring it will be a riskier, quicker, and more coercive process (Magee, 2010). HUMINT demands to be more on the field compared to other *collection disciplines*. Human intelligence operations take a significant risk that threatens both the recruiter and the recruitable. Disclosures threaten to end an operation on which a great deal of time and resources have been spent. Johnson (2010) describes the necessity of patience in the following:

> For an operations officer to succeed as an ace recruiter, he or she would ideally know the language, history, politics, and customs of the assigned nation; after all, winning the confidence of a local government official depends upon establishing rapport, in part, and it is easier to relate to foreigners when one displays a certain comfort level in the norms of their society. Some experts believe that it takes about seven years to reach this level of familiarity. (Johnson, 2010)

Next, I elaborate on the costs and benefits of clandestine and covert HUMINT in conclusion. Time is what makes HUMINT expensive, but it also pays off in the end when operatives are accustomed to the local environment of operations. Clandestine and covert human intelligence is a risky intelligence activity that demands patience, durable effort, deniability, and deception through either informal or formal covers. HUMINT acquires key information that is beyond the reach of other collection disciplines from relevant persons in target organizations or states about the goals, plans, and intentions that meet the given RFI (request for information). Human intelligence is either acquired by humans or from humans, or both.

2.2 What is meant by cyber-prefix in the context of cyber HUMINT?

Next, I will explain the cyber-prefix in cyber HUMINT references. The cyber-prefix in cyber HUMINT has different variations. They all encompass HUMINT

activity with the added use of information technological innovations. The main concept is cyberspace, which references the digital milieu in which cyber HUMINT is conducted. Cyberspace is, by definition, an interconnected totality of information networks. The interconnectivity creates a coherent and complex space of interactivity. It acts as a medium for the exchange of information between digitally connected systems and ”devices” (Lehto & Neittaanmäki, 2015, p. v). Cyberspace does not include humans in a conceptual sense, but it works as a medium for humans to interact with each other for all kinds of purposes. Devanny and others (2021) state that there is still too little research on cyber HUMINT (Devanny *et al.,* 2021). The reviewed literature provides a framework for further research.

2.2.1 What is Cyber-HUMINT?

Amit Steinhart (2014) and Paola Giannetakis, Lucia Iannilli, and Federica Caravelli (2020) consider cyberspace as a concept where cyber HUMINT is operated (Giannetakis *et al.,* 2020; Steinhart, 2014). Steinhart (2014) mentions the *cyberworld* without defining it further (Steinhart, 2014). Cyberworld as a framework includes humans as users, while cyberspace does not.

Steinhart (2014) sees *social engineering*—a cyberespionage technique—as an activity that resembles human intelligence collection. Social engineering is used to overcome technical obstacles by exploiting human nature based on "social conformity." Cyberespionage is often technically oriented, but the human side of cyberespionage is to target human users and manipulate them to achieve different kinds of purposes. Social engineering has strong similarities with HUMINT but has lacked methodological prowess. Social engineering has benefits in the knowledge of operating in cyberspace (Steinhart, 2014).

The intelligence process can be accelerated in theory by targeting, assessing, and handling in a cyber environment. This lowers the risk and the time used to recruit people. Steinhart (2014) comes to the following conclusion in *The future is behind us? The human factor in cyber intelligence: Correlations between Cyber-HUMINT and Hackers' Social Engineering*:

> In recent years, we have been able to observe professional cooperation between experienced HUMINT professionals and cyberwarriors skilled in defense technologies and social engineering. The innovation proposed here is the development of a new direction, which I refer to as: “Cyber HUMINT,” the system in which human-factor mainstays like false identity creation, recruiting, human sources, and complex information manipulation are exploited by cybersecurity and HUMINT experts together. The expected outcome, when given the necessary time and resources, is the creation of a human intelligence structure in the cyberworld (Steinhart, 2014).

Steinhart's conclusion reveals a future convergence of cyberespionage and HUMINT. The technological prowess of cyberespionage meets the methodological prowess of HUMINT. Understanding human behavior is combined with technical expertise to reach targets and sources without entering the target

country. Social engineering is human-oriented cyber espionage, which describes a HUMINT-like process. HUMINT and social engineering have different conceptual frameworks. Both still pursue their goals by using people to give required access or information.

Giannetakis, Iannelli, and Caravelli (2020) hold *cyber HUMINT* as HUMINT in *cyberspace*. According to them, the whole agent-acquisition cycle can be operated by cyber means. Recruited targets are *virtual agents*. Operatives build a rapport with targets in cyberspace. For that, operatives require digital covers (Giannetakis *et al.,* 2020). The same principles that have been essential in traditional HUMINT are being adapted to cyberspace. Giannetakis and others (2020) describe a part of the process of agent acquisition as follows:

> Within the intelligence cycle, once the target has been determined, the team takes care of the entire preparatory phase of the operation (technical preparation, creation of profiles, etc.) and subsequent exploitation through real active participation that involves recruitment of sources and/or approach to the target, all rigorously online. For this reason, the team created ad hoc prepares an operation like the way in which a traditional HUMINT activity is set up (Giannetakis *et al.,* 2020).

Cyber HUMINT is analogical to HUMINT. Differences are found in the technical conducting of operations. Giannetakis and others (2020) make the notion of covert operations having two central points: *cover* and *access*. A hub is formed for sets of covers (created fronts, backstories, and identities) to gain web traffic and to gain information on visitors. Access to cyber groups begins with building rapport on forums and social platforms with *users*. Building rapport with targets and maintaining relationships with sources requires persistence (Giannetakis *et al.,* 2020). Cyber HUMINT is HUMINT in cyberspace, and it requires specialization in the milieu of activity.

> Therefore, at the base, there is the creation of a profile, which can be assimilated into the equivalent creation of a cover story. This story must be consistent, as must all the traces that must necessarily be released on the web to support it. CYB HUMINT is, therefore, a full-time activity that, on average, requires several months before it can be implemented via an active profile on the net without creating suspicion, months during which the social profiles must be fed with all the material necessary to outline exactly the characteristics of the "virtual agent" (Giannetakis *et al.,* 2020).

As mentioned earlier, Giannetakis and others (2020) assert that cyber HUMINT can be operated in cyberspace. "Delocalization and dematerialization" make cyber HUMINT a fully comprehensive whole. Cyberspace makes it possible to approach people digitally who would be difficult to meet physically (Giannetakis *et al.,* 2020). Cyber HUMINT would be a subspecies of HUMINT. It requires specialized operatives to function in cyberspace.

2.2.2 What is Cybernetic HUMINT?

Tal and Siman-Tov (2015) coined the term *cybernetic HUMINT* to name a "new subprofession" under HUMINT (Tal & Siman-Tov, 2015). What is cybernetic in cybernetic HUMINT? Siman-Tov and Tal do not explicate what is meant by cybernetic in their article. Based on their description of cybernetic HUMINT and HUMINT in the cybernetic age, cybernetic HUMINT is identical to cyber-HUMINT as Giannetakis and Steinhart have described it. Tal and Siman-Tov (2015) refer to "cybernetic tools," which give rise to cybernetic HUMINT. Those are "internet" and "online forums" (Tal & Siman-Tov, 2015). In the cybernetic HUMINT, the agent-acquisition cycle is operated in *cyberspace*. Tal and Siman-Tov (2015) see the possibilities of *cybernetic HUMINT* as follows:

> In the cybernetic HUMINT era, the candidates for recruitment are diverse and almost unlimited. The intelligence required to locate them can be obtained quickly, the selection is broad, and access is easy. Furthermore, cyberspace makes it possible to conduct the recruitment and handling stages with relatively little risk, at almost no cost, and with almost no effort, with the help of impersonation or anonymity, including multimedia meetings. Connecting with individuals and groups can be done easily, without any physical danger. Cybernetic HUMINT is groundbreaking and significantly improves the ability of HUMINT personnel to reach remote target audiences that are difficult to recruit (Tal & Siman-Tov, 2015).

Tal and Siman-Tov's definition of *cybernetic HUMINT* is similar to that of the concept of *cyber-HUMINT* (Chapter 2.2.1). They see it as a subcategory of HUMINT operated in cyberspace. What was done in traditional HUMINT is doable in cybernetic HUMINT when it is fitted to cyberspace.

The development of cybersecurity makes it more difficult for operatives to conduct operations in cyberspace. Tal and Siman-Tov (2015) indicate that digital footprints are more noticeable when digital surveillance develops (Tal & Siman-Tov, 2015). This is why having a good cover for covert operations in cyberspace is important. As discussed in Chapter 2.1.3, Stefano Musco (2017) noted that covers must be situationally fit. As in the physical milieu, the digital cover should fit a particular forum or social media group. Siman-Tov and Tal (2015) name cover in cyberspace as *avatar*. Those are fake "identities," which are represented by digital features such as "icons" and "images." Avatars are formed to meet situational criteria and are used for varying purposes. The range of covers as avatars is as vast as imagination allows. Those are created to operate on different kinds of social media platforms (private and public) and are used to do various tasks such as checking users' identities (there are technical applications to support this kind of activity). When developing digital relationships with humans, it is preferable to have "social sensitivity." This, combined with emotional intelligence, makes good cybernetic HUMINT operatives (Tal & Siman-Tov, 2015).

2.2.3 What is Cyber-enabled HUMINT?

Gioe et al. (2020) show that technology-enabled HUMINT has gained new collection disciplines or new technical means to operate with. Gioe brings forth two major benefits of cyber-enabling: "distance" between operative and source and "plausible deniability if caught" (Gioe *et al.,* 2020). New possibilities with the reduction of risks are made possible by technological innovation and the adoption of those innovations, which are relevant in enabling HUMINT with new methods and techniques. Gioe and others (2020) give the following notion of technologies leading to conceptual developments when new technical means are adopted to support intelligence tradecrafts:

> […] converging specialisms might be seen as the forebears of technological development enabling other collection methods that have evolved in contemporary terms such as "cyber-enabled HUMINT" or the converse, "HUMINT-enabled cyber operations," such as the Stuxnet attack on Iran's nuclear program (Gioe *et al.,* 2020).

Technology, which allowed new collection disciplines to emerge, is the main driver of intelligence collection. The results of human intelligence collection depend on technological adoptions. Cyber-enabled HUMINT allows HUMINT to operate in cyberspace without mutating into a wholly another new collection discipline. Cyber-enabling lowers risks and grows the reach of operations.

2.2.4 What is HUMINT in the Cyber Age and Hybrid Intelligence?

David Gioe (2017) holds that human intelligence collection stays "traditional" but concludes that cyberspace makes operating human intelligence more vulnerable. He thinks that other collection disciplines will commend human intelligence more via cyberspace. HUMINT as the core activity is supported and, in turn, hinged by cybersecurity, cyber espionage methods, social media intelligence (SOCMINT), disseminating secret information on the internet, and open-source intelligence (OSINT). These require HUMINT to adapt to the new demands of the evolving operational environment. HUMINT also gains a "force multiplier" in cyber when digital data is reached from a distance. Social media allows seeking information on potential targets and foreign operatives but requires more from covers and fake profiles because of a" digital footprint." Hacked private digital records potentially reveal operatives' or targets' vulnerabilities. Gioe holds that digital meetings leave more possibilities for deception than physical meetings between an operative and a recruitable target or a handled source (Gioe, 2017).

Gioe (2018) asserts in another article that a combination of traditional human intelligence and cyber methods is conducted by state actors to expose damaging information. This is called *hybrid intelligence*. It means combining human and cyber espionage with information operations (Gioe, 2018). Hybrid intelligence is not just intelligence. It is a combination of intelligence to produce leaks,

which cause damage to a hacked person's or organization's reputation, or to let guarded secrets be publicized on the internet.

According to Gioe (2017), the effect of cyberspace on HUMINT remains to be unanswered. Gioe assures that at least the intelligence cycle has been accelerated by cyber (Gioe, 2017).

2.2.5 What is the human domain in cyberespionage?

Human-targeting cyberespionage and HUMINT share similarities. Both use humans as sources of information and/or get access to an information source. Brian Mitchell (2020) divides cyberespionage threats among human resources between *outsiders* and *insiders* and between *external actors* and *internal actors*. In case of an outside attack, insiders are manipulated and exploited. On the contrary, in case of an inside attack, insiders as internal actors pursue gains or satisfaction in their self-interests. Outsiders, as external actors, use either technical means or insiders from the target organization to get access to the required information. A method of using human resources in cyberespionage is called "social engineering" (Mitchell, 2020). External actors using insiders resemble traditional human intelligence. Mitchell's (2020) following description of an external actor using insiders for cyberespionage has close similarities with the agent-acquisition cycle:

> If the external actor recruits a person within the organization, then this adds a human dimension because the internal participant is normally acting on the instructions of the external actor that continues to control the attack vector. This human dimension requires planned means of communication and transfer of information (physical or virtual contact) […] (Mitchell, 2020).

Mitchell (2020) explains that malintent outsider "recruits" insiders and exploit them to conduct cyberespionage (Mitchell, 2020). Mitchell's article shows that methods from human intelligence tradecraft are found in other frameworks and contexts. Concepts of cyberespionage are different from concepts of HUMINT but share similarities in the definition.

2.3 How do traditional and cyber HUMINT differ from each other?

The literature review on human intelligence (HUMINT) highlights that intelligence can be gathered directly by operatives from sources or indirectly through agents. It also covers the methods used to acquire and maintain operational cover, as well as the need to balance risks and rewards when conducting operations.

The recruitment process involves identifying potential sources, evaluating their potentiality, converting them into a source, extracting information from them, and ending the source status if necessary. Obtaining a reliable source is a lengthy process that involves choosing the right source and knowing the target

in advance to avoid misleading, uncooperative, or inaccessible sources. Intelligence can be gathered directly from targets or indirectly through technical devices or recruited agents. HUMINT requires covert operations with appropriate covers for the person, objective, and cultural milieu. It is a risky activity that demands deniability and deception and acquires critical information from relevant individuals in target organizations beyond the reach of other collection disciplines.

The cyber HUMINT literature review identifies several common denominators. Firstly, it highlights cyberspace as the milieu of technology-enabled human activity. Secondly, it emphasizes the need to adapt to a new environment where targets reside. Thirdly, it notes the new means and opportunities provided by new technologies to operate through every part of the agent-acquisition cycle. Fourthly, it mentions the option to operate both physically and digitally. Lastly, it highlights the importance of having operatives with the required skillset or technical means to conduct operations.

Tal and Siman-Tov (2015) note that handling of intelligence sources is crucial in cyber HUMINT. Building rapport is weaker in cyberspace, but it offers lower risk and more convenience for denial and deception. Digital footprints are trackable. Cyberspace allows connections with people in secure areas. Big data and a flood of information help keep the operation hidden. Multiple HUMINT organizations operate in cyberspace and provide liaisons for operational support. (Tal & Siman-Tov, 2015). Tal and Siman-Tov (2015) see cybernetic HUMINT as a promising intelligence activity that has not yet been set in stone. They sum it up with a notion of expanding cooperation as follows:

> It is too early to tell whether a new discipline has emerged, but the combination of the two, with new concepts and practical features, requires an innovative synergy between the clandestine environment and the civilian-commercial environment (Tal & Siman-Tov, 2015).

Information is readily available in operation support for cyber-enabled HUMINT. Giannetakis and others (2020) hold as important benefits of having cover profiles, language specialists, logs of activity, and knowledge management of operations readily at hand (Giannetakis *et al.,* 2020). The analysis could be done with accurate information on the side of collection operations. Giannetakis, Iannelli, and Caravelli (2020) see a lot of potential in cyber HUMINT as an option for intelligence collection. Lots of information can be found online (Giannetakis *et al.,* 2020).

Kyle Cunliffe (2021) asserts that high-access targets demand extraordinary work from intelligence operatives to penetrate states with high security and an advanced digital surveillance network. "A digital footprint" and "biometrics" create new kinds of obstacles for sustaining cover. Logs and social media profiles are the new cover stories for operatives. Having a social media profile with little information and activity could be suspicious in security checks. Advancements in digital surveillance force human intelligence operations to adopt cyber methods. Contemporary cyber security also makes fully non-physical operations very

difficult to conduct (Cunliffe, 2021). This means that physical presence in the country of operation demands a consistent profile and cover story in cyberspace. Either operating on the internet or physically, the digital cover will become a necessity. The former will be purely digital, and the latter will be partial to support a *non-official cover*. This means that traditional HUMINT can be supplanted with cyber methods. The threshold for leaking information is then lowered when physical drops are not needed. The negative side is to be without physical proximity to a source. This lessens the bond between a handler and its source. Cyber methods could make intelligence less risky by allowing targets to be approached remotely for recruitment purposes without the need for physical presence. Devanny and others (2021) show that digital espionage does not yet have the same political ramifications as traditional HUMINT (Devanny *et al.,* 2021).

The operational environment is different between physical and digital/cyber environments. Operatives are perceived either virtually or physically. Targets are approached, evaluated, and recruited, and sources are handled differently, either digitally or physically, with either digital covers or non-digital covers. The similarity is in the process of the acquisition of human agents to collect required information.

2.4 Summary

What was done with spy devices could be done via spear-phishing. There are two collection types (cyber and traditional HUMINT) that are interchangeable in an analogous manner. The principles remain constant in both the physical and digital environments, but the technical methodologies employed may differ. In addition to social engineering, OSINT (Open-Source Intelligence) and SOCMINT (Social Media Intelligence) share commonalities with cyber HUMINT. This means that traditional HUMINT can be supplanted with human-targeting cyber methods.

Based on previous research on cyber HUMINT, the following observations can be made:

- The concepts commonly used for the cyber prefix are "cyberspace," "cybernetic," "digital," and "cyber-enabled."
- Cyber HUMINT does not exclude traditional HUMINT.
- Cyber HUMINT is analogous to traditional HUMINT.
- Cyber HUMINT offers benefits that traditional HUMINT does not have.
- Traditional HUMINT has benefits that Cyber HUMINT does not have.

- Traditional HUMINT can be cyber-enabled to varying degrees to meet information requirements and operational demands.

The focus in cyber HUMINT research is not on cyberspace but rather on the nexus of cyber and traditional methods. Cyber HUMINT and traditional HUMINT are more on a spectrum that has benefits and trade-offs. They can be used variably in tandem. Cyberspace and digitalization enable traditional HUMINT to find optimized ways to acquire the required information. The synthesized concept would be cyber-enabled human intelligence collection, which is defined here as human-targeting espionage following the process of HUMINT and operating fully or partially in cyberspace.

The use of technology has made it possible to gather human intelligence in cyberspace and digital environments. The process of HUMINT has been adapted to work in these environments. Cyber HUMINT and cyber-enabled HUMINT are essentially the same as traditional HUMINT, which is human intelligence collection. Cyber HUMINT involves using information technology to carry out the process partially or entirely in cyberspace. In this method, the agent-acquisition cycle and the creation of cover can be conducted online. The costs and benefits of traditional and cyber HUMINT are weighed against each other in cyber-enabled HUMINT, depending on the operational environment, targets, and sources.

The comparison between cyber HUMINT and traditional HUMINT highlights the significance of HUMINT as a crucial framework for studying cyber HUMINT. The use of emerging technologies has made research in cyber HUMINT promising and interesting. The cyber environment provides many advantages for human intelligence operatives in comparison to traditional human intelligence collection. These benefits include non-physical presence, vast opportunities for information, covers, and targets, which are not available in traditional human intelligence collection.

3 RESEARCH METHOD AND PROCESS

In this exploratory research, the aim was to examine how human activity in intelligence collection translates into a new digitalized environment in the context of cyber security. My research problem was to identify how traditional human intelligence collection adapts to this new environment. The research question was: What is cyber HUMINT in cybersecurity?

The research method chosen to answer the research question is content analysis. The source chosen for the content analysis was written by Tuomi and Sarajärvi in 2009 and 2018. Tuomi and Sarajärvi (2009) identify two types of content analysis: qualitative and quantitative. Qualitative content analysis seeks to identify qualities that are similar to and different from the data, while quantitative content analysis counts different types of content in the data (Tuomi & Sarajärvi, 2009, p. 106). Content analysis is a qualitative research method used to explore data that is made up of observations and experiences (Tuomi & Sarajärvi, 2018, pp. 22-29). In this research, primary sources are used, which include published web content from private cybersecurity and security organizations, such as Adeo, Cyber Cupula, CyberProof, Intel471, and SOS Intelligence.

The method referred to as "text analysis" (Tuomi & Sarajärvi, 2009, p. 104) involves analyzing data in the form of text. This text can be gathered through interviews, observation, or as a transcription of people's speech. Tuomi and Sarajärvi (2009) differentiate between content analysis and discourse analysis. The content analysis seeks to answer the question of what the explanations are, while discourse analysis focuses on how the explanations were presented. (Tuomi & Sarajärvi, 2009, p. 104). Content analysis is chosen as the method to analyze web content on cyber HUMINT.

The approach used in the analysis is data-driven, according to Tuomi and Sarajärvi (2018). They refer to the logic of this type of content analysis as inductive, which means that it is based solely on the data and does not rely on any prior knowledge or understanding. In contrast, deductive analysis involves drawing conclusions from a theory that is based on previous knowledge and understanding. In data-driven analysis, a framework is created from the data itself, which then guides the analysis towards theoretical concepts (Tuomi & Sarajärvi, 2018, pp. 108–110). The analysis will result in a synthesis of grouped data, as stated by Tuomi and Sarajärvi in 2009 (pp. 96–97). Private cybersecurity and security organizations provide content on cyber HUMINT, which serves their purpose in consulting and teaching. However, intelligence communities do not define their concepts of cyber HUMINT, thus the content created by private organizations may provide a different understanding of cyber HUMINT. The synthesis is formed by grouping data, and the process of data-driven content analysis will be presented in tables (Table 1-4).

As briefly mentioned in the introduction (Chapter 1.3), Timo Laine has outlined the process as follows: limit the content, review, and take notes, exclude any irrelevancies, combine the selected, encode the content, and then report the

analysis (Laine; Tuomi & Sarajärvi, 2009, p. 92). The key to successful research is to have a manageable amount of data that addresses the research question (Tuomi & Sarajärvi, 2009, p. 92). This thesis aims to analyze web content related to cyber HUMINT and synthesize the collected data to define the phenomenon of cyber HUMINT in cybersecurity. The content analysis method will provide an analytic framework to identify differences and similarities in content on cyber HUMINT from the viewpoints of private security and cyber security specialists. Lastly, I give a notion of my use of Grammarly – an AI-enabled grammar and writing assistance software – to correct my written English language in reporting.

3.1 Research Data

Next, I report on the research data. Data should include qualities comprehensively, but the size of data should remain within the borders of the research task. Data should show qualities of the phenomenon and verifiably by consistency within a multiplicity of sources. Data should be reasonable so it could give answers within the limits of this master thesis. Research data, in general, are written documents, which are web pages of private security and cybersecurity organizations that include written content about cyber HUMINT in the context of cybersecurity.

Written documents interpret a phenomenon, in this case, collected from the Internet. Research material is obtained from private security cybersecurity organizations' websites using Bing's search engine. It is important to narrow down the data to answer the research question without making the task too broad. Sufficient data should still be gathered to ensure consistent results with the overall phenomenon. Search sentences are formed based on cyber HUMINT and are employed in a trial-and-error manner during the search process. The references are organized in Mendeley after collecting for managing the web content. The content is encoded. Hirsjärvi, Remes, and Sajavaara (2009) have proposed the saturation principle, which aims to limit data size. According to this principle, when new data does not add to the quality of the existing data, it becomes saturated (Hirsjärvi *et al.,* 2009, p.182). The content referred to in this thesis is a result of saturation.

3.2 Research Method

The research method follows the American tradition of content analysis. According to Miles and Huberman (1994), data-driven content analysis includes *reduction*, *categorization*, and *abstraction*. Relevant content is collected as *citations*. Citations are *reduced* to simpler forms or divided into parts, and reduced parts of the content are grouped into *classe*s. These *classe*s are then grouped again until there

is only one *class* left. These *classes* are named to define grouped content. This process is called *abstraction*. (Miles & Huberman, 1994; Tuomi & Sarajärvi, 2018, pp. 122-123). The analysis is forming groups from similar contents and larger groups of similar groups towards a whole. *Categorization* and naming of classes enable the formulation of the answer to the research question.

Through reduction, categorization, and abstraction, content analysis synthesizes web content into a larger whole. This will be conducted using analysis tables. There are columns for *citations*, *reductions*, and different *classes* from multiple *categorizations* (TABLE 1). Citations from web content are listed first. Reductions made from Citations are listed. Lower Classes are formed from Reductions. Upper Classes are formed from Lower Classes. The Main Class results from categorizing the Lower and Upper Classes. If multiple Main Classes remain, those are grouped into a Combined Class.

TABLE 1 The data-driven content analysis process

Citations	Reductions	Lower Class	Upper Class	Main Class	Combined Class

TABLE 1 This shows the analysis process from reduced parts picked from citations to multiple categorizations of conceptual classes.

Saturation marks that there are enough qualities pulled from web content. The content column includes *citations* from web content within the research problem and is listed in a column (Citations). *Reductions* are made from *citations* and listed in a column (Reductions**)**. *Reductions* are combined into Lower Classes and added to a column (Lower Class). Column of Upper Class includes categories grouped from Lower Classes. The Main Class categorizes the Upper classes (Main Class). Column of Combined Class includes a singular class formed from Main Classes (Combined Class). *Abstraction* is the naming of categories that include all classes.

3.3 Research Process

Next, I will explain the research process. The research methodology was based on data. The content was from private cybersecurity and security organizations' websites. The sites which provided content on cyber HUMINT and HUMINT in cybersecurity were included. The traditional HUMINT was excluded. The content was web searched, brought to a reference manager, imported to data analysis software, and listed to Excel data sheets as explained in chapter 3.2.

The search was done in English using Microsoft Bing's search engine. Search words were used in multiple conjunctions using Boolean operators. The web search using Bing was as follows:

1. Using sentence -- ("cyberhumint" or "cyber-humint" or "cyber humint") and (advanced persistent threat) –- 4 sources were chosen from 1630 results.

2. Using sentence -- ("cyberhumint" or "cyber-humint" or "cyber humint") -- 10 sources were chosen from 15700 results.

3. Using sentence -- ("cyberhumint" or "cyber-humint" or "cyber humint" OR "Cyber Human Intelligence") – 0 sources were chosen from 675 results.

4. Using sentence -- ("cyberhumint" or "cyber-humint" or "cyber humint" OR "Cyber Human Intelligence") AND "cyber security" -- 0 sources were chosen from 189 results.

5. Using sentence -- ("cyberhumint" or "cyber-humint" or "cyber humint" OR "Cyber Human Intelligence") AND (cybersecurity OR "cyber security") – 4 sources chosen from 264 results.

6. Using sentence -- ("cyberhumint" or "cyber-humint" or "cyber humint" OR "Cyber Human Intelligence") AND (cybersecurity OR "cyber security") AND Blog - 0 sources were chosen from ninety-one results.

7. Using sentence -- ("cyberhumint" or "cyber-humint" or "cyber humint" OR "Cyber Human Intelligence") AND "cyber security" - 0 sources were chosen with one hundred results.

8. "digital humint" AND blog - 5 sources were chosen from 13900 results.

Search results often showed repetitive results. Different search sentences were used and modified to limit and vary search results. The chosen sources included web pages consisting of content cyber HUMINT and HUMINT in cybersecurity, which were gathered for content analysis. Twenty-three sources were imported to Mendeley Library. Fourteen documents were included in the research data after nine were excluded. Reasons for exclusions were the following: Only HUMINT without cyber; not a private security or cybersecurity organization; the concept was Virtual HUMINT.

Next, the websites and web publications of private security and cybersecurity companies will be reviewed. First, there will be a short introduction to the company or organization, followed by a summary of their text about HUMINT in cybersecurity and/or cyber HUMINT.

SOS Intelligence is a company that offers threat intelligence services. Its focus is on surveilling data leaks and alerting those affected. On its website, it informs us that it monitors, for example, the dark web to alert people about leaks and risk monitoring. It also provides threat-hunting services. The company collects data using automation. (SOS Intelligence, no date) Amir Hadzipasic discusses Cyber HUMINT and automation on the company's website, focusing on efficient data collection techniques. (Hadzipasic, 2021)

Cyber Cupula is a cybersecurity company that works together with clients and law enforcement to identify and counter cyber threats. On their website, they state that the company specializes in using human intelligence in cybersecurity to attribute threat actors and provides effective tools for protection. Their target audience is companies in the financial sector. Through their Cyber HUMINT services, Cyber Cupula combines human intelligence with web and open-source intelligence to guard against cyber threats (Cyber Cupula, no date).

The International Anti-Crime Academy offers specialized training courses in digital investigation and combating cybercrime. On their website, they state that the courses are instructed by experienced professionals. Courses concentrate on practical and applicable skills on topics such as Cyber HUMINT, digital analysis, and personal information protection. The training can be beneficial for individuals who are interested in acquiring advanced investigative techniques. Furthermore, law enforcement agencies in the United States have utilized this training to combat financial crimes. (International Anti-Crime Academy, no date)

Cyber Risk GmbH in Switzerland provides professional training and consultancy services on cybersecurity topics like cyber espionage, cyber HUMINT, and cyber threats' impact on businesses. George Lekatis founded the company, which specializes in compliance and risk management. (Cyber Risk Gmbh, no date) The company writes on cyber espionage and warfare, with a brief touch on cyber HUMINT. Cyber espionage is hard to detect, making cybersecurity training and awareness crucial. (Cyber Risk GmbH, no date)

Intel 471 provides Cyber Threat Intelligence services to businesses to improve their cyber defenses against potential financial loss, data leaks, damage to public image, or intellectual property theft. They use human analysis and data collection to identify cyber threats (Intel471, no date). In their blog, Michael DeBolt informs about Cyber HUMINT, which involves using human collectors to gather intelligence from digital sources, providing insights into adversaries' motives and tactics that automated methods may overlook. Combining automation and cyber HUMINT is a powerful approach for enterprise security, offering critical details for effective risk mitigation and staying ahead of evolving threats. (DeBolt, 2023)

CQR is a cybersecurity outsourcing company based in Eastern Europe that provides IT security services. They offer various solutions, including red teaming and penetration testing, to enhance their clients' security measures. (CQR Company, no date.) CQR highlights the importance of HUMINT in cybersecurity, detailing its types, methods, benefits, limitations, tools used, and ethical considerations on its website. HUMINT plays a critical role in threat intelligence, incident response, vulnerability assessment, and gathering contextual information. (CQR Company, 2023)

Grey Dynamics is a London-based intelligence firm that prioritizes timely, accurate, and actionable intelligence services. They offer a range of services, including articles on intelligence, intelligence reports, research, and investigations (Grey Dynamics, no date). A blog by Rachele Momi informs about HUMINT and touches briefly on the topic of cyber HUMINT. (Momi, 2021)

Rapid7 simplifies cybersecurity challenges through a comprehensive security platform and services. Their Insight Platform automates operations and enables teams to focus on priorities (Rapid7, no date). Intelligence tools, including HUMINT, are crucial for effective cybersecurity strategies that recognize adversary motivations, according to Nathan Teplow's blog (Teplow, 2018).

CyberProof offers cybersecurity assistance for businesses transitioning to digital cloud environments utilizing virtual and human analysts along with

automation. The company is multi-certified and emphasizes the importance of adapting to the opportunities and threats presented by the cloud era (CyberProof, no date). Eva Prokofiev, a Senior Intelligence Analyst at CyberProof, explains cyber HUMINT - a combination of traditional espionage techniques with cyber capabilities to proactively prevent cyber threats. By integrating classic HUMINT strategies with cyber methods, cyber HUMINT enhances cybersecurity measures by gathering critical information, engaging with threat actors, and preventing attacks before they occur. (Prokofiev, 2019)

ADEO Cyber Security provides cybersecurity services to corporate customers in Türkiye and the MEA region, with expertise in offensive and defensive cyber offense, cyber resilience, and technology procurement. Their team is committed to continuously improving their customers' cybersecurity defenses (ADEO, no date). Effective cybersecurity defense requires understanding the human element of cyber threats through HUMINT and developing strategies accordingly. (Adeo, 2023)

Treadstone 71 provides cyber intelligence services. The founder has expertise in linguistics and cybersecurity. They offer courses on cyber intelligence and provide threat assessments, planning, and research services (Treadstone 71, no date). Treadstone 71 writes on cyber HUMINT and its automation that automation leads to effective intelligence gathering on adversarial activities in cyber environment. (Treadstone 71, 2023)

Hacktoria, a Helsinki-based company, provides story-driven Capture The Flag (CTF) challenges that use gamification to teach various cybersecurity and digital investigation skills (Hacktoria, no date). The company provides information on social engineering and cyber HUMINT techniques for CTF challenges (Hacktoria, no date).

CrowdStrike is a cybersecurity company that provides AI-powered cybersecurity platforms, threat intelligence, and threat-hunting solutions (CrowdStrike, no date). HUMINT is crucial in cyber security to understand adversaries and enhance protection, according to Bart Lenaerts-Bergmans, a Senior Product Marketing Manager with over 20 years of experience at CrowdStrike (Lenaerts-Bergmans, 2023).

Cyberarch is a cybersecurity consulting firm that provides tailored services globally, with a focus on Information Security and Computer Forensics. The company has expertise in risk management consulting and provides services to manage the challenges of Information Technology (Cyberarch, no date). Their published content emphasizes the use of HUMINT in cybersecurity to counter cyber threats effectively. They leverage strategies such as social engineering and engagement with hacker communities to enhance cybersecurity defenses. (Cyberarch Admin, 2021).

The content was encoded, and citations were brought in as sentences for the content analysis. The chosen content as citations was reduced to simpler forms (Table 2). The content was encoded and analyzed by using data analysis software called "Atlas.ti." Content was encoded based on research questions and data. I used Atlas.ti to perform reduction and the first two rounds of categorization.

Codes, citations, reduced content, and lower and upper classes were then exported to Microsoft Excel. Citations were excluded if they did not answer the research question.

TABLE 2 Examples of content analysis, from Citations to Reductions

Citations	Reduction
"Cyber-HUMINT is frequently understood to mean social engineering activities – which, in the context of security, means the psychological manipulation of people into divulging confidential information, or performing actions they do not want to do." (Prokofiev, 2019)	Cyber-HUMINT psychological manipulation social engineering activities to divulge confidential information to perform unwanted actions
"Cyber-HUMINT has two aspects to it: on the one hand, there are espionage methodologies such as agent recruitment and information gathering through deception; and on the other hand, there is Cyber-HUMINT – the deception methodologies that are commonly referred to as social engineering. " (Prokofiev, 2019)	agent recruitment Cyber-HUMINT deception methodologies espionage methodologies information gathering social engineering through deception
"Cyber-HUMINT means putting into action the information passively gathered by intelligence analysts and operatives." (Prokofiev, 2019)	Cyber-HUMINT gathered by intelligence analysts and operatives information put into action

Table 2. The examples above show the process of reduction.

The final phase of the content analysis was categorization and abstraction. Words and phrases after the reduction were grouped together based on their similarity. Classes were named based on the denominating factor. These lower classes were connected to the upper classes (Table 3).

TABLE 3 Examples of grouping of Lower classes

Reduction	Lower Class
interplay between cyber HUMINT, hackers, and social engineering phishing attacks psychological manipulation social engineering social engineering activities social engineering strategies and practices	Social engineering
deception deception methodologies online deception through deception	Deception
agent recruitment recruitment	Recruiting
an ethical dimension in cybersecurity	Ethical consideration

combination of automated collection and cyber HUMINT-derived insights combine the collected data with other sources of intelligence not a standalone solution	Combination

Table 3. The examples above show the reduction grouping.

Upper classes were named based on the consistence of the class. This was done again to form two main classes and eventually one combined class. Categorization was conducted inductively from data. The categorization is shown in chapter 4 (Table 4).

4 Proactive Cyber Human Threat Intelligence

I will now present the findings of a data-driven qualitative content analysis. The report will include categories (TABLE 4) and descriptive quotes from the research data. Two main categories were formed from lower-level classes. The first category is "Covert Human Threat Intelligence Professionality," while the second is "Proactive, Compliant, and Scalable Cyber Intelligence Tool." These categories are combined into "Proactive Cyber Human Threat Intelligence." The research question was: What is cyber HUMINT in cybersecurity?

TABLE 4 Categorization of Classes towards Main Combined Class

Lower Class	**Upper Class**	**Main Class**	**Combined class**
Social engineering	Exploiting human attack vector	Covert human threat intelligence professionality	Proactive cyber human threat intelligence
Recruiting			
Targeting			
Relationship building			
Infiltration			
Humans as an attack vector			
Deception	Denial and deception		
Digital cover			
Threats	Threat intelligence process		
Collection			
Analysis			
Insights			
Decision support			
Expert knowledge	Professionals		
Operators			
Training			
Intelligence methodologies	Proactive intelligence methodology	Proactive, compliant, and scalable cyber intelligence tool	
Proactive			
Benefits	Benefits, potentiality, and challenges		
Technological development			
Ethical consideration			
Tool	Cyber intelligence tool		
Cybersecurity			
Cyber intelligence			
Digital forensics/investigations			
Counterintelligence			
Combination			
Operating digital environment			

Table 4 Categorization process of the content analysis is presented above.

4.1 Covert Human Threat Intelligence Professionality

This main class includes the following upper classes: Exploiting the human attack vector, Denial and deception, Threat intelligence process, and Professionals.

4.1.1 Exploiting the Human Attack Vector

The first upper class was named Exploiting the human attack vector, which included the following lower classes: Social engineering, Targeting, Recruiting, Relationship building, Infiltration, and Human attack vector.

Social engineering is a core method in cyber HUMINT. The following citation from the data states: "Cyber-HUMINT starts with traditional human intelligence processes (recruitment, training, intelligence gathering, deception, etc.), combined with social engineering strategies and practices." (Cyber Risk GmbH, no date). The concept overlaps with social engineering in terms of using humans to obtain information. The data cites the following: "Cyber-HUMINT is frequently understood to mean social engineering activities—which, in the context of security, means the psychological manipulation of people into divulging confidential information or performing actions they do not want to do." (Prokofiev, 2019).

Recruiting is part of Cyber HUMINT as the following citation states: "Recruiting Human Agents: Cyber Humint involves recruiting human agents strategically to gain insights into potential threats and hostile actors." (Hacktoria, no date-b). Targeting is identifying potential sources to recruit. Relationship building is necessary to create trust between operative and the target. Relationship building is done online, and it is fast-paced, which the following quote from the data reflects: "On the other hand, Cyber-HUMINT is based on a short-term and virtual relationship." (Momi, 2021).

Infiltration is the main operation to get access to relevant digital communities to reach recruitable sources. A quote from the data mirrors this as follows: "Cyber HUMINT operators were able to infiltrate online spaces where the group was active." (Adeo, 2023).

Humans are attack vectors in cyber HUMINT. They are manipulated and exploited for attaining required information. A following quote from the data reflects this thought: "Cyber-HUMINT refers to the strategies and practices used in cyberspace, in order to collect intelligence while attacking the human factor." (Cyber Risk GmbH, no date)

4.1.2 Denial and Deception

The next class in the hierarchy is known as Denial and Deception, which is further divided into two lower classes named Deception and Digital Cover.

The lower class, named Deception, is conducted to conceal the true purpose of a particular operation, referred to as a part of cyber HUMINT in an earlier quote, while Digital Cover is employed to hide the identity of the operative as well as their organization. According to a quote from the data, "However, cyber HUMINT typically involves a single human collector who operates under a digital identity - commonly referred to as a persona, sock puppet, handle, or moniker - that is carefully crafted with believable backstories and motivations, also known as legends (similar to traditional HUMINT)." (DeBolt, 2023).

4.1.3 Threat Intelligence Process

The following text describes the Threat intelligence process, which is composed of five lower classes: Threats, Collection, Analysis, Insights, and Decision Support. Threats are the biggest challenge in cybersecurity. To tackle this issue, Collection is the most important operation in cyber HUMINT. It involves gathering information about threats to cybersecurity.

As the data states, "Our Cyber-HUMINT handlers, together with talented analysts, are operating Digital Avatars interacting with and collecting data from the threat actors in the Cyber vicinity." (Cyber Cupula, no date). Another essential part of cyber HUMINT is analysis, where gathered information about threats, threat actors, and the overall threat landscape are assessed. It helps to string together the collected information.

Insights are critical information received from threat actors. They provide a better understanding of the intentions of the threat actors. As mentioned in the data, "In other words, cyber HUMINT has the advantage over other types of cyber intelligence collection methods because it reaches below the surface to reveal critical insights necessary to solve security and risk use cases that would be otherwise missed using other collection methods." (DeBolt, 2023).

Decision Support is the final step in the Threat intelligence process. It helps cyber HUMINT operatives and cybersecurity professionals to use gained intelligence effectively. Decision Support identifies critical threat actors and provides guidance on how to defend against threats. As stated in the data, "Cyber-HUMINT means putting into action the information passively gathered by intelligence analysts and operatives." (Prokofiev, 2019).

4.1.4 Professionals

The following text explores the cyber security profession and its essential parts further.

The profession comprises professionals with expert knowledge of the operational environment, methods, tactics, and procedures. They need to know

where they operate and how to gather critical information about the threat landscape and actors, which the following quote reflects: “When it comes to the concept of Cyber Humint, the role of cyber experts and human intelligence specialists is crucial.” (Hacktoria, no date,b)

Operators are the professionals who know how to operate cyber HUMINT. This requires not only cyber security expertise but also the ability to handle humans in a cyber environment. Here is a quote from CyberProof, for example: “Our cyber threat intelligence professionals use Cyber-HUMINT to identify individuals or groups that are secretly trading sensitive information belonging to […] customers, as well as those who are conducting other forms of malicious activity.” (Prokofiev, 2019)

As quoted earlier, training is a relevant aspect of this profession. Professionals must possess human skills and the ability to operate in the digital environment and, for that reason, use a fitting set of techniques and procedures in cyber HUMINT.

4.1.5 Conclusion

This set of classes consists of four upper classes that focus on different aspects of human intelligence and threat intelligence. The first upper class, "Exploiting human attack vector," deals with the techniques and strategies used to exploit human weaknesses and gain access to threat actor’s information. The second upper class, "Denial and deception," aims to prevent exposure of the operation and the identity of an operative. The third upper class, the "Threat intelligence process," is focused on collecting, analyzing, and disseminating information about potential cyber threats to enhance protection measures. Finally, the fourth upper class, "Professionals," is dedicated to educating and training cybersecurity professionals, improving their skills and knowledge to keep up with the evolving threat landscape.

In cyber HUMINT, social engineering plays a pivotal role in information collection. This approach uses human intelligence processes and social engineering tactics to manipulate individuals to obtain intelligence. The process includes the steps of recruitment, targeting, building relationships, infiltration, and analysis; it often involves deception and digital cover to operate under false identities. Cyber HUMINT professionals use digital avatars to interact with threat actors and gain critical insights that aid in decision-making for cybersecurity defense. Adequate training is essential for these professionals to perform effectively in the cyber HUMINT field.

4.2 Proactive, Compliant, and Scalable Cyber Intelligence Tool

This main class includes the following upper classes: Proactive intelligence methodology, Benefits, potentiality and challenges, and Cyber intelligence tool.

4.2.1 Proactive Intelligence Methodology

The following text explains the Proactive Intelligence Methodology, which has two lower classes called Intelligence Methodologies and Proactive. Intelligence Methodologies are techniques used in intelligence collection outside the domain of Cyber HUMINT.

Cyber HUMINT is the collection of intelligence by human means, which is the foundation of Cyber HUMINT. The quote is an excerpt from the data: “Cyber HUMINT, or the application of traditional human intelligence techniques in the digital realm, provides a unique and proactive perspective on the intentions, tactics, and plans of adversaries.” (Adeo, 2023)

Proactive refers to offensive cybersecurity, which is different from technical and defensive cybersecurity systems that passively gather information from web traffic to identify and detect malicious attacks. Proactive cybersecurity tools actively find human sources to uncover threats. Proactive cybersecurity does not wait for the first indications of a malicious attack. The quote exemplifies, "Cyber HUMINT is an important component to this proactive intelligence gathering approach, providing “eyes and ears” visibility into pre-attack signals that would otherwise go undetected.” (DeBolt, 2023).

4.2.2 Benefits, Potentiality, and Challenges

The next upper class was Benefits, potentiality, and challenges. The next level in cyber intelligence is Benefits, Potentiality, and Challenges, which consists of three sub-levels: Benefits, Technological Development, and Ethical Considerations.

Cyber HUMINT, a method of collecting intelligence from human sources, has many benefits in providing insights about the intentions of threat actors that would otherwise be unknown using other cyber intelligence tools. The following quote from the data suggests the benefits, "Cyber HUMINT has the advantage over other types of cyber intelligence collection methods because it reaches below the surface to reveal critical insights necessary to solve security and risk use cases that would be otherwise missed using other collection methods." (DeBolt, 2023)

Technological development is an integral part of cybersecurity, and it plays a significant role in optimizing the operational cycle of cyber HUMINT in the digital environment. The technical environment in which cyber HUMINT operates generates a lot of data, and therefore, technical expertise is required to automate multiple processes and utilize big data. As the following quote from the data suggests, "The general approach is to identify relevant sources of targeted cyber HUMINT, develop automated mechanisms to collect information from identified sources, apply text mining and natural language processing (NLP) to automatically process and analyze the collected data, combine the collected data with other sources of intelligence, contextual analysis, cross-reference and verification, threat actor profiling, visualization and reporting, and continuous monitoring and update." (Treadstone 71, 2023)

The following quote from the data looks at the relationship between humans and ethicality: "Moreover, the human aspect of Cyber HUMINT also brings an ethical dimension to cybersecurity." (Adeo, 2023). Proactive cyber intelligence in the human domain requires compliance with legal and privacy frameworks and consideration of ethical questions about human exploitation even though the person in regard would be a threat actor.

4.2.3 Cyber Intelligence Tool

The next upper class was the Cyber intelligence tool. It includes seven lower classes as follows: Tool, Cybersecurity, Cyber Intelligence, and Digital forensics/investigations.

Cyber HUMINT is a tool used for cybersecurity to gather threat intelligence about cyber threats and threat landscape. A following quote from the data mirrors this: “However, while Cyber HUMINT is a powerful tool, it is not a standalone solution.” (Adeo, 2023)

Cyber HUMINT is threat intelligence for cybersecurity. This can be seen from the following quote gathered from the data: “In conclusion, Cyber HUMINT is an invaluable component of any robust cybersecurity framework.” (Adeo, 2023). However, Cyber HUMINT is cyber intelligence gathered from humans in a cyber environment. The data quotes: “Cyber HUMINT reminds us that behind every line of code, every digital footprint, and every cyber threat, there are human beings with their motives, strategies, and tactics.” (Adeo, 2023)

Cyber HUMINT is used for Digital forensics and investigations, as laid down in the following quote from the data: “If an attack takes place, companies can use Cyber-HUMINT methodologies to engage with threat actors during the investigation of the attack, to gain more information – i.e., to reveal the extent of the damage and its broader impact.” (Prokofiev, 2019)

Cyber HUMINT is applied for Counterintelligence in cybersecurity, as the following quote from the data refers to: “On the side of cyber security experts and intelligence analysts, cyber-HUMINT is leveraged for counterintelligence purposes” (Prokofiev, 2019).

Cyber HUMINT is used in combination with other intelligence collection types. Here is the following quote to form a view of a combined methodology: “[…] intelligence products & solutions are based on a unique methodology fusing Cyber-HUMINT with WEBINT and OSINT.” (Cyber Cupula, no date).

Cyber HUMINT is Operated in a digital environment or cyberenvironment like this. The following quote suggests that “To fully understand the relevance and application of Cyber HUMINT, we need to appreciate that cybersecurity isn’t just a game of advanced algorithms and sophisticated software; it’s a human battleground where motives, tactics, and strategies are as important as technical proficiency” (Adeo, 2023).

4.2.4 Conclusion

The primary class consists of a set of upper classes that collaborate to develop a Proactive, Compliant, and Scalable Cyber Intelligence Tool. The Proactive Intelligence Methodology class outlines the approach utilized to anticipate and prevent cyber threats, whereas the Benefits class highlights the advantages of employing this tool. The Potentiality and Challenges class provides a comprehensive analysis of the tool's capabilities and limitations, and the Cyber Intelligence Tool class describes the type of cyber intelligence collection utilized to procure threat intelligence.

Cyber HUMINT refers to collecting intelligence from human sources in the cyber environment. This method is particularly useful in determining the intentions of cyber threats, which cannot be found through other cyber intelligence methods. To ensure that Cyber HUMINT is effective, it is important to use technological advancements and have experts handle vast amounts of data. However, because Cyber HUMINT is centered around humans, ethical considerations must be considered to ensure cybersecurity. While Cyber HUMINT is a powerful tool for gathering intelligence, it should only be used as part of a comprehensive cybersecurity strategy and not as a lone intelligence collection type. Cyber HUMINT is also used for digital forensics, investigations, and counterintelligence and is often combined with other intelligence collection methods in the cyber domain.

Cyber HUMINT, a "Proactive, Compliant, and Scalable Cyber Intelligence Tool," helps organizations stay ahead of cyber threats and attacks. It detects potential threats before they can cause damage and complies with industry standards and regulations. It can be customized to meet the changing needs of the environment. This tool complements cybersecurity strategy as it provides a perspective on the human domain in cyberspace.

4.3 Proactive Cyber Human Threat Intelligence

Cyber HUMINT is proactive cyber human threat intelligence. It focuses on gathering information about threat actors and a threat landscape from humans in a digital environment. The cyber intelligence gathered from the human domain helps organizations stay ahead of potential cyber threats by providing valuable threat intelligence to support the development of effective strategies to prevent cyber-attacks.

Next, I conclude the key aspects of cyber HUMINT as a proactive cyber human threat intelligence. It combines covert human threat intelligence professionality" with a proactive, compliant, and scalable cyber intelligence tool. Cyber HUMINT involves collecting information about the threat landscape and threat actors in the digital environment from humans. In the human domain social engineering is a crucial technique used in cyber HUMINT, as it combines traditional

intelligence methods with manipulating individuals to gain access to sensitive information or perform actions. Cyber HUMINT involves activities such as recruitment, building relationships, infiltration, and analysis, which use human operatives to collect intelligence. This approach provides valuable insights into the intentions of threat actors, which can help make informed cybersecurity decisions. Cyber HUMINT requires appropriate training, ethical considerations, and technological advancements to be successful. It is often used with other intelligence collection techniques, such as digital forensics, investigations, and counterintelligence, to enhance cybersecurity efforts.

5 DISCUSSION

The focus of this research was the crucial role of human intelligence in the digital age, particularly in the realm of cybersecurity. The study delved into the concept of "cyber HUMINT". The investigation involved analyzing web content from cybersecurity institutions to understand how human intelligence is integrated with digital technologies and used against malicious threat actors. Through a content analysis, this study drew on various web sources on cyber HUMINT. The aim was to provide valuable insights into how human intelligence can function in a digitalized world and help improve organizational security measures, as well as to provide an answer to the research question, what is cyber HUMINT in cybersecurity.

The analysis concluded that cyber HUMINT is proactive cyber human threat intelligence, combining "covert human threat intelligence professionality" with a "proactive, compliant, and scalable cyber intelligence tool." Cyber HUMINT focuses on gathering information about threat actors and the threat landscape from humans in a digital environment.

The results explored the first category, "covert human threat intelligence professionality," in detail. This category encompasses a broad range of topics related to cyber HUMINT techniques used to gain insights into threat actors' intentions and the emerging threat landscape. The topics covered include the exploitation of the human attack vector, which involves identifying and targeting human vulnerabilities to gain access to adversarial information or systems. Denial and deception tactics, which involve the deliberate spread of false information or the concealment of information to mislead adversaries, were part of the covert human threat intelligence concept. The threat intelligence process is another key area covered in this category. This involves collecting, analyzing, and disseminating information about potential threats to an organization's security. Finally, the results gave the class “Professionals,” which refers to experts and operatives working in this field, including their skills, expertise, and challenges. Overall, this category provides a comprehensive overview of the methods and strategies used by cyber HUMINT professionals to protect organizations from increasingly sophisticated threats.

The results elaborated on the significance of proactive cyber intelligence gathering and its role in identifying potential cyber threats before they cause harm. The "proactive, compliant, and scalable cyber intelligence tool" category encompasses a methodology to stay one step ahead of cybercriminals. This category comprehensively explains the benefits, potential challenges, and techniques involved in collecting and analyzing cyber intelligence. Moreover, the results explain how cyber HUMINT is crucial in cyber intelligence gathering, for instance, by involving gathering information from human sources to identify potential cyber threats. The results also highlight the need for decision support to form strategies to prevent cyber threats, such as gathering threat intelligence to support implementing threat prevention measures. Individuals and organizations

can safeguard themselves against potentially devastating attacks by leveraging a proactive approach to cyber intelligence gathering. In addition, the results emphasize that developmental automation makes scaling cyber HUMINT operations possible. This automation can help streamline gathering, analyzing, and visualizing information, making it easier to identify potential threats and act quickly to mitigate them. However, the results also highlight the importance of considering cyber HUMINT's ethical and legal aspects. It is crucial to ensure compliance with the legal framework and avoid causing harm to individuals or organizations. Therefore, it is essential to consider cyber HUMINT's ethics and prioritize safety and security. Overall, the categories of proactive cyber intelligence approaches offer a comprehensive understanding of the importance of proactive intelligence gathering that is compliant with the law. The benefits of proactive cyber intelligence are leverageable but must ensure compliance and forethought of ethical violations of cyber HUMINT.

The content analysis answered the research question. Cyber HUMINT in cybersecurity is a proactive cyber intelligence tool to gather threat intelligence from threat actors about their intentions and knowledge about the current threat landscape. The traditional human intelligence collection methodology is being adapted to cyberspace. Cyber HUMINT combines two frameworks of intelligence and cybersecurity and uses HUMINT methodology together with cyber methods to combat cyber espionage and cybercrime. Methods and techniques used in HUMINT are adapted to cyberspace. Human sources are still very relevant in the non-traditional cyber environment. The process of digitalization involves adapting traditional human activities to a digital environment. The core tradecraft is human intelligence tradecraft. Psychological and cultural knowledge are relevant in the new environment. Human relationship-building skills and understanding human emotions and motives remain the main know-how in cyber HUMINT.

Data showed that private cybersecurity specialists use cyber HUMINT in their work. This is still a relatively small area of expertise, with different interpretations of what it entails. Consistency was found in the content on cyber HUMINT provided by the private security and cybersecurity organizations' web pages. To sell their products, these providers must explain what cyber HUMINT involves because many people are unfamiliar with the concept. The information available on this topic was useful for exploratory research. Expert interviews, operational logs, or real-life case studies are needed to study cyber HUMINT methodology in more detail. However, one of the challenges of researching this area is that the specific methods used are often kept secret. This is particularly true in the intelligence and private cybersecurity communities, where sharing trade secrets could give competitors an advantage or reveal sensitive information to adversaries.

The research used a qualitative content analysis method following the American tradition, which proved to be suitable for the research purpose. This was because there is no clear or fundamental definition of cyber HUMINT yet. The method was clear, streamlined, and data-driven, making it a great fit for the

topic. Sentences about cyber HUMINT were collected from various web sources and then broken down into simpler forms, grouping them into similar classes. The grouping process was repeated several times. This method allowed for transparent analysis from the original web page citations to the synthesized result. The analysis unit was chosen to be the form of a sentence, which set some restrictions on the citations used in the analysis. Therefore, the result could differ from an alternative analysis unit's usage. I used Grammarly, an AI-powered writing assistant, to correct my English. It has helped me review my written text's correctness and readability. However, it is not a content creator - it needs reasonably well-written text to analyze and give suggestions for improving the writing. Without qualitative content and precision, it could have given false information. It was a good aid to check on the quality of the written text.

The groupings of the conceptual classes were done in a data-driven way while trying to keep previous understandings from influencing the analysis. The groupings led to a more tactical side of cyber HUMINT and a wider view of the strategy and operation of cyber intelligence in the human domain. Different researchers could have different results, but those results would not be far from each other. Abstracting was a challenging process, but it concluded with the key aspects of cyber HUMINT that are definitive within the research task and answer the research question: "What is cyber HUMINT in cybersecurity?". Different research questions would have given a different conception of the phenomenon. The results now mirror the framework of cybersecurity.

Cyber HUMINT emphasizes the human domain of cyberspace and cybersecurity. We should consider a more human-centric view of cyberspace and cybersecurity. Cyber HUMINT weighed on the criticality of adversarial insights and intentions. Behind sophisticated attacks, there are human threat actors. It was interesting to see notions about the ethicality of cyber HUMINT. In covert cyber HUMINT, valuable insights usually require deceiving and exploiting human beings. Cyber HUMINT in cybersecurity could be considered counterintelligence, where the threat landscape is mapped proactively by engaging with the communities and networks of threat actors. It could be considered offensive cyber intelligence in the cybersecurity framework. Digital and cyber environments are evolving, and the technical side is being developed. The automation gives scalability and leverage for cyber HUMINT, which in digital environments would be the most effective development for any HUMINT activity because it is the environment of operations with access to big data. Cyber HUMINT emphasizes the human domain in cybersecurity, cyber intelligence, cyberspace, and the digital world.

Further research could be done regarding the methodology of cyber HUMINT using expert interviews and case studies, AI-enabled cyber HUMINT, the legality of cyber HUMINT according to Finnish law, and a theoretical view from a framework of the *cyberworld* (Lehto, 2015), and its *cognitive layer*, which would include the human domain to cybersecurity in the case of cyber HUMINT. Researching the methodology, effect of artificial intelligence, compliance and

ethics, and theoretical framework on the topic of cyber HUMINT would enhance our understanding of its place in Finnish cybersecurity.

6 CONCLUSION

This study explored how human intelligence collection functions in the digital age, particularly in the context of cybersecurity. It investigated the concept of cyber HUMINT in cybersecurity. By analyzing web content from cybersecurity organizations, the research aimed to understand how technology impacts human activity in ensuring security. The study utilized content analysis as the research method and drew on various academic sources on intelligence, HUMINT, cyber HUMINT, and cyber espionage. The goal was to show how human intelligence adapts and operates in a digitalized world, providing insights for enhancing organizational security measures.

This research explored the adaptation of traditional human intelligence collection to the digital environment in cybersecurity. The chosen research method was content analysis on cyber HUMINT, using data from published web content. The process involved limiting, reviewing, excluding, combining, encoding, and reporting the analyzed content. Data was collected from private security and cybersecurity organizations' websites to define cyber HUMINT in cybersecurity. The analysis followed American tradition, involving reduction, categorization, and abstraction to answer the research question. The synthesis of web content was presented in tables to identify similarities and differences in cyber HUMINT content. The saturation principle was used to determine data relevance.

The research question was appropriately addressed through content analysis. Cyber HUMINT is a form of proactive cyber human threat intelligence that concentrates on gathering information about threat actors and the threat landscape from humans in a digital environment. In the cyber domain, human threat intelligence assists organizations in staying ahead of potential cyber threats by providing valuable intelligence to support the development of effective strategies to prevent cyber-attacks.

This research focused on the importance of human intelligence in cybersecurity, specifically exploring the concept of "cyber HUMINT". The study analyzed how human intelligence is integrated with digital technologies to combat cyber threats. The findings highlighted the proactive nature of cyber HUMINT, combining covert intelligence techniques with scalable cyber tools to gather information on threat actors in the digital landscape. The research emphasized the significance of proactive intelligence gathering to identify and prevent cyber threats before they occur. It also addressed the ethical and legal considerations of cyber HUMINT. The study concluded that cyber HUMINT plays a crucial role in cybersecurity by gathering threat intelligence from human sources to enhance organizational security measures.

REFERENCES

Adeo. (2023). *The Vital Role of Human Intelligence (HUMINT) in Cybersecurity*. Adeo. https://adeo.com.tr/en/the-vital-role-of-human-intelligence-humint-in-cybersecurity

ADEO. (no date). *ADEO*. Retrieved 13.4.2024, from website https://adeo.com.tr/en

CQR. (no date). *CQR*. Retrieved 13.4.2024, from website https://cqr.company/

CQR Company. (2023). *HUMINT*. CQR. https://cqr.company/pentesting-process/humint/

CrowdStrike. (no date). *CrowdStrike*. Retrieved 13.4.2024, from website https://www.crowdstrike.com/en-us/

Cunliffe, K. S. (2021). Hard target espionage in the information era: new challenges for the second oldest profession. *Intelligence and National Security*, *36*(7), 1018–1034. https://doi.org/10.1080/02684527.2021.1947555

Cyber Cupula. (no date). *The Art Of Active Cyber Humint*. Cyber Cupula. Retrieved 5.4.2024, from website https://cybercupula.com/

Cyber Risk Gmbh. (no date). *Cyber Risk GmbH*. 13.4.2024, from website https://www.cyber-risk-gmbh.com/

Cyber Risk GmbH. (no date). *From Espionage to Cyber Espionage*. Cyber Espionage. Retrieved 7.4.2024, from website https://www.cyber-espionage.ch/

Cyberarch. (no date). *Cyberarch*. Retrieved 13.4.2024, from website https://cyberarch.eu/

Cyberarch Admin. (2021). *What is the importance of human intelligence HUMINT? - CYBERARCH*. Cyberarch. https://cyberarch.eu/our-blog/what-is-the-importance-of-human-intelligence-humint/

CyberProof. (no date). *CyberProof*. Retrieved 13.4.2024, from website https://www.cyberproof.com/

Dando, C. J., & Ormerod, T. C. (2020). Noncoercive human intelligence gathering. *Journal of Experimental Psychology: General*, *149*(8), 1435–1448. https://doi.org/10.1037/xge0000724

DeBolt, M. (2023). *Gaining the Intelligence Advantage with Cyber HUMINT - Part One*. Intel471. https://intel471.com/blog/gaining-the-intelligence-advantage-with-cyber-humint-part-one

Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. *Undefined*, 1–22. https://doi.org/10.1080/23738871.2021.2000628

Merriam-Webster. (no date). *Digitalization Definition & Meaning*. https://www.merriam-webster.com/dictionary/digitalization#medicalDictionary

Merriam-Webster. (no date). *Enable Definition & Meaning*. https://www.merriam-webster.com/dictionary/enable

Giannetakis, P., Iannilli, L., & Caravelli, F. (2020). Cyber Humint. A Behavioral Analysis Perspective. *American Journal of Multidisciplinary Research & Development (AJMRD*, *2*(11), 27–33. www.ajmrd.com

Gioe, D. V. (2017). 'The More Things Change': HUMINT in the Cyber Age. *Undefined*, 213–227. https://doi.org/10.1057/978-1-137-53675-4_12

Gioe, D. V. (2018). Cyber operations and useful fools: the approach of Russian hybrid intelligence. *Intelligence & National Security*, *33*(7), 954–973. https://doi.org/http://dx.doi.org/10.1080/02684527.2018.1479345

Gioe, D. V., Goodman, M. S., & Stevens, T. (2020). Intelligence in the Cyber Era: Evolution or Revolution? *Political Science Quarterly*, *135*(2), 191–224. https://doi.org/10.1002/POLQ.13031

Grey Dynamics. (no date). *Grey Dynamics*. Retrieved 13.4.2024, from website https://greydynamics.com/

Hacktoria. (no date -a). *Hacktoria*. Retrieved 13.4.2024, from website https://hacktoria.com/

Hacktoria. (no date -b). *Utilizing Social Engineering Techniques in HUMINT*. Hacktoria. Retrieved 5.3.2024, from website https://hacktoria.com/social-engineering-humint/

Hadzipasic, A. (2021). *Automating Cyber HUMINT Collection*. SOS Intelligence. https://sosintel.co.uk/automating-cyber-humint-collection/

Hirsjärvi, S., Remes, P., Sajavaara, P., & Sinivuori, E. (2009). *Tutki ja kirjoita* (15. uud. p.). Tammi.

Intel471. (no date). *Intel471*. Retrieved 13.4.2024, from website https://intel471.com/

Johnson, L. (2010). Evaluating "humint": The role of foreign agents in U.S. security. *Comparative Strategy*, *29*(4), 308–332. https://doi.org/10.1080/01495933.2010.509635

Lehto, M., & Neittaanmäki, P. (2015). *Cyber security : analytics, technology and automation*. Springer International Publishing.

Lenaerts-Bergmans, B. (2023). *What is Human Intelligence (HUMINT) in Cybersecurity?* Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/human-intelligence-humint/

Lowenthal, M. M. (2017). *Intelligence : from secrets to policy* (Seventh ed). CQ Press.

Lowenthal, M. M. (2020). *Intelligence : from secrets to policy*. SAGE/CQ Press.

Lowenthal, M. M., & Clark, R. M. (2016). *The five disciplines of intelligence collection*. CQ Press.

Magee, A. C. (2010). Countering nontraditional HUMINT collection threats. *International Journal of Intelligence and CounterIntelligence*, *23*(3), 509–520. https://doi.org/10.1080/08850601003798807

Mitchell, B. (2020). CORPORATE CYBERESPIONAGE: IDENTIFICATION AND PREVENTION PART 2. *https://doi-org.ezproxy.jyu.fi/10.1080/07366981.2020.1798595*, *62*(6), 1–14. https://doi.org/10.1080/07366981.2020.1798595

Momi, R. (2021). *HUMINT: The Human Intelligence Discipline*. Grey Dynamics. https://greydynamics.com/humint-the-human-intelligence-discipline/

Musco, S. (2017). The art of meddling: a theoretical, strategic and historical analysis of non-official covers for clandestine Humint. *https://doi-org.ezproxy.jyu.fi/10.1080/14751798.2017.1377367*, *33*(4), 380–394. https://doi.org/10.1080/14751798.2017.1377367

Prokofiev, E. (2019). *Leveraging Traditional Humint Methodologies in Cyberspace*. CyberProof. https://blog.cyberproof.com/blog/leveraging-traditional-humint-methodologies-in-cyberspace

Rapid7. (no date). *Rapid7* . Retrieved 13.4.2024, from website https://www.rapid7.com/

SOS Intelligence. (no date). *SOS Intelligence*. Retrieved 13.4.2024, from website https://sosintel.co.uk/

Steele, R. D. (2010). *Human Intelligence: All Humans, All Minds, All the Time*. http://www.strategicstudiesinstitute.army.mil/

Steinhart, A. (2014). The future is behind us? The human factor in cyber intelligence: Interplay between Cyber-HUMINT, Hackers and Social Engineering. *Списание Дипломация*. https://web.archive.org/web/20140903143855/http://diplomacy.bg/arch

ives/1190%0Ahttps://www.academia.edu/7432960/Cyber_Humint_article_end

Stottlemyre, S. A. (2015). HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence. *http://dx.doi.org.ezproxy.jyu.fi/10.1080/08850607.2015.992760*, *28*(3), 578–589. https://doi.org/10.1080/08850607.2015.992760

Tal, A., & Siman-Tov, D. (2015). *HUMINT in the Cybernetic Era: Gaming in Two Worlds*. *7*(3).

Teplow, N. (2018). *HUMINT: The Riskiest (and Most Valuable) Form of Cyber Intelligence*. Rapid7. https://www.rapid7.com/blog/post/2018/09/12/humint-the-riskiest-and-most-valuable-form-of-intelligence-gathering/

Treadstone 71. (no date). *Treadstone 71*. Retrieved 13.4.2024, from website https://treadstone71.com/

Treadstone 71. (2023). *Analyzing Targeted Cyber-HUMINT*. Treadstone 71. https://treadstone71.com/intelligence-briefs/analyzing-targeted-cyber-humint

Tuomi, J., & Sarajärvi, A. (2009). *Laadullinen tutkimus ja sisällönanalyysi* (6. uud. laitos). Tammi.

Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Uudistettu). Kustannusosakeyhtiö Tammi.