Human Intelligence Throughout History: An Analysis of the Changes in Human Intelligence Collection Techniques from the Cold War to the Present

July 2023

2673945L

21109290

82449305

Presented in partial fulfilment of the requirements for the Degree

Of International Master in Security, Intelligence and Strategic Studies

Word Count: 22,055

Supervisor: Dr. Erika Biagini

Date of Submission: 26th, July 2023

Abstract

This dissertation seeks to investigate how the human intelligence (HUMINT) collection field has evolved from the Cold War to the modern day. To conduct this investigation this dissertation will examine the HUMINT activities of three case study countries, the United States, Russia, and China. Along with the analysis of these case studies' HUMINT activities, this dissertation will also analyze how technology has changed over time to aid HUMINT in the digital world of today. This analysis serves to prove a pattern in the evolution of HUMINT activities along with the rise of new technologies. By analyzing patterns of the evolution of the HUMINT technology relationship, this dissertation will provide insight into the possible future of the HUMINT collection field.

Table of Contents:

1. Introduction:

1.1 Research topic and question:

Throughout history the concepts of different intelligence collection techniques have played vital roles in the intelligence field. As time went on, more and more intelligence collection techniques were developed to serve the evolving aspects of the Intelligence Community (IC). Today there are many different types of intelligence collection techniques ranging from the use of technology and technical tools, such as with the use of signals intelligence (SIGINT) and measurement and signature intelligence (MASINT), to the use of human sources conducting intelligence activities in human intelligence or HUMINT as it is referred to by scholars and the IC. All intelligence collection techniques have their own advantages and challenges that coincide with their use. Sometimes certain intelligence techniques are better suited to the situation at hand when compared to the use of other techniques. Often times intelligence collection operations involve

the use of multiple intelligence collection techniques. This allows for a more complete understanding of the intelligence operation.

This dissertation, while still mentioning the use of other intelligence collection techniques, will be examining the role that HUMINT as a collection technique has played and how it has evolved since the Cold War. Since the Cold War, there has been a significant increase in technological developments that have led to changes in the way intelligence collection is conducted. Even though HUMINT utilizes humans and not technology as a source of information gathering, it is still greatly affected by the evolution of technology. The aim of this dissertation will be to show the changes in the intelligence field regarding intelligence collection techniques, more specifically how the technique of HUMINT has changed with the rise of technology across the globe since the Cold War. Instead of looking at how the use of technology has eclipsed that of HUMINT, an argument sometimes made in the literature, in this dissertation I am going to look at how has technology impacted HUMINT - e.g., has HUMINT become secondary and lost its value in the intelligence collection field? Has HUMINT become more efficient thanks to the use of technological advancements? How has technology impacted the work of intelligence officers in the field? – by doing so through this dissertation, I hope to demonstrate that HUMINT is still crucially relevant in the field of intelligence collection today, despite the enormous advancements of technology. I believe that technology has advanced and evolved alongside HUMINT activities. I aim to prove that HUMINT has adapted to operate in a world of technology. The goal of this study is to assess the relevance of HUMINT aided by technology in intelligence operations and activities from the Cold War to the modern day and offer some speculations about the future of HUMINT.

1.2 Why this is important to examine:

This research is significant for a number of reasons. First, it is important to understand the world of HUMINT in the modern day and what has led to its current state. The intelligence collection field of HUMINT is a fast-paced environment that has evolved tremendously as time progressed and understanding the field is crucial to continue to conduct successful intelligence activities in the future. The increasing reliance of technology for intelligence purposes as time progressed since the Cold War has led to the decline of the role for more traditional intelligence collection methods, such as HUMINT. Yet, I argue that HUMINT still remains a key form of intelligence collection for more reliable intelligence, and to collect intelligence that the more technologically focused intelligence collection methods cannot collect.

Second, the use of HUMINT activities has been changed immensely since the Cold War. It is important to examine the changes in the use of HUMINT throughout history as it can shed some light on the possible future of the intelligence collection field today based on past historical trends. By examining the past, I hope to be able to see the trends of how intelligence collection techniques have changed. I hope to be able to see how the use of the different HUMINT collection techniques have changed and evolved, as well as see what has proven effective or ineffective. With the quick rise in the technological advances from the Cold Wat to modern day, perhaps intelligence will become technologically driven, leading the use of HUMINT activities to be used sparsely if at all. I do not think this is the case, but it is a possibility scholars should consider and discuss.

Third, it is important to consider the types of organizations that use HUMINT. How will they use HUMINT in the coming years? How can nations better prepare themselves for this ever-changing intelligence world? These are all important questions for the future of the IC that this dissertation hopes to provide

insight into. These predictions can be used to better prepare intelligence organizations for the future of the IC and its capabilities. HUMINT is too useful of an intelligence collection technique to disappear. Perhaps there will not be a disappearance in the use of HUMINT, but perhaps an evolution in the practice that will make HUMINT more reliant on technology. I am hoping to uncover this in this dissertation by examining the use of technology with HUMINT operations and activities.

Fourth, Examining the history of HUMINT is also beneficial when we consider one of the IC's most important teachers, intelligence failures. By examining past HUMINT operations we can see where and why they went wrong and learn from these past mistakes. These so called "lessons learned" are extremely valuable for the IC today. That does not mean this dissertation will only examine intelligence failures, intelligence successes can teach us many things well. Examining the past is what can help us grow today. We will be able to learn from these successes and failures.

1.3 Anticipated conclusions:

Throughout my research I anticipate discovering that HUMINT was one of the predominant intelligence techniques used during the Cold War, and then as time went on there was an increase in the use of HUMINT activities aided by technology. I do expect to find that the use of technological devices has also evolved with the evolution of the IC's needs and capabilities of HUMINT activities. I expect to find this as stated before, as time has progressed there has been an increase in the use of technology from the Cold War to today. I believe that these factors have in many ways directly and indirectly affected the intelligence field. While each of the case study countries, that will be mentioned later, are different geographically and politically, I expect to find unique evolutions in the use of HUMINT, along with similar ones. What I expect to be

different is the way that HUMINT activities are conducted, the number of HUMINT activities that have occurred, and how HUMINT has evolved in each of these countries. What I expect to be the same is that HUMINT was heavily used during the Cold War years of this study, and a that there was decline in the utilization of HUMINT activities with the more technical intelligence techniques becoming more prominent as time went on, proof that HUMINT has evolved in some manner or another. This can be shown by the lack of available information about the use of HUMINT activities as I move from the Cold War time period to the more modern period.

2. Literature Review

2.1 What is Intelligence?

Before this dissertation delves into the question of how HUMINT has changed over time and the role it has played, it would be beneficial to discuss what exactly "intelligence" means. In Michael Warner's *Wanted: A Definition of "Intelligence* he goes on to say that "In a business as old as recorded history, one would expect to find a sophisticated understanding of just what that business is, what it does, and how it works. If the business is intelligence, however, we search in vain" (Warner, 2002, p. 15). What Warner is trying to say here is that there are many different meanings and definitions of intelligence. In fact, there is no universally accepted definition of intelligence (Wheaton and Beerbower, 2006). Without an understanding of what intelligence is, how can we expect to be able to explain how it works (Warner, 2002)? A proper definition of intelligence should be able to encapsulate both the national/international security field and the IC, as well as the intelligence in regard to the business and law enforcement sectors (Wheaton and Beerbower, 2006). That is not to say that there have not been attempts to create one.

First, we can take a look at a definition from the man regarded as the father of strategic intelligence in the United States, Sherman Kent (Aclin, 2010). Kent was a history professor at Yale University and a member of the United States Central Intelligence Agency (CIA). He is best known for his literary works regarding intelligence analysis. Kent focuses on the informational aspect in his definition of intelligence stating "intelligence, as I am writing of it, is the knowledge that our highly placed civilians and military men must have to safeguard the national welfare" (Kent, 2015, p. 7). Kent's definition labels intelligence as knowledge, not just some information and data the way many other scholars define intelligence (Aclin, 2010). As we will see in the many definitions this dissertation will cover, intelligence can mean many different things and definitions turn to the use of the word "information" quite often. Intelligence cannot be looked at as just a bunch of information and data.

The United States CIA produces the most all source intelligence for senior United States policymakers. For obvious reasons one would think that this means that the CIA would have a robust and clear definition of what intelligence is. Unfortunately, this is not the case. The CIA, despite being one of the top intelligence agencies in the world and even having intelligence in their name, has a fairly short and simple definition of intelligence. This organization states that "reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us—the prelude to decision and action by US policymakers" (Warner, 2019, p. 16). Just like Kent's definition, this definition does not mention anything about the activities of intelligence. It does, however, mention the importance of foreknowledge.

Another definition we can look at is one offered by one of the former Deputy Director of the CIA, Vernon Walters. Walters defines intelligence as

"information, not always available in the public domain, relating to the strength, resources, capabilities, and intentions of a foreign country that can affect our lives and the safety of our people" (Aclin, 2010, p. 16). This definition of what intelligence constitutes is a bit more in depth than that of Kent's. It does a better job to highlight that the information intelligence collects is not always generally available to the public domain. One issue that John Aclin identifies in this definition in his *Intelligence as a Tool of Strategy* is that there is a lack of any mention of non-state actors (Aclin, 2010). Aclin believes this makes this definition an outdated one (Aclin, 2010). There is also the issue that this definition only mentions intelligence as a kind of information or data, it does not mention that intelligence also requires activity (Aclin, 2010). Intelligence requires certain kinds of activities to discover this kind of usable information.

The Next definition we can look at the definition that is provided by the Department of Defense (DOD) in the United States. The DOD defines intelligence as "the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas" and "information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding" (Warner, 2019, p. 16). While this definition does give a more in-depth description of what intelligence is by being the first one to mention some intelligence activities, such as processing and analysis, which are parts of the intelligence cycle, it does not help shed any light as to what intelligence is specifically meant to do (Johnson, 1986). That is what makes this definition incomplete like many others. It is, however, a better definition than the others provided which do not provide any sort of activity that intelligence involves. Mark Phytian and Peter Gill in their *Intelligence in an insecure world* state that it is the British intelligence agencies that label intelligence as not only information but also action (Phythian and Gill,

2018). As mentioned prior, a clear definition of intelligence should include what some of the activities of intelligence are. How can we keep expecting to define intelligence if we do not understand its activities.

Another definition from a United States intelligence agency of what intelligence constitutes is given by the Office of the Director of National Intelligence (ODNI). It states the following:

> Intelligence is information gathered within or outside the U.S. that involves threats to our nation, its people, property, or interests; development, proliferation, or use of weapons of mass destruction; and any other matter bearing on the U.S. national or homeland security. (ODNI Home).

Again, there is no mention here of intelligence activities. As I have stated before, how can one know what intelligence is when one does not even know what kind of activities are involved in intelligence. To put it simply, we cannot. An even bigger argument to the adoption of this definition is that it states that intelligence is United States focused. Intelligence is not limited to a single country or even state or non-state actors. Intelligence is used all over the world. If there is to be a universally accepted definition of intelligence it should be one that can be used by all entities, whether foreign or domestic.

Looking away from intelligence agencies definitions, Intelligence.gov in the United States made an attempt to define intelligence stating that:

> Intelligence is . . . a body of evidence and the conclusions drawn therefrom that is acquired and furnished in response to the known or perceived requirements of consumers. It is often derived from information that is concealed or not intended to be available for use by the acquirer. (Wheaton and Beerbower, 2006, p. 324)

Some Scholars, such as Kristan J. Wheaton and Michael T. Beerbower, in their *Towards a New Definition of Intelligence,* do not agree with this definition of what intelligence is. These two believe that the use of the word "evidence" may imply that intelligence is trying to establish a kind of truth, rather than having a focus on determining future events (Wheaton and Beerbower, 2006). As Sun Tzu once said, "what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge" (Tzu, 2009). Just as the CIA did, the great Chinese General Sun Tzu mentions the key word "foreknowledge". What he is trying to say here is that strong and useful intelligence is focused on predicting possible future events. Wheaton and Beerbower also do not like the use of the phrase "furnished in response to known or perceived requirements of consumers" (Wheaton and Beerbower, 2006, p 324). They believe that this almost labels intelligence as "some sort of library" (Wheaton and Beerbower, 2006, p.324). Another issue with this definition is that it makes it seem as if intelligence is only hidden and concealed information, similar to former Director Vernon Walters's definition. This is not true. Intelligence is not always information that is concealed or hidden, it can be public information as well. This is apparent when we consider the intelligence collection technique of open-source intelligence (OSINT). This is a useful intelligence collection technique when one is trying to uncover non-classified information. OSINT information is not hidden or concealed from the public as Intelligence.gov's definition of intelligence states.

It is also imperative that we take a quick look and consider the ways law enforcement agencies define intelligence. Firstly, we can take a look at the United States Department of Justice's (DOJ) definitions. In their 2003 National Criminal Intelligence Sharing Plan, it defined intelligence as "the product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities

suspected of being, or known to be, criminal in nature" (Wheaton and Beerbower, 2006, p. 327). Only shortly after the publishing of the 2003 National Crime Intelligence Sharing Plan, in 2004, the law enforcement community decided to adopt a new definition of intelligence in a report which was funded by the DOJ, the Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies. In this new guide, it states that law enforcement intelligence can be defined as "the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality" (Wheaton and Beerbower, 2006, p. 328). These definitions go further than just stating that intelligence is some sort of information (Wheaton and Beerbower, 2006). They even encompass some of the activities that intelligence requires better than the previous definitions, though the DOD still does a better job of describing these activities.

As it will be one of the case study countries for the research portion of this dissertation, I should also examine how Russia defines intelligence. The tricky part here is that Russia's intelligence agencies, such as the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), and the Main Intelligence Directorate (GRU), do not publicly state how they define intelligence. These agencies keep their definitions classified to protect their way of conducting intelligence a secret. This furthers the issue and debate on what constitutes how intelligence can be defined in terms of a universally accepted definition.

Another definition of intelligence that needs to be considered for our research is the definition China uses. Unfortunately, there is not much public information as to what exactly how China's government and intelligence agencies define intelligence. Interestingly enough, many scholarly works on Chinese intelligence are quite similar to the definitions of intelligence used by the United

States (Mattis, 2012). Chinese scholarly definitions of intelligence have a strong focus on the process of intelligence rather than the end result (Schwark, 2018). There are many different Chinese Scholars that define intelligence as "the end product of an analytical process that takes raw information and integrate it into a form that offers foreknowledge and guides decision making" (Schwark, 2018, p. 4). Again, just like the CIA and the great General Sun Tzu, China puts emphasis in that intelligence contains a sort of foreknowledge. This seems to be a recurring concept in terms of a definition of intelligence even internationally.

As discussed above there are many definitions, this section did not even come close to scratching the surface of the definitional debate of what intelligence can be defined as. After examining these many different definitions, we can see a few ideas that are shared in common in most of these definitions. The first being the idea that intelligence can be labeled a kind of knowledge or information. Intelligence can also be seen as not just something that is there, but rather something that requires action and certain kinds of activities to take place in order to become useful. Another point made is that intelligence is often times something that is not commonly accessible, other than with the use of OSINT of course. It is something more times than not that others prefer to keep a secret from those trying to collect it. After reviewing these definitions of intelligence, for this dissertation I should define what intelligence is. It should be one that utilizes concepts from the previous definition with an emphasis on the activities of intelligence, more specifically the activities included in the intelligence cycle. For this we can use the definition created by Mark Phythian and Peter Gill "Intelligence comprises 'the mainly secret activities – targeting, collection, analysis, dissemination and action – intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities" (Phytihan and Gill, 2018, p. 16). I decided to use this definition of intelligence as

it firstly includes some of the activities of intelligence, it is key to remember intelligence is not a thing that is just there. There is a process in making intelligence products. It also highlights the secretive nature of the information that intelligence utilizes. It mentions that intelligence is a kind of foreknowledge. Finally, it states that intelligence is used to enhance security and power relations by adversaries or others.

2.2 What is Human Intelligence?

Now that we have covered what intelligence is, or the many ways it can be considered, we should look at what does HUMINT actually mean, and what kinds of activities are involved in its use. HUMINT is one of the most difficult intelligence collection techniques and is one that requires a vast amount of time and resources to collect and analyze information (Margolis, 2014). It is the way of collecting intelligence through the utilization of human sources. HUMINT's activities tend to have a more secretive nature when compared to other intelligence collection techniques. Some of the activities that are involved are: espionage, diplomatic talks, manipulation, deceit, and recruiting foreign spies to conduct espionage (Sano, 2015). Therefore, the information that is collected through the use of HUMINT can prove crucial to intelligence operations.

This intelligence technique often utilizes the use of HUMINT agents also referred to as intelligence officers, who also act as spies and handlers (Margolis, 2013). An intelligence officer is someone who has official cover and may be located in a foreign state to conduct diplomatic talks or even recruit foreign spies for espionage purposes (Margolis, 2013). There are also intelligence officers that possess non-official covers. Unlike the official cover intelligence officers, non-official cover intelligence officers do not receive any form of diplomatic immunity in case their cover and mission are discovered (Margolis, 2013). For this reason, the operations conducted by the non-official cover officer are much

riskier. These individuals do not pose as government officials or employees as official cover intelligence officers may, they pose as the common man such as a businessman or tourist on vacation (Lowenthal, 2012). Just like official cover intelligence officers their role is to uncover sources with useful information in regard to their assignment (Margolis, 2013). An example of this is offered by Gabriel Margolis in his *The Lack of HUMINT: A Recurring Intelligence Problem* there could be an intelligence officer with a non-official cover that may attend a convention on nuclear energy and this undercover officer will create contacts with the convention's scientists that may aid in their nation's nuclear weapon plans (Margolis, 2013). These officers often times have to complete long intensive training courses that include skills such as learning foreign languages, how to conduct, detect, and evade surveillance, recruiting skills, communications equipment training, weapons training, and many more unique skills (Jones, 2010). These intelligence officers can provide states with valuable information that cannot be acquired with the use of technical sensors (Hulnick, 1999).

One of the key duties of these HUMINT intelligence officers is that they are in charge of recruiting potential sources of information. These officers have to identify, recruit, and manage human sources of intelligence (Margolis, 2013). They need to be aware of what kind of information they are looking for before they go to recruiting sources. It is also quite crucial that the intelligence officer has information regarding the potential source before making contact. They should know things such as, are they trustworthy? Can they provide the kinds of information that they wish to seek? How likely will they be to give them the information they would like? These are just a few of the things that an intelligence officer needs to know before even thinking about the possibility of making contact and recruiting a potential source. As will be mentioned more in depth later in this dissertation, OSINT will come in handy when researching potential targets

for recruitment. It is not an easy task getting someone to divulge national security information to a foreign country. A term often used in the IC when it comes to recruiting susceptible individuals is money, ideology, compromise, ego (MICE) (Burkett, 2013). All of these are factors that can play a large role when trying to persuade an individual to spy or give up information about their nation's or organization's security. After a source is recruited the intelligence officer needs to build a sense of respect between the recruited individuals and themselves. This is a crucial component to make sure that the recruit does not get spooked or even worse reports the intelligence officer to the authorities. Intelligence officers are also responsible for keeping these individuals safe and protected. This includes using things such as secure communication methods, codenames, encryption methods, and other counter methods that will aid the recruited individual from having their espionage activities discovered. These intelligence officers also provide these recruited individuals with training that will aid the individual in their abilities as a source of information. This training includes things such as operational security (OPSEC), collection techniques, intelligence reporting and many other things that will allow them to collect information and stay safe and hidden (Stark, 2018).

HUMINT also does very well when it is paired up with the use of other intelligence techniques such as SIGINT (Sano, 2015). It should continue to be used with other collection techniques. "Signals intelligence (SIGINT) is the interception and decoding of foreign electronic communications" (Turner, 2014, p. 234). This intelligence technique is made up from the use of communication intelligence (COMINT), electronic intelligence (ELINT), and telemetry intelligence (TELINT) (Margolis, 2013). HUMINT activities may be able to see the deeper intentions of an individual and SIGINT is able to confirm their intents through monitoring communications and their activities (Aid and Wiebes, 2001).

This allows for a deeper understanding of the situation. A more complete intelligence product is produced with less gaps in the information. These two also complement each other in that they can confirm the information that each has found respectively. Confirming information during intelligence activities and operations is crucial to a mission's success. HUMINT can also aid SIGINT, and of course vice versa, in selecting targets for SIGINT operations. HUMINT activities can help by identifying potential individuals, groups, or systems that SIGINT practitioners could benefit from (Sano, 2015). This also allows for the ability to inform SIGINT practitioners of the kinds of equipment, devices, and communication methods used by an adversary (Home). This is useful knowledge that can lead to SIGINT operations having much higher success rates. HUMINT can help start the intelligence operation and then SIGINT can start and finish their operation, and vice versa. Both of these allow for SIGINT practitioners to prioritize their collection efforts. According to John Sano in his *The Changing Shape of HUMINT* a large selection of SIGINT operations are made possible because of the use of HUMINT activities (Sano, 2015). For example, some SIGINT operations are able to occur since a human source had to be the ones to initiate the penetration system (Sano, 2015). Without this human source, the technical connection could never have been made thus making the SIGINT activity obsolete. HUMINT and SIGINT operations working in tandem should continue to work in this relationship.

Another intelligence collection technique that works well with HUMINT is cyber intelligence (CYBINT). CYBINT collection involves the collection and analysis of information and data related to cybersecurity attacks and other cyber related crimes (Kandiko, 2018). This intelligence collection technique helps to mitigate the influence of malicious cyber activities from adversaries. With the rise of technology cybersecurity attacks and cybercrimes have become more prevalent

(Lallie et al., 2021). HUMINT has the ability to provide assistance even in this modern-day cyber world we live in. Just as SIGINT can, HUMINT is able to aid in identifying potential threats. The human aspect provided here can allow HUMINT intelligence officers to identify possible individuals or groups who pose possible cyber threats. They are able to monitor suspected individuals and look into their possible intentions and reasons for committing these cyber-attacks. It is crucial that HUMINT intelligence officers be mindful of the possibility of insider threats that are high risk for CYBINT (Scott, 2013). By monitoring and examining the actions of suspected cyber threat actors the HUMINT intelligence officer is able to let CYBINT professionals know about these possible cyber threats. This makes it much easier for those conducting CYBINT operations. This helps CYBINT professionals in prioritizing who they should be watching for possible threats and act accordingly to prevent any damage that may come about from these malicious actors. HUMINT also has the added benefit of being able to perform behavioral analysis that these technical intelligence collection techniques cannot perform. This further allows intelligence professionals the ability to look deeper into the tactics, techniques, and procedures (TTPs) used by malicious cyber threat actors (Maymí et al., 2017). This can allow for HUMINT intelligence officers to collect information regarding the methods and ways of attack that the adversary is capable of conducting. They can also uncover the social engineering tactics utilized by the adversary, such as phishing, that can reveal some details about the adversary's potential targets as well (Hyat, 2023). This can help CYBINT practitioners to be able to better anticipate and prevent future cyber-attacks as well as inform and protect the potential targets.

HUMINT is not an easy collection technique to use. There are many challenges to its use. One of these challenges is that HUMINT is susceptible to counterintelligence (CI) efforts. Counterintelligence is the process of identifying

and countering adversaries intelligence activities (Turner, 2014). This provides a kind of security measure in regard to keeping secret information from getting into an adversary's possession. For example, if a foreign state knows the identity of an informant, they can make them feed false information to the intelligence officer handling them (Margolis, 2013). This can cause the intelligence process to become slower or even produce incorrect intelligence products. Events such as this have been common intelligence failures throughout the history of the CIA (Margolis, 2013). Another challenge that HUMINT faces is trust. When an agent goes undercover and infiltrates a group, such as a terrorist organization, there is suspicion and distrust for the undercover agent. In a situation like this the undercover agent may have to participate in illegal activities or, in worst cases, attacks to gain the adversary's trust. The intelligence organization that the undercover agent works, for obvious reasons, cannot condone these acts and most likely would have to shut down the HUMINT operation (Byman, 2014). But it is not only the case of the human source being trusted by the target, but the human source themselves may prove to be untrustworthy. As mentioned before, it is crucial to build a relationship of trust, mutual understanding, and respect when it comes to source recruitment. This can be a very challenging and time-consuming task as individuals may have their own motives and biases for agreeing to be a human source (Gioe, 2017). Sources may mislead or provide false information. This too can lead to incorrect intelligence products being produced. Validating the source to make sure they are credible and reliable is a challenge in itself. It is also no easy task to recruit a human source.

There is also the fact that humans, while as simple as we may think we are, are unpredictable in nature. As mentioned prior, HUMINT adds human behavior to the intelligence collection field. The tricky thing is that human behavior is complex, unpredictable, and ever changing (Thompson, 2014). This

can add many challenges to the HUMINT field. Selective memory is one of these challenges. A recruited human source may have trouble recalling the correct information that they have collected; these are often individuals who have never imagined themselves living this kind of lifestyle after all. At times the magnitude of what they are doing can become quite overwhelming which in turn can affect their performance in the intelligence collection process.

It is natural to expect someone who just recently became an intelligence source to forget pieces of information or even remember it how they believed it happened, rather than what actually happened. They may even disregard information that perhaps they find irrelevant but could have proved quite useful to intelligence analysts. It is the HUMINT intelligence officer's job to train recruited sources to remember the important information that is needed. They need to be clear in teaching the source what they would like them to collect on. It is also hard for individuals to completely eliminate their cognitive biases. Individuals will have their own prior ways of thinking and judgments. Biases such as confirmation bias, favoring information that supports preexisting beliefs, can have negative effects on the collection process making the information collected false or unreliable (Libicki, 2018). Perhaps a recruited individual may also feel the need to prove themselves, so they may look for easily accessible information, for this the source may end up having some form of availability bias. Availability bias is "the human tendency to overestimate things that can easily be imagined or recalled, and conversely, underestimate things than are not as easily imagined or recalled" (Yuill et al., 2007, p.7)

Keeping to the theme of the challenges human sources can pose, is that there are also emotional factors that play key roles. A human source can be affected by their emotions, both good and bad, during the collection process. Their fear and anxiety can get in the way of reporting sound, usable, and reliable

information. Fear can also lead these recruited individuals to hesitation when it comes to sharing information with their handlers. This is a high-risk form of collection so it is only natural that newly recruited sources are nervous about what they are doing as the consequences can be quite severe if caught. This is another point as to why it is so important for HUMINT intelligence officers to build a strong relationship of trust with these recruited individuals. All of these challenges can have great negative impacts on the intelligence collection process and even in some cases ruin HUMINT operations all together.

2.3 Ancient use of Human Intelligence: Egyptian Empire, Roman, and Ancient China:

Now that we have discussed what HUMINT means it would be beneficial to talk about its ancient history before we get to its use from the Cold War to modern day. One of the points this dissertation hopes to add to research is the possible future of HUMINT. Without talking about the early uses of HUMINT we will not be able to see how it has remained a crucial intelligence collection technique all this time. This is important to show that HUMINT has been around for a very long time and has remained a vital and useful intelligence collection technique throughout the passing of time.

First of the ancient civilizations I will mention is ancient China, who heavily relied on the use of HUMINT collection. This time period ranges from around 6,000 B.C.E to 220 C.E. Ancient Chinese HUMINT covered a vast number of activities. Firstly, to mention, ancient Chinese HUMINT involved the use of spies quiet frequently. These individuals would conduct operations in secret using covers such as merchants, scholars, and the common citizen (Sterckx, 2018). Spies had many purposes during this time period, one of these was for

military purposes. Spies would be sent into enemy controlled areas to collect information on things such as troop movements, supplies, and fortifications. Ancient Chinese spies and informants were also used for political reasons. They would be in charge of monitoring political activities, potential threats, and internal and external stability (Verstappen, 1999). These individuals were also in charge of conducting intelligence on the public to maintain a sense of loyalty and obedience. They would report any form of disloyalty or disobedience to the empire (Verstappen, 1999). This was key for the ruling party to monitor political discontent or possible uprising among the community.

Another ancient civilization to discuss is ancient Egypt which range from the Old Kingdom period, 2,700 B.C.E, to the New Kingdom period, 1,100 B.C.E. This time period was not very well documented for the use of HUMINT; however, it was still ever present and used. Research shows that the Pharaohs in ancient Egypt would often times deploy spies to collect intelligence in regard to neighboring kingdoms, internal threats such as rising rebellions, and external threats such as invasion (Breen, 2019). These spies would report on military movements, political alliances, and other threats to their kingdoms (Breen, 2019). A more specific case during this time period can be attributed to Pharaoh Thutmose III during his reign. Pharoah Thutmose utilized a large network of spies and scouts who would provide military and war intelligence during his expansion of the Egyptian empire.

Lastly, we can look at ancient Rome's use of HUMINT ranging from the Period of the Kings, 625 B.C, to the Imperial Rome period, 31B.C. HUMINT was heavily used during the ancient Rome time period. The Roman Empire saw the value of HUMINT and its capabilities for intelligence collection in regard to adversaries, potential threats, and political activities early on in history. Just like in ancient Egypt, ancient Rome also used spies and informants also known as

"delatores" during this time (Wedeck, 1945). The Roman Empire used HUMINT especially in their military reconnaissance. Unlike today where we have SIGINT and other forms of seeing the battlefield from a safe distance, the Roman Empire had to rely on these spies and scouts to look ahead to get an advantage on enemy troop movements and information about their size, fortifications, and supply routes. These informants would observe and watch for possible political rivals that may rise up and pose a potential threat. I believe that this played a key role in the Roman empire's ability to maintain its government's stability and power.

As we can see above HUMINT has been used for a very long time. HUMINT was very basic back in ancient times, with all three of these great ancient civilizations utilizing spies to conduct HUMINT activities. There was a lack of technologies that could aid these HUMINT practitioners during these times. And yet throughout the years it remained a crucial form of intelligence collection. The activities of HUMINT may not have changed much during these ancient times but this dissertation serves to show that in the many later years of the Cold War HUMINT activities have evolved as technology has grown. The use of the spy is still used during the Cold War to today, this will be shown later in this dissertation. If HUMINT was used in the distant past of ancient times and is still used today, I believe that it has proved its value as an intelligence collection method.

2.4 How the Rise in Technology has Changed the Intelligence and Security Fields:

As time has advanced so have the innovations in technology. These advances in technology have greatly impacted the intelligence and security fields. This has led to changes in the way things are done in the intelligence and security fields. Here I will talk about what I believe to be the three most influential technological advances that have emerged or grown since the start of Cold War

that impact the HUMINT activities of today. I will discuss both the positives and negatives they have brought to the intelligence and security fields, as well as their effect on the HUMINT collection field.

The first advance we should address is the rise of a more modern intelligence technique that was mentioned earlier, OSINT. OSINT is "unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question" as defined by Robert David Steele (Steele, 2007, p 129). OSINT provides information such as strategic, historical, cultural insights, infrastructure, current conditions, and commercial geospatial information (Steele, 2007). In fact, The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission) believes that intelligence analyst who use OSINT collection techniques have proven to be more effective than those who did not (Robb et al., 2005). OSINT has become quite a useful tool in the modern age and is still continuing to grow in use today. The rise of OSINT has led to a greater use of technology. OSINT can be done with the use of things such as the internet, social media, and other digital platforms (Gill, 2023). Since the rise of OSINT collection there has been a rise in the accessibility of information and data that can be utilized to serve the intelligence and security field. Things such as social media and the internet have made it much easier together large amounts of information in a short time frame and with the use of very little resources. This has aided the intelligence and security field greatly. Since professionals can utilize social media and the internet the intelligence collection process for OSINT is now cheaper and can pull a large amount of data in a quicker manner. OSINT has also led to a broader information network. These new networks are not the typical intelligence networks that intelligence agencies often rely on. They now have easier access to things such as public records, social

media as mentioned before, and other public information sources (Gill, 2023). This new scope allows for greater possibilities of more comprehensive analysis of the information.

While these two previous changes have been positives there are also negatives that have arisen with the use of OSINT. One of these negatives is that there has been a rise in misinformation and disinformation among the intelligence and security fields. As mentioned before, social media plays a key factor in modern OSINT activities and collection operations. The negative here is that not all information on social media is the truth. Adversaries can use social media to spread misinformation and disinformation online (Del Vicario et al., 2016). This can make it quite difficult for intelligence professionals to find reliable and usable information online. One can expect that these professionals now have to conduct more fact checking when finding this information online. This also means while social media and the internet are vast pools of information for intelligence professionals, they can also be quite misleading and dangerous to rely on.

Another negative may sound like a positive, but I assure you it is not. With this in mind intelligence professionals may very well be able to find vast amounts of information, but this may prove to be too much information. OSINT collection is quite susceptible to information overload. Information overload can be defined as "the inability to extract needed knowledge from an immense quantity of information for one of many reasons" (Nelson, 1994, p. 3). These intelligence professionals may very well find difficulties utilizing such vast amounts of information. Not all information found using OSINT can be deemed useful either. This may distract intelligence professionals from making the best analysis of a situation. This can later lead to delays and inaccuracies in the intelligence analysis process.

OSINT has directly affected the HUMINT collection field as well. Its use compliments HUMINT collection in the sense that it provides a way to confirm or validate the intelligence gathered by the HUMINT source (Bărbulescu, 2016). OSINT has also helped in aiding intelligence officers to conduct research to uncover possible sources of information (Gill, 2023). By using OSINT intelligence officers are able to research possible leads for information. They can do this by checking social media for prospective sources they can later look into. With a simple internet search intelligence officers can find a plethora of information on these sources. These officers can also use OSINT to see how reliable the information the source is by cross-referencing the information provided to see if it is true (Bărbulescu, 2016). There are also the negatives that the rise of OSINT has brought the HUMINT collection field. There is an increased risk to the OPSEC. OPSEC is crucial to every aspect of the intelligence field, without good OPSEC an operation cannot be successful. Since there is now access to public information with the use of OSINT it is possible for adversaries to be able to identify intelligence officers and their sources (Gill, 2023). This is a serious issue for those intelligence officers with non-official covers. For this intelligence officers need to receive quality training in how to remain hidden not only in the field but online as well.

The next evolution I want to highlight is the recent emergence of artificial intelligence (AI). AI can be defined as:

> The science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable. (McCarthy, 2007)

AI has the power to process large quantities of data and even notice patterns in this data faster than a human source could, and sometimes even noticed patterns a human could never notice. It can even make predictions just how a human intelligence analyst does. While the rise of AI in the intelligence and security fields is fairly new at the time this dissertation was written, there have been massive leaps in its evolution.

First to mention is that AI has changed the way that the intelligence and security field deals with mass amounts of data and information. As mentioned before AI has the potential to deal with large quantities of data all at once. Because of this AI can analyze large sets of information and big data much quicker and more efficiently than a human intelligence analyst could (O'Leary, 2013). AI can deal with pattern detection and conduct complex calculations better than humans can (Korteling et al., 2021). This allows for more efficient analysis when dealing with large sets of information. In fact, AI has been proven to make many different kinds of analytical judgments with high level of accuracy (Li, Keel, & He, 2018). This allows intelligence professionals to deal with large amounts of information all at once, thus allowing quicker analysis of the situation.

Another productive use of AI in the intelligence and security field is that AI has great use when it comes to cyber security. There has been a recent increase in cyberattacks in the modern age and the need for advanced cyberthreat securities has propelled the implementation of AI for this very reason. AI systems can detect and react to dangerous cyberattacks in a quick and efficient manner (Moisset, 2023). It is able to detect and nullify cyber-attacks that have the aim to deceive or mislead non-AI powered security measures. Just like before, AI's ability to detect patterns comes into play here too. AI is able to quickly detect patterns in cybersecurity attacks. As AI certain AI technologies learn to adapt, it may even be able change its defenses and counter such attacks all on its own (Moisset,

2023). This in theory eliminates the need of a human source to create new defenses.

AI is not a perfect tool, and most likely it will never be. While it may sound all great at first there are risks that come with everything, and the use of AI is no exception. The emergence of AI has also brought negatives to the fields of intelligence and security. One of the most impactful negatives that has been brought about is the rise of deepfakes or manipulation with the use of AI (Karnouskos, 2020). Deepfakes are videos, pictures, or even audio that, with the use of AI, places the image of one person's face or voice onto another person (Maras and Alexandrou, 2019). This is done by the AI system utilizing tools such as Google image searches and social media websites (Maras and Alexandrou, 2019). This negative possesses many challenges for intelligence professionals. It is becoming more and more difficult for professionals to be able to tell the difference between a deepfake and the real thing. With the use of deepfakes it is possible for adversaries to spread disinformation, just like with the use of OSINT (Karnouskos, 2020). For example, with the use of deepfakes one could in theory have one country's leader say things that they never said about another nation's leader, thus creating tensions between the two or even across the globe.

The next negative I will mention is that AI technology relies on the use of large and complete data sets. It is also quite challenging to obtain such large data sets especially when it comes to information that requires a clearance to access or is secure from adversary's hands. There are often times errors or inconsistencies when it comes to these large data sets, and it is these errors that can cause issues and confuse the AI technology. AI utilizes historical data, if that data is incomplete, it cannot later lead to less accurate analysis (Frąckiewicz, 2023). Without these large and complete sets AI is also subject to bias and discrimination. Without these, it can cause the results or findings the AI

technology uncovers to be biased or skewed. These can be biases such as racial profiling, gender biases, and many more.

The Rise of AI has also surprisingly affected the HUMINT collection field. As mentioned prior, one of the activities that is involved with HUMINT collection is scouting out potential sources to recruit. One positive that AI has brought to HUMINT is its aid in identifying these potential targets as sources of intelligence. AI technology can analyze information from multiple open sources at once, these are open sources such as social media accounts and internet searches of individuals (Pastor-Galindo et al., 2020). Much of the analysis done by AI for this task is done with OSINT, this furthers my point on the large impact that OSINT has had on the intelligence and security fields. The AI will identify individuals and groups that meet specific criteria. It even has the capabilities to assess a possible threat level and potential impact when it comes to recruiting an individual (Sridevi and Suganthi, 2022). This makes the selection of potential targets for intelligence officers to recruit much easier as it does one part of their intensive job for them. This can help to save time and resources, which is crucial to an intelligence officer, when it comes to uncovering individuals.

AI has also had negative effects on the HUMINT collection field. As with anything, overuse can lead to misconceptions and misunderstandings. AI use is no different. Overreliance on the use of AI in HUMINT operations can cause issues. HUMINT collection is a unique intelligence collection technique as it requires humans to be the source of intelligence, whether that be for information or the human subject performing the analysis of a situation. AI and its algorithms, as mentioned before, aim to process data, and identify patterns, it does not have the capabilities to fully understand context of specific situations, cultural nuances, or subtle and minor changes that HUMINT practitioners can notice (Dickson, 2020). There needs to be a sense of human expertise and judgment that AI cannot

currently fully replicate. Perhaps in the future it may be able to, but who knows? Without the human aspect HUMINT is not HUMINT it is another form of intelligence. This overreliance on the use of AI and its algorithmic analysis can lead to a lack of critical thinking which can lead to negative analysis and false intelligence products.

The final advancement in technology that has arisen in the intelligence and security fields I will mention is the rise of cybersecurity. As technology made advancements so did the ability of adversaries and criminals. It is estimated that cybersecurity first emerged around the 1960s (Warner, 2012). First, I should mention what cybersecurity is exactly as there is some controversy in defining this term just like the definition of what intelligence is. That being said, this dissertation will not be deep diving into that discussion, so I will provide the definition provided by Basie von Solms and Rossouw von Solms in their *Cybersecurity and Information Security – What Goes Where?*. In this they state, "we now define cybersecurity as that part of information security which specifically focuses on protecting the confidentiality, integrity and availability of digital information assets against any threats, which may arise from such assets being compromised via (using) the internet" (Solms and Solms, 2018, p. 6). Cybersecurity prevents adversary efforts to steal information, interrupt or hack key systems, and tamper with critical infrastructure.

Cybersecurity has brought about many changes to the intelligence and security fields, some positive and of course some negative. One of these positives attributed to the rise of cybersecurity is the bolstered defense capabilities that have come with it. Since there is now the increased risk of cyber-attacks intelligence and security agencies have both increased their defensive measures (Albahar, 2019). They have created stronger more robust encryption systems, authentication systems, and much more modern and secure communication

networks, just to name a few advancements made to increase cybersecurity measures. The emergence of cybersecurity has also brought about more advanced and comprehensive threat detection and prevention capabilities. With the creation of intrusion detection-systems (IDS), intrusion prevention-systems (IPS) intelligence and security agencies are able to use these to monitor their security in real time (Fuchsberger, 2005). This allows for the agencies to be able to interrupt or even stop cyberattacks before they occur or cause harm to the system. With the use of indicators of compromise (ICOs) agencies are able to notice patterns of attack as well as information on the actors attacking (Haber and Rolls, 2020). With this knowledge the cybersecurity team is able to bolster their defenses where they are needed to prevent further attacks from not just the current adversary, but future adversaries as well.

Another positive that has been brought about is the rise of cyber intelligence and cyber espionage. The rise in the use of cybersecurity has allowed for the creation of intelligence professionals who collect intelligence and information through cyber efforts. This is done by watching online activities of potential threats, such as suspected terrorist and criminal networks, this is similar to OSINT. Monitoring their activities in the cyber world can help give intelligence and security agencies a sense of the potential dangers they may pose. Cyber intelligence also benefits greatly from cyber espionage. Agencies may also choose to conduct cyber operations in infiltrating a target network. This is done by the use of methods such as hacking or malware implantation that allows for access to previously secured databases to collect intelligence (Bederna and Szadeczky, 2020). Often times the targets of cyberespionage are entities such as governments, organizations, or individuals with connections to crucial infrastructure (Bederna and Szadeczky, 2020).

To no disbelief there are negatives yet again. One of these inevitable negatives is that cybersecurity has brought about a new kind of threat and attack landscape. Previously intelligence professionals had to worry about other problems during intelligence operations, now they have to worry about how cyber-attacks can affect the operation in question. The digital and cyber worlds have kept growing since their creation back in the 1960s. Technological developments such as the rise of the internet, cloud networks, and the modern interconnected systems in cyberspace have brought about this new threat landscape. While greater connectivity may sound like a good thing, in the cybersecurity world it is not. Since the digital world of today is so vast and nearly everyone is connected in some way or another, smart phones, laptops, etc., this has increased communication and data sharing possibilities and possess as a great threat in this new landscape. Devices that are connected to a network are at risk for cyber criminals to pick them as targets for an attack. Attacks on one device can spread like a virus to other devices. These and many other systems can be utilized for malicious reasons by adversaries. Because of this, intelligence professionals have to spend time and valuable resources to combat this new threat. Adversaries are also adapting in their cybers attacks, this means intelligence professionals must stay ever vigilant in combating this new threat landscape.

Another negative to mention is that now intelligence and security agencies have to worry about the threats posed by advanced persistent threats (APTs). Hussin Jose Hejase, Hasan Kazan, and Imad Moukadem state that APTs are "prolonged and targeted cyberattack in which an unauthorized person (an intruder) gains access to a network and stays there undetected for a long period of time" (Hejase et al., 2020). It was first used by adversaries to use cyber espionage to steal information and data in regard to monetary gain (Jeun et al., 2012). APTs

are quite difficult to detect and that is because of their nature. It is their persistence and stealth that aids them in their abilities to avoid detection and cause harm. They utilize advanced evasion techniques, and anti-forensic measures to stay hidden, they even have the capabilities of expanding their access after initial access (Hejase et al., 2020, p. 1). This poses a huge problem as even if intelligence professionals discover the initial access point that does not mean they have defeated the APT. It requires a large number of resources and advanced threat intelligence to detect and combat these long-term cyber-attacks, making them a challenge and a nuisance for intelligence agencies and professionals.

One may think how can cybersecurity affect HUMINT which requires humans as the source? Just like everything else mentioned prior HUMINT does not say untouched by the rise of cyber security. In a positive way, as a way to combat cybersecurity there has been a rise to create more secure communications channels for HUMINT communications. These secure channels are crucial for HUMINT operations and intelligence officers. These communication channels are often encrypted making them more secure and allowing HUMINT intelligence officers to use them to discuss sensitive intelligence without worrying of being listened to. Encryption systems make the information that is sent unreadable unless the receiver possesses the correct decryption key to decipher the message. This means that even if the information the intelligence officer is trying to hand off is intercepted, without the proper decryption key it will become useless to the adversary. These encryptions work with many things such as video, voice calls, and file transfers. There are also methods of securing information that we as regular people can do without being HUMINT intelligence officers, and that is multifactor-factor authentication (MFA), commonly known as two factor authentication. This is when an individual needs to provide more than one form of proof to prove that they have proper access to the information. This proof can be

special time sensitive passwords or codes that can be sent to mobile devices or other devices. MFA adds an extra layer of security when passing information to make sure only the authorized personnel get access to it.

A negative aspect to the rise of cybersecurity and its effects on HUMINT is that of the increased digital footprint that is left behind by HUMINT intelligence officers in the modern day. Today there is a growing reliance on technology and that has increased all of our digital footprints. HUMINT intelligence officers do not escape this fate either. This increased digital footprint can cause issues during HUMINT operations, such as intelligence officers having a much harder time conducting covert intelligence gathering operations. By analyzing the online activities of suspected HUMINT intelligence officers, adversaries are able to identify who they may be. This is a very similar thing that intelligence officers do when trying to find potential sources of information. The cyber and digital worlds appear to be double-edged swords. The increased threat of the large digital footprint we all leave today has the potential to expose or uncover HUMINT intelligence officers and their assets, whom they need to protect, and the operation as a whole (Gioe, 2017). Increased digital footprints can also make it timelier for intelligence officers to vet potential sources of intelligence to see if they a truly trustworthy or not (Akhmetov, 2020).

As shown above, the change in technology has played a crucial role in changing the intelligence and security fields in both positive and negative ways. The advancements in technology that were mentioned are only a fraction of the changing technologies that have impacted the intelligence and security fields up from the Cold War to the modern day. There have been far too many advances and changes to discuss. OSINT, AI, and cybersecurity have all played crucial roles in the ever-evolving intelligence and security fields. While in the analysis of this paper I will mention and highlight the technological advances I have mentioned

above, I will also be examining other technological advances that have occurred from the Cold War to today in HUMINT activities and operations. This will be important to show the vast impact the growth of technology has had on the intelligence and security fields. In the following sections I will discuss the methodology I plan to use to analyze how technology has changed the HUMINT field from the Cold War to today, as well as some limitations I expect to find as I conduct my research.

3. Methodology:

For this dissertation I will utilize case studies as the method of research. These case studies will be from different countries and the HUMINT activities and operations they have conducted during three set time frames. Deciding to use multiple case studies will allow me to see how HUMINT has been used and how it has changed differently on the international stage. Not all HUMINT is performed in the same. It can change from agency to agency and from location to location. For this reason, I decided to use three different countries and their use of HUMINT as case studies. There is the added benefit of looking at how three different countries use HUMINT. The case studies countries I will be examining in this dissertation are the United States, Russia, and China though briefly as China tends to have less public information in regard to their HUMINT activities. I chose to examine these countries as they all are considered world powers and have powerful intelligence capabilities, especially when it comes to the use of HUMINT. They are also important international stage actors of recent events as this paper is written, the war in Ukraine (Russia) and rising tensions with the United States (China). I also expect these countries to prove quite interesting in their use of HUMINT and how they differ from one another. If they differ at all that is. It will be interesting to see how HUMINT has changed depending on the location and country history.

Now that I have settled on the case studies, I need to select a good time frame to examine the HUMINT activities and operations that have occurred. HUMINT activities during set periods of time. The time frames in question will be HUMINT activities from the Cold War (1947) to the present (2023). Between these two dates I will use three periods of time as mentioned before. The first will start in the 1940s and finish in 1998. During this period the Cold War took place and I believe this gives me plenty of HUMINT activities to examine. The second time frame will be from 1999 to 2015. There were many technological advancements and world events that the case study countries were involved in during this time frame. The last time frame I will examine will be from 2016 to 2023. This will show the modern use of HUMINT in today's age. Setting time frames to be examined will allow for ample research to be done. If the timeframes are too small there will not be enough historical evidence to analyze and vice versa, if the time frame is too large there is too much to realistically analyze. These time frames cover just the right amount of time to examine many changes but not too large to examine all the changes that have occurred throughout history. The Cold War is a great starting point as during this period there was a heavy reliance on the use of HUMINT collection techniques and there were great technological advances in the following years. This growth in technology is a great impactor in the change in the HUMINT collection field. Researching up to modern times will allow us to analyze how HUMINT activities are used today with the growth of technology. There is also the idea that with the examination up to modern times, depending on trends, hopefully, we may be able to anticipate possible changes for the future of HUMINT.

Lastly, to discuss this research I need to clarify what exactly will be examined and analyzed. This paper will cover many of the significant HUMINT activities conducted by the United States, Russia, and China. The research will

cover many wartime and non-wartime HUMINT activities from the Cold war until today. As mentioned before, since HUMINT can be paired well with other intelligence collection techniques, I will also discuss operations where HUMINT has played a role and was not the main collection technique used. For these operations I will also mention some of the technologies that were used to aid the HUMINT activity. As mentioned during the time frames that this analysis will cover there have been great advancements in technologies. These technologies will range from things such radio listening devices to things such as computer data programs. However, since I expect there to be a large overlap of the technologies used in one HUMINT activities when comparing it to the others, I will try not to repeat technologies where possible so I can examine a much larger scope of the different kinds of technologies that were used in each time period. The use of the United States, Russia, and China as case studies will also provide a plentiful selection of historical information that I can examine as I believe there have been many historical events that utilized HUMINT in each of these countries as time has progressed. To conduct this research there will be a reliance on the use of secondary sources such as scholarly articles, books, histories, etc. I will also reference non-academic sources because HUMINT is such a broad and secretive topic getting a larger scope will benefit the research. For these non-academic sources I will cross-reference and confirm them to confirm that the information states are true. Because of all of these factors there will be a plethora of information available to be analyzed on the use of HUMINT as time has progressed. This method of research should not cause any ethical concerns either.

4. Limitations in the Research I Expect to Find:

There will also be some limits due to the topic of this of this dissertation. There will be limited data available due to the secretive nature of the IC and intelligence operations. In the intelligence field many intelligence operations,

especially those of the HUMINT variety, remain classified, and/or undocumented. At the time this dissertation was written, some perhaps more impactful HUMINT operations may remain classified. Perhaps later these operations will become unclassified, adding more to the argument I am seeking to make. Because of this I may not be able to mention the most influential operations from the Cold War to modern times. I will only be able to provide contextual evidence based upon the HUMINT operations that have been unclassified and have available information for public access. I also expect that there will also be more information regarding HUMINT's use during the Cold War period and the 2000 to 2015 period when compared to that of the modern-day period. This again is caused by the secretive nature of the IC and HUMINT activities of these three countries.

There is also the limitation of the amount I am able to discuss in this dissertation. I will not be able to mention every change that occurred in the HUMINT collection field, technology is not the only thing that has caused HUMINT to evolve and adapt since the Cold War. There are also far too many HUMINT activities and operations that have taken place since the Cold War. I will only be mentioning those that are, as mentioned before, unclassified and what I deem to have the impact.

Additional challenges I may face is that both Russian and Chinese past and current intelligence activities and operations tend to remain classified or undocumented, unlike that of my other case study the United States. This may limit the research to have a more United States focus. Because of that, I may only really get to see how technology has changed the HUMINT collection field in the Unites States rather than globally. The United States is still a very large actor in the intelligence and security fields so I believe it will still add something to the field.

5. Analysis: HUMINT's History: Cold War to the Modern Age:

Now let us dive into the core analysis of this dissertation. Here I will discuss HUMINT operations and activities that have occurred since the Cold War to the modern day. To do this there will be three sections split into different time periods, 1940s to 1990s, 1999 to 2015, and 2016 to 2023 as mentioned in the previous section. This will show that HUMINT activities have continued to be used as time has progressed. I will also take a look at the technologies that were involved in aiding these activities and discuss how they have progressed as well.

5.1 1940-1998:

The United States:

Here I start my discussion on some of the HUMINT activities and operations that the United States was involved in during this time period.

The Berlin Tunnel Operation:

There were many HUMINT operations that were conducted throughout the Cold War period. The first operation I would like to mention is the Berlin Tunnel operation that occurred from 1954 to1956 with the joint effort of the United States and the United Kingdom (Central Intelligence Agency). Since Berlin was divided at this time, the western half being controlled by the United States, the United Kingdom, and France and the eastern half controlled by the Soviet Union, the West wanted to collect information about the actions and capabilities that the axis powers had in East Germany. The goal of the operation was to do just that, gather intelligence regarding the Soviet's and East Germany's activities in the East Berlin region (Central Intelligence Agency). A secret tunnel was built by engineers from both the United States and the United Kingdom starting near the American sector's border with East Berlin starting in an abandoned warehouse in the area (National Security Agency/Central Security Service, 2012). This allowed for the tunnel to be dug in secret. In fact, this

operation was kept so secret that it is most likely that it was on a need to know basis and only a few officials in the IC knew about its presence and the operation. The tunnel was quite long at an expected length of 1,500 feet (457 meters), ending near a listening post in East Berlin (Collier, 2018). This tunnel was engineered with its secret nature in mind. There were actions taken to minimize its noise and to minimize vibrations caused by its construction (Collier, 2018). Once complete listening and other surveillance equipment was installed inside the tunnel to conduct technical intelligence (TECHINT). TECHINT is an intelligence collection technique with a focus on collection information from electronic communications, satellite imagery and technical documents (Pike). It is made up of a few other intelligence collection techniques such as SIGINT, imagery intelligence (IMINT), MASINT, and OSINT. This operation proved to be quite successful. During its period of operation, the secret tunnel collected approximately 50,000 reels of audio tapes and around 40,000 hours of Soviet and East German conversations (Central Intelligence Agency). The conversations recorded proved to be quite useful as they contained information about enemies' military operations, troop movements, and activities (Central Intelligence Agency). Unfortunately, in April of 1956 the operation became compromised when a Committee for State Security (KGB) mole, George Blake, was found inside the British intelligence service. Blake informed the KGB about the tunnel during its planning stages, however the Soviets allowed by the production of the tunnel to protect Blakes cover as a mole (Central Intelligence Agency). In April that year the KGB acted on the tunnel by claiming they just then discovered its existence.

It was not just the TECHINT that was collected that made this intelligence operation a success, HUMINT played quite an important role in this operation too. HUMINT was present in the sense of recruiting and handling sources from

East Berlin and Germany to validate the information that the tunnel's intercepted with its equipment. Without the human aspect there would not have been a way to see if the collected information was even true, perhaps it was misinformation, remember as mentioned prior in this dissertation this is something that is often used to combat HUMINT activities. These recruited individuals also allowed the West to have access to information that would have been priorly inaccessible to them. This will be a common theme to find during the Cold War period. The information that these human sources provided often complemented the information discovered by the conversations collected in the tunnel (Collier, 2018). Analysts were able to see a clearer picture combining the information collected from the tunnel and the human sources. As mentioned earlier in this dissertation, this allows for a more complete analysis of the situation. Not only did the information collected from these human sources complement the tunnel's findings, but it was also crucial for confirming what was collected as well.

The Penkovsky Papers:

Next to discuss is the case of the Soviet military intelligence officer Colonel Oleg Penkovsky. While it is not a specific intelligence operation, the Penkovsky Papers proved the value of the use of HUMINT activities during the Cold War. Colonel Penkovsky was recruited by the combined efforts of the CIA and the United Kingdom's Secret Intelligence Service (MI6) back in 1961 as a spy (Scott, 1999). As a high-ranking military official with access to sensitive information, he was a great potential source for HUMINT intelligence officers to try and recruit. His thoughts were that the rising tensions for nuclear war between the two global superpowers, the United States, and the Soviet Union, could end up

leading to mass destruction and many lives lost (Scott, 1999). For this reason, he believed he could help to mitigate the chances of this happening by providing information to the West. The purpose of recruiting Colonel Penkovsky was to have him provide information on Soviet military capabilities, nuclear weapon developments, and intelligence operations. In fact, between 1960 and 1962 he supplied the west with around 10,000 pages of classified military material he had taken photos of (Scott, 1999). Just as the Berlin Tunnel operation came to an abrupt end, so did the Penkovsky Papers when the Soviet Union discovered that Colonel Penkovsky was providing classified information to the West. It is suspected that the KGB started to find the activities of the Colonel suspicious and decided to investigate him. October of 1962 he was arrested and accused of treason and passing on military secrets to the West (Dunns, 2013). He confessed that he had been proving western intelligence agencies with classified information. He was later sentenced to death in May of 1963 (Dunns, 2013). With Penkovsky dead so were the Penkovsky Papers as they later came to be known. His involvement with the western intelligence agencies was not made public until after his death.

There was quite a bit of HUMINT by the Colonel. He would smuggle things such as classified documents, photographs, and other useful notes to the West (Scott, 1999). These notes contained information about military plans and strategies (Scott, 1999). The information that he provided to the West was of great value too. His information proved useful in shedding light on Soviet Missile capabilities, strategic plans, as well as the way the Soviets assessed the West military capabilities (Scott, 1999). In fact, some of the information he provided included the documents to confirm that there were Soviet missile sites located in Cuba. This in turn can be attributed to the discovery of the Cuban Missile Crisis that occurred in 1962. Without the information collected and passed along by

Colonel Penkovsky the United States may never have located the missile launch sites in Cuba.

Technology was also used during this HUMINT activity. The use of photography played a major role in Colonel Penkovsky's contributions to the efforts of the West (Scott, 1999). He would take photographs of the prior mentioned materials, such as military plans and other classified documents. These photos were later sent to the West. For this he would use a miniature camera to covertly capture photos of the classified documents. This was common when it came to HUMINT operations during the Cold War (Blackstock, 1966). The use of the Minox subminiature camera is the most well-known miniature camera used by intelligence agencies during this period of time, and was used by Penkovsky himself (Fischer, 2023). It was so small it was even able to be embedded into the tip of a pen. Often times intelligence agencies would use technological devices such as this that were created by the agencies themselves to best serve the task at hand. Photography was not the only form of technology used in this HUMINT activity, there was also a reliance on encryption methods to make sure communication between the Colonel, the CIA, and MI6 was safe and secure. While the exact methods are not known to the public, during the 1960's a number of encryption technologies were commonly used.

Russia:

Now I will discuss some of the HUMINT activities and operations Russia conducted during this time period. It should be stated that in this section Russia will be referred to as the Soviet Union as it is Russia's predecessor and was known as the Soviet Union at the time. The Soviet Union also heavily utilized HUMINT during the Cold War as well.

Operation Raketno-Yadernoe Napadeni:

One of these HUMINT operations was Operation Raketno-Yadernoe Napadeni (RYAN) or operation Nuclear Missile Attack in English. Operation RYAN was a Soviet military operation that occurred during the 1980's. Its purpose was to be a precautious measure to counter any attempts of a preemptive nuclear attack from the United States and the North Atlantic Treaty Organization (NATO) (Shaefer, Jones, and Fischer, 2014). General Yuri Andropov had suspicion that the United States could be showing signs of planning a nuclear attack on the Soviet Union. Thus, operation RYAN aimed to enhance the intelligence capabilities of the Soviet Union to be able to better detect a possible nuclear threat from the United States and NATO (Shaefer, Jones, and Fischer, 2014). The Soviet Union's intelligence agencies monitored and analyzed signs of possible nuclear threats, these were signs such as military exercises, communication networks, and political talks (Shaefer, Jones, and Fischer, 2014). The close monitoring and surveillance done by the Soviets during the operation further increased and heightened the tensions between the West and the Soviet Union. This was a major intelligence operation for the Soviet Union as, for obvious reasons, a nuclear threat would have been devastating. The success that this operation had can be attributed to its well-kept secret. The Soviet public was not made aware that this operation was taking place until later in 1991 when the Soviet Union came to an end and the operation was unclassified.

The intelligence collected during Operation RYAN heavily relied on human sources that the Soviet Union's KGB and the GRU had recruited to spy (Jones, 2009). The use of human sources during the Cold War period was more prevalent on the side of the Soviet Union that that of the United States, rather the United States utilized defectors more often, such as Penkovksy (Macrakis, 2010). The Soviet spies would monitor diplomatic activities between the West and the Soviet Union for information about nuclear threat rumors and other information.

This was information about political developments, negotiations, and military actions. The United States was not the only power here to utilize informants and defectors during the operation (Cold War espionage 2020). The Soviet Union was always on the lookout for new outlets of information. These informants and defectors would prove as great new outlets into the United States and NATO for insider information. The Soviet HUMINT intelligence officers also deployed moles. A mole is a placed spy or HUMINT agent that operations inside another organization, such as military or intelligence agencies, and conducts secret espionage activities supporting the goals of another organization or government (Language of espionage). These undercover spies would infiltrate western intelligence agencies and government organizations and continue gathering intelligence while on the inside, similar to defectors.

Technology also played an important role in Operation RYAN. The utilization of listening devices and radio intercept stations allowed the Soviets to be able to pick up on radio transmissions, conversations, and telephone communications regarding information of possible nuclear threats. While the specifics of these listening devices used during this specific operation remain classified, during this time period Russian HUMINT agents used listening devices that were custom made for the operation. This allowed for the devices to stay hidden and undetectable while in use. They would be disguised as things such as pens, notebooks, and other common items. This is quite similar to the miniature cameras that were mentioned earlier. During this time period discreet HUMINT technologies appeared to be similar in design. These devices were able to uncover information on things such as military and nuclear threat related plans. The Soviet Union was able to collect similar information that other SIGINT devices could collect, while only using HUMINT technologies. IMINT was another kind of technology that aided the operation providing visual information to confirm

Soviet intelligence. This was done with the aid of satellites systems during this period (Jones, 2009). Most of the satellite reconnaissance done by the Soviets during this time was focused on the United States. Along with the use of satellites, the Soviet Union also employed aircraft for reconnaissance. This was done by equipping cameras and sensors onto aircraft. The aircraft would then fly over the area where there were suspected nuclear arms and photograph the area for further analysis. The use of IMINT was key for the Soviets to be able to visually confirm the possibility of a nuclear threat. HUMINT agents would then be able to confirm whether or not the images taken by these reconnaissance aircraft were true or not. This furthers the argument that HUMINT and other intelligence collection techniques can build off one another.

Resident Spies:

Another Soviet activity that involved HUMINT during this time period was their use of resident spies in the United States. These were different from the regular spy. Regular spies during this time were able to have diplomatic cover. These were individuals who lived in the United States and possessed the non-official covers that were mentioned in the early section. Also as mentioned prior in this dissertation, these non-official cover spies posed as ordinary citizens and lived ordinary non suspecting lives with fake identities, lives, and jobs to appear normal and to avoid suspicion (Brady, 2021). These resident spies, as I will call them, operated under the KGB's Directorate S (Riehle, 2020). It was the KGB that had the job of recruiting and training these individuals for spying. The targets of these resident spies were mainly government agencies, political organizations, and people with access to highly sensitive information (Llewellyn & Thompson, 2020). Their objective was to live amongst the American people and collect information for Soviet intelligence agencies, sabotage United States activities, recruit, and promote support for the Soviet Union in the United States. This was a

high-risk high reward tactic used by the Soviet Union. These resident spies had to maintain an airtight cover at all times to avoid detection. The high risk of capture could have led to the United States to collect information from interrogation of these individuals.

One of the most notorious examples of these resident spies was the married couple Morris and Lona Cohen. Both Morris and Lona were born in the United States and had Russian ancestry (Hagerty, 2016). They both also shared interest in the communist ideology that the Soviet Union was pushing. Because of this they were recruited by the People's Commissariat of Internal Affairs (NKVD) in the lates 1930's prior to the start of the Cold War (Carr, 2016). Later in the midst of the Cold War, the two moved to New York City to spy for the Soviet Union posing as a Canadian couple with their aliases, Peter and Helen Kroger (Carr, 2016). Here they posed as antique dealers, a great example of the kinds of jobs those with non-official covers pose as. Their main objective of spying was to collect information on the United States nuclear plans though contact with individuals and organizations involved in nuclear research. They would use HUMINT techniques such as the use of dead drops, which is where an undercover agent will physically deposit items containing information at a designated point that will later be retrieved by their handlers, to communicate and pass information on (Srinivasan, Dong, and Stavrou, 2017). It was not until 1961 that the British Directorate of Military Intelligence (MI5) discovered their extensive espionage activities (Hagerty, 2016). They were turned over to the United States where they were found guilty of espionage later the same year. Later in 1969 both Morris and Lona Cohen were exchanged in a spy for a spy type exchange. They were exchanged for Gerald Brooke, a British spy (Hawkins, 2013).

Technology was heavily used by the resident spies throughout the duration of the Cold War for collection purposes. The resident spies had to rely on

technology to have contact with their KGB handlers. Along with the use of the already mentioned dead drops, this communication was primarily done with the aid of shortwave radios (Barnes, 2020). Due to the secret nature of the resident spy the specific models and make of the shortwave radios used in operations are not known to the public. However, during this time there were a number of companies that were making shortwave radios that were often used by intelligence professionals and resident spies during this time. One example of the short-wave radios manufacturers during this time was Grundig radios and their Satelitt series. These shortwave radios would allow KGB handlers to send coded messages containing instructions and information. This method was crucial so they could keep their covers and remain undetected by the United States government. They also utilized the use of miniature hidden microphones and hidden cameras which allowed for quick and direct eavesdropping as well (Barnes, 2020). These devices were often used to pick up on information from meetings, on sensitive topics, and on personal information of targets. These hidden devices were often made quite small to avoid detection, some small enough to even be hidden inside a pen (Macrakis, 2010). The benefit of utilizing these microphones and cameras was that the target was completely unaware of their presence. However, the use of microphones did not stop at its mere presence in the room. Directional microphones eliminated the need for the listening device to even be in the same room as the conversation. These are special microphones that are able to collect audio samples at a specific point and help minimize background noise. They allowed for audio information to be collected at a distance and even through walls or other obstructions (Wiesen, 2023). Again here, the specifics of the make of these directional microphones still remain classified at the time this dissertation was written. There were a multitude of companies that were making directional microphones during the Cold War; however, it can be

expected that the Soviet Union utilized their research and development teams to manufacture this kind of equipment to be used by HUMINT agents in the field.

China:

Along with the United States and the Soviet Union, China had significant HUMINT activities during the Cold War period.

The Sino-Soviet Split:

As the Cold War progressed the Soviet Union and People's Republic of China's relationship started to deteriorate. These tensions took place from around the 1950s to the 1980s. Both powers were operated and run by communist parties, however this split was due to the fact that both powers had ideological differences in what communism should be, with Mao Zedong of China believing in the belief that a class system was more productive, and while Nikita Khrushchev believed that coexistence was the more productive form of communism. This would lead both Mao Zedong and Nikita Khrushchev to have power disputes between one another. Border disputes also added to the rising tensions between them, more specifically disputes over the Xinjiang region. China actively accused the Soviet Union of supporting separatist in the region. Needless to say, there were many contributing factors to the Sino-Soviet split.

Because of these high tensions mentioned above, HUMINT was used from both perspectives on one another during this time. On the topic of border security China integrated the use of border intelligence units alongside their patrols. These patrols would be responsible for monitoring intelligence activities on the border with the Soviet Union (Kovacevic, 2021). Intercepting communications at the border was key to their success as well. This spying at the border likely intensified the tensions between the two communist powers. China also relied on the use of spies and intelligence agents during this period of tension. These Chinese spies

would integrate themselves in Soviet institutions of education, government agencies, and diplomatic discussions (Llewellyn and Thompson, 2020). This allowed the Chinese spies to collect information such as the military capabilities of the Soviet Union in case the tension between the two became too great and conflict broke out, as it did in the conflict in the island of Damansky in 1969 (Chernysheva, Budykina, and Shadrina, 2021). Informants and defectors were quite useful as well, along with the use of the Chinese Communist Party (CCP) Networks. The CCP had officials and sympathizers who resided in the Soviet Union during the time of tension (Kovacevic, 2021). This allowed for greater insight into the political happenings in the Soviet Union at the time. China also used propaganda with disinformation to dissuade the Soviet people (Chang, 1995). The goal was to gain popularity in the Soviet Union amongst the local people. Informants and agents would spread false information regarding the Soviet Union to dissuade their supporters and make them think that China was doing the right things and that the Soviet Union had communism all wrong (Chang, 1995).

Technology was also used during this time of tension to aid HUMINT. The human sources that were used, spies and informants, had to use secure and covert communication methods as one would suspect. This is where the technology really shined. This was done with the use of encrypted telegrams and radio transmitters to keep the information secure, similar to their use by Soviet Union during this time period. China's research and development was very good at creating technologies with their use in military and intelligence activities in mind. This is a reoccurring technology that has been used throughout time as we will see in the following time periods. Just as the Soviet resident spies, the use of surveillance and listening devices were quite useful in this situation. These were

used the same way the Soviet Union used them, to collect audio information on unaware individuals of interest.

Since there was also so much information coming in, the use of computers for data management was crucial. These computers were nowhere near as advanced as they are today. China actually had less developed computer technologies, 15 years behind in fact, during this time when compared to the Soviet Union and the United States (Maier, 1980). During this time period, China had isolation from the West, this in turn led to the use of domestically produced computer technologies (Maier, 1980). The use of computers made it possible to store and organize data that could later be analyzed. The analysis of the data could also be done by advanced analysis programs on these computers. This significantly lowered the workload on HUMINT intelligence officers. The data here would be a database of other intelligence collection techniques that could all be cross-referenced with one another to build a more complete analysis of the situation.

As we can see above there have been numerous uses of a variety of HUMINT activities across the globe during the Cold War time period. The above verifies that HUMINT was used quite heavily during this time period. It also confirms that there has been a large number of technologies that have aided these HUMINT activities. These technologies played crucial roles in the HUMINT activities mentioned and in some cases were the tools that allowed HUMINT agents to collect information.

5.2 1999-2015:

In this next section I will discuss the use of HUMINT and the technology that has aided these HUMINT activities from 1999 to 2015. This time skip should allow me to see how HUMINT and technology have evolved as time progressed.

The United States:

Like the previous section I will start with the United States.

The Iraq War:

During this time frame, the United States, under President George W. Bush, was at war in Iraq starting in March of 2003. There were many HUMINT operations and activities that aided the United States during this war. The technology at the time was more advanced than that during the Cold War years. This new time frame will now allow us to see how the technology that is used to aid HUMINT activities has advanced. One of the major HUMINT activities that took place during the Iraq War was the United States recruiting potential sources of information (Immerman, 2016). This was done for similar reasons and in similar ways to how it was used in the Cold War. It was important for the United States to recruit sources to aid in information gathering. A vast amount of information could come from these insider sources. During the war the United States also conducted another type of HUMINT activity, targeted raids, and arrests. These allowed for the capture of individuals and were known as high-value targets (HVTs). These were individuals that held higher position in the Iraqi regime such as bomb makers and terrorist leaders (Narchet et al., 2015). For these raids and captures to happen, HUMINT identification had to happen first. Human sources provided intelligence officers with information regarding the locations of these HVTs. This information came in a number of ways such as defectors willing to share information, documents that were collected by field operatives, and even intercepted communications (Spy Resources). HUMINT was also used to give accurate real time communication during operations such as precision strikes on these HVTs and other insurgent groups.

Technology was more advanced at this time and was able to aid HUMINT in new more effective ways. One of the new more advanced technologies that came about during this new time period was the implementation of biometric data systems for identifying individuals (Hristova, 2014). Biometric systems utilize the unique physical characteristics of individuals for the use of identification, verification, or authenticating purposes (Dantcheva, Elia, and Ross, 2015). This includes information such as fingerprints, facial recognition, and even iris scanners (Dantcheva, Elia, and Ross, 2015). This information was recorded from individuals who were involved in HUMINT activities so they could be identified and verified later on. The collected information would be used to look at a database of known identities to see if the individual matched any of these wanted individuals (Phillips et al., 2000). This was key when it came to speedy identification and capture of known terrorists. It was later possible that these captured individuals became sources of information. The United States used multiple pieces of technological equipment to record this biometric data. The use of the Handheld Interagency Identity Detection Equipment (HIIDE) was often utilized in the field (Faddis, Howard, and Stracener, 2011). This advanced piece of technology was able to quickly capture biometric data such as iris and fingerprint scans. It was also used to quickly confirm or identify individuals a HUMINT agent may be in physical contact with. The HUMINT agents could also store basic biogeographic data such as their names, ages, and nationalities that could aid in better identifying the individual (Dantcheva, Elia, and Ross, 2015. The information recorded on these devices would be stored on a much larger database that would be used for identification purposes. Another new technology during this period was the use of more mobile technology. The use of these mobile devices allowed for quicker forms of communication that could be in real time. These mobile devices were technology such as small handheld radios, that allowed for direct and secure communication while in the field, or even mobile

cell phones (Baker, 2007). Devices such as the mobile cell phone were able to pass not only verbal communication, but they could also send information such as photos, videos, and audio recordings. This allowed for greater speed when it came to getting the information out to those who needed it who were out in the field (Baker, 2007). Mobile cell phones even played great roles in recruiting potential sources of information. The agents could establish a relationship between the potential source through the phone. They did not even need to have physical contact any more for this key component of source recruitment (Baker, 2007). For security reasons the intelligence officer could even stay anonymous while contacting the potential source and vice versa. These mobile devices also contained technology such as global positioning systems (GPS). This allowed the HUMINT agent and soldiers to be able to better understand the physical environment they were operating in (Murray and Scales, 2004). These GPS systems could be used while actively in the field with handheld devices such as Garmin, Trimble, or Rockwell Collins, all who manufacture handheld GPS devices suitable for warzones during this period. Knowing where they were and where they were going is crucial for any HUMINT agent, especially when planning an operation. They also had the capabilities to confirm other intelligence collection techniques information in regard to locations coordinates. The mapping applications that these devices had aided in providing visual confirmation with things such as pictures, with the cameras attached to the mobile phones, to confirm locations and coordinates (Baker, 2007).

Operation Red Dawn:

Another great example of the use of HUMINT was Operation Red Dawn, the operation to capture the former Iraqi president Saddam Hussein (Lawton, 2016). When the start of the war in Iraq occurred Saddam Hussein went into hiding. There was great value in the finding and capturing of the Iraqi president.

On December 13th of the same year as the start of the war, 2003, intelligence collection efforts helped the United States to identify and confirm the location where Hussein was hiding. The former Iraqi president was hiding near his hometown Tikrit (Lawton, 2016). He was found hiding in a spider hole, a concealed hiding place or underground bunker typically used for evasion or concealment, that a soldier discovered before leaving the site of investigation (Lawton, 2016). He surrendered with little to no resistance. This was a major turning point of the United States during the war in Iraq as it had tremendous effects on the morale of Saddam Hussein's Regime.

While it was not the only intelligence collection technique being used here, HUMINT played a vital role in uncovering Saddam Hussein's hideout location. One of the HUMINT methods that provided a great deal of information was the use of interrogations. Interrogations hold valuable intelligence and information, especially in times of conflict (Gallagher, 2011). The United States was able to capture high value individuals, such as some of those who made up part of Saddam Hussein's inner circle (USAICoE Command History Office, 2013). From these individuals they were able to gain information about the whereabouts of the Iraqi president's secret location. There was also vital information that came from the locals in Iraq (Lawton, 2016). It is quite important to build rapport with recruited human sources, this is also true when it comes to building rapport with the locals. This was specifically important when it came to the United States and their ability to conduct intelligence operations in the region. One thing to come out of this was the creation of intelligence collection points. These were areas in villages and towns where the local Iraqi people could come and provide information and stay anonymous. The better the relationship between the locals and the United States occupiers, the more information would be reported, in theory. These tips played a crucial role in finding Hussein's hideout.

Informants also played a role in the HUMINT process. The United States intelligence officers and military units were looking for possible individuals they could rely on for information. Defectors from Hussein's regime were also highly valuable here. They were able to provide a deeper understanding of Saddam Hussein's security levels. It also showed that he was growing weaker as a leader if his people were choosing to defect.

Technology aided the HUMINT activities during this operation as well. HUMINT field agents greatly benefited from the use of technology. The use of surveillance equipment aided field agents greatly. The use of cameras for documentation likely had a great impact on Operation Red Dawn's success just like with the Penkovsky Papers and the cameras used by the Soviet resident spies. The use of surveillance cameras helped out when it came to identifying and confirming possible targets for interrogation that were a part of Saddam Hussein's regime. It appears that the use of cameras by HUMINT agents has continued to be used as time progressed as they have proved a useful tool for the agent to collect information. Unfortunately for this analysis the type of cameras used for Operation Red Dawn still remain classified at the time this dissertation was written. Since he was hiding perhaps it was better for Saddam to move and operate under the shadow of night to avoid detection. The use of imaging technologies, such as thermal and night vision, negated the cover of the night (Murray and Scales, 2004). This allowed intelligence collection efforts to occur even at night. Similarly, to the Cold War operations, advanced communication methods were key for HUMINT agents operating in the field to be able to share the information they have collected safely and securely. The need for secure communication channels was quite pertinent to the success of the operation. This secure communication was accomplished in a number of ways such as the use of one-time pads. A one-time pad uses a random key to encrypt and then decrypt

messages that are sent (Froehlich, 2022). This software was incredibly good at generating random pad keys. Even if they somehow got their hands on the unencrypted message without the key, they could not decode the message. The use of encryption technology allowed the United States to protect information that was passed during conversations. Another way that the information was encrypted was through the use of radios that held encryption capabilities. These were often used by the HUMINT field agents and military personnel. The radio encryption technology allowed for secure communication channels. While the specific radios used during Operation Red Dawn remain classified, there were quite a few that were being used at the time. The use of radios allowed for real time communication for the operation, which as mentioned before is crucial for HUMINT agents in the field (Davidson, 2009). Another way of real-time communication that helped out was with the use of satellite communication systems (Davidson, 2009). By using these secure satellites with encryption capabilities, the United States was able to have secure communication channels even in remote environments. The use of these satellites allowed for HUMINT agents located in Iraq or another location to be able to communicate with intelligence command centers all the way in the United States.

Operation Neptune Spear:

On May 2nd, 2011, the United States conducted Operation Neptune Spear. This was the operation that led the long sought after death of the worlds most wanted man, Osama bin Laden. This was a significant intelligence operation for the United States's global war on terrorism. Through intense intelligence efforts the United States discovered that bin Laden was hiding in Abbottabad, Pakistan (Khokhar, 2011). After discovering the hidden location of his compound, the United States Navy's SEAL Team Six conducted a raid on the site. It was during

this raid where members of SEAL Team Six killed Osama bin Laden. After his death they were able to collect quite a large amount of intelligence materials such as hard drives and documents regarding valuable information on al-Qaeda (Govern, 2012).

HUMINT played an absolutely vital role in Operation Neptune Spear. HUMINT actually led to the most important piece of information in regard to the operation, the location of bin Laden's hidden compound. This was done by using informants to locate and track Abu Ahmed al-Kuwaiti, one of the couriers for bin Laden (Mcain, 2011). By tracking this human source, intelligence agencies, specifically the CIA, were able to locate where Bin Laden was hiding. Utilizing HUMINT agents like this also allowed for surveillance and reconnaissance around the suspected compound. These agents were able to assist in providing information on the local presence in Abbottabad. This allowed the planners of the operation to anticipate possible challenges that may arise during the operation. This allowed for a more concrete and plausible plan in case things went one way or another. While it is often an overlooked topic when it comes to intelligence operation, these agents could have learned about the sensitivities of the local people. This was important so that the operation could take place without making matters worse and minimizing the possibility of casualties in Abbottabad. This is crucial to keep in mind when conducting intelligence and military operations in a foreign country. The use of HUMINT agents also allowed for suspicions of bin Laden's location to be confirmed (McCain, 2011). These agents could travel to the suspected compound's location to verify it does in fact exist as a possible hiding spot.

Technology played a critical role in aiding the HUMINT aspect of Operation Neptune Spear. While the specifics about the use of technology remain classified, we can look at the typical technologies that were aiding HUMINT

during the time period. Secure communication methods were needed for HUMINT agents to share the information they had with intelligence agencies. A new technology that arose during this period was the use of virtual private networks (VPNs). A VPN is a technology that creates a secure encrypted connection in public space that allows for the sending and receiving of data safely (Gillis, 2021). They could even start masking their IPs which would have made it much more difficult for adversaries to trace the origins of the communication if it was ever discovered. During this period of time there was also the use of secure cloud storage platforms. These are online spaces where an individual or organization can store data and information on secure servers (Seelig, 2023). This allows the individual to be able to store pieces of information safely and securely such as documents, photos, and videos. The service that provides the cloud system storage provides quite strong encryption technology that protects both information that is stored and information that is being sent. Unfortunately, the specific cloud storage program that was used by the United States during this time remains classified. Around this time there were popular cloud storage programs such as the. This is just another example of a new way that HUMINT agents can keep the information they have discovered safe and secure during this time period when compared to the Cold War.

Russia:

Moving out of the Cold War era Russia still continued their use of HUMINT quite frequently.

The Second Chechen War:

During this timeframe Russia continued to utilize their HUMINT capabilities in the Second Chechen War which started in 1999 and lasted until 2009. This conflict was between Russia and the Chechen separatist in the region

of Chechnya. This war was started after a number of bombings took place in Russia and the suspected culprits were part of the Chechen separatist group (Chapple, 2019). After these bombings, President Vladimir Putin decided to make efforts to acquire this former territory back (Chapple, 2019).

HUMINT activities aided Russia in their efforts to regain the Chechen territory during this war. One of the HUMINT activities that was used during this conflict was the infiltration of the Chechen separatist rebel groups (Shuster). This allowed Russia to collect a significant amount of insider information. This was done in the classic HUMINT fashion, deploying HUMINT agents, recruiting insider sources, and the classic use of spies. These undercover agents often disguised themselves as locals in the region. This allowed for deeper covers and less suspicion of these individuals and their actions. Once inside the rebel groups these undercover agents would be collect information on the activities of the rebel groups as well as disrupt their activities covertly. Another type of undercover HUMINT agent that was used by Russia and would collect similar information is the double agent. A double agent is a person who seems to be working for one country or organization, as they can appear in business intelligence as well, who performs unsuspecting normal duties but is passing information or conducting espionage activities for the goals of another country or organization (Dimmer, 1955). These individuals were quite useful during this time as they were much harder to detect as they would still operate as active members in these rebel groups. While acting as active members for the rebels, they would pass information to Russian intelligence agencies. These double agents were able confirm the accuracy of information collected by the Russian intelligence agencies.

As one would expect, technology played a large role in aiding these undercover HUMINT agents and double agents. The use of updated counter-

surveillance technologies was also implemented. As time progressed from the Cold War so did adversary's abilities to detect undercover HUMINT agents. New technologies rose up to combat these new detection abilities so that HUMINT agents could continue to operate unnoticed. One technique in particular was the use of many different types of electronic countermeasure (ECM) technologies. This technology allowed the HUMINT agent to combat the surveillance devices that their adversary was using. One of these ECM technologies was the use of electronic jammers that were able to detect, locate, and disrupt counter-surveillance technologies (An introduction into jammers and jamming techniques, 2019). There were a number of types of electronic jammers that were used during this time period to combat detection capabilities. Communication jammers were used to disrupt any communication attempts the adversary was trying to conduct by emitting waves at the same frequency being used. (Jamming Devices: Communication Jammers " phantom technologies 2022). These effected electronics such as radios or other devices that did not utilize a wired connection. Another was the use of radio frequency detectors. These were portable pieces of equipment that could allow an individual to see radio signals of the surrounding area (How to use the power of RF detectors in protecting your security, 2023). The HUMINT agent would use these to see if there were any hidden microphones or other radio frequency emitting devices in the area of operation. These two technologies worked very well together. Using these frequency detectors allowed HUMINT agents to discover communication channels and the communication jammers could block these communications.

Russian and Georgian War:

Another situation that had Russia utilizing HUMINT activities was with their war against Georgia. To give some background on this confrontation, after the Soviet Union fell in 1991 the Georgian Soviet Socialist Republic separated

making their own country of Georgia. The two regions of South Ossetia and Abkhazia wanted to separate from Georgia as their own independent nations (Cohen, 2011). As time progressed the conflicts between Georgia and the two regions grew more and more violent. Russia provided support of the South Ossetia and Abkhazia regions and placed military personnel in the regions (German, 2018). As further conflicts erupted in 2008 Russia started to conduct military actions even behind the Georgian borders (Coffey, 2015). After Russian forces were able to capture the city of Gori, Georgia, the European Union (EU) established a ceasefire agreement (Georgia, 2008). Even though they were not supposed to, Russia later announced that they recognize the South Ossetia and Abkhazia regions as independent from Georgia. This most likely is what led to a decrease in international relations between Russia and the western countries.

As with any conflict between nations, there was quite a bit of HUMINT taking place during conflict. This conflict is a great example to see how HUMINT can be used alongside, military conflicts. Since this was a conflict over separation from Georgia, the local people played crucial roles once again in the HUMINT process. HUMINT agents were able to utilize these locals as HUMINT sources of information and disinformation as they still do today (Seskuria, 2021). These locals could provide information in regard to Georgian troop movements and even their military capabilities. Good relations with the locals were also a must for HUMINT agents here. Keeping good relations allowed for the HUMINT agent to maintain a cover identity while operating in the region where Georgian authorities patrolled (Phillips, 2011). It was also likely that locals could also prove to be sympathizers and agree with the Russian ideology of recognizing the two regions as separates from Georgia. These sympathizers were great targets for Russia to recruit them as sources of information. These HUMINT agents were also able conduct CI actions against the Georgian forces. It is possible that the people in the

South Ossetia and Abkhazia regions could have been sympathizers that could have provided Georgia with Russian insider information. To combat this, Russian HUMINT agents worked to spread misinformation and propaganda in the regions (Al Jazeera, 2008).

Technology greatly aided in Russia's HUMINT effort to support the separatist regions. Russian HUMINT agents conducted a large number of cyberattacks on not only the South Ossetia and Abkhazia regions, but Georgia directly (Hollis, 2011). These cyber-attacks were more difficult to counter during this time period as the threat was so new. As mentioned before, the rise of internet and social media played a major role in how technology has changed HUMINT as time progressed. Social media played a large role in the many activities during the conflict (DeKraker et al., 2021). This was a powerful new use of technology that emerged during this period. The HUMINT agents could monitor social media accounts to recruit potential sources of information, as well as spread misinformation as the Russians did (DeKraker et al., 2021). They could even use social media to vet potential sources and conduct backgrounds investigations on individuals. They could perhaps have monitored social media for post regarding Georgian military forces to monitor troop movements and their activities. Social media posts also allowed for HUMINT agents to identify and travel to confirm areas that may have heightened numbers of conflicts. If these areas were receiving heightened actions, it would be beneficial for the HUMINT agent to travel there to conduct intelligence collection operations. The use of analytical data programs also came about during this time. These programs greatly aided in HUMINT activities as well. Since intelligence collection at times can lead to massive amounts of information at once, HUMINT agents can have trouble making sense of it all. HUMINT agents can utilize their pattern recognition capabilities that have proved to be useful during military operations (McLemore and Lauzen,

2018). This can help to verify information quickly. HUMINT agents always need to confirm the information they collect as it may not always be true, disinformation and misinformation become key with the rise of social media during this time period. These kinds of programs allowed them to confirm their information with information collected from other intelligence collection techniques. With the use of pattern recognition and other collected information HUMINT agents are able to predict things such as possible movements of individuals of interest or possible events that may play out that could provide useful information. This allowed for more complete intelligence products and understanding.

China:

Much like the Chinese definition of intelligence, there is no unclassified information in regard to China's use of HUMINT operations during the years of 1999 to 2015. It can be expected that the pattern of the use of HUMINT by the United States and Russia can also be followed by that of China. China is known to have very strong HUMINT capabilities, and their secrecy in the matter is one of the factors that contributes the most to their strong capabilities.

5.3 2016-2023:

Let us skip ahead one last time to a more modern time frame, 2016 to 2023. The information during this time frame is not as clear as the prior time periods as most of the recent intelligence operations and activities still remain classified. That being said, HUMINT is still being utilized in these modern times and should be mentioned as well. This section will be a bit different from the previous sections. Due to the fact that Russia and China tend to be more secretive in their intelligence activities and that the nature of these HUMINT activities is also just as secretive I will not be mentioning the modern use of HUMINT by

these two countries. I will be mentioning the modern use by the United States, as something should still be said about the use of HUMINT in the modern day.

Monitoring North Korea and Their Nuclear Capabilities:

The United States continues to utilize HUMINT operations and activities today. This shows that even in the modern day of digital technology HUMINT is still a viable way to collect information. The United States continues to use HUMINT for a variety of reasons. As recent tensions have grown between the United States and North Korea, one of the ways HUMINT is used in the modern day is to monitor information in regard to the nuclear weapons program, their capabilities, and the intentions of North Korea. This is done by the United States by deploying HUMINT agents to monitor North Koreas nuclear facilities. This includes the close monitoring of individuals such as researchers, nuclear research centers, nuclear testing facilities, and production facilities as well. HUMINT agents will monitor the activities and research done at these facilities and keep a close watch on North Korea's nuclear capabilities. While in these facilities HUMINT agents are able to inform the United States on topics such as any new research North Korea has done and possible dates of weapons test. The United States also relies on the use of interrogations and interviews as methods to collect information regarding North Korea, much like what was used in the past by the United States. They still rely on this old HUMINT tactic. These interrogations and interviews can be from individuals who have had contact with those officials of North Korea or defectors who want to share information. This allows for insider knowledge to be collected. However, it is not that simple, those interviewed or interrogated need to be vetted as reliable sources and not an adversaries HUMINT agent feeding false information.

As expected by now with any HUMINT activity technology plays a role in aiding the individuals conducting the HUMINT activity. Technology in this case

seems much like the previous technology used. The use of communication technology plays a vital role here. There is still the need for intelligence activities, especially those of the HUMINT variety, to remain secret and covert. For this the use of encryption technology is still presumed to be utilized in the modern time period (Weinstein, 2023). Today there are many more unique ways to have these encrypted communications, such as mobile phone applications. These are applications such as Signal and Whatsapp. These examples use end-to-end encryption (Wegerer, 2023). This means that a message can only be seen by the original sender of the message and the one on the receiving end (Wegerer, 2023). Not even the messaging application company can access these messages (Wegner, 2023). This allows for secure information sharing between HUMINT agents and their handlers. It should be noted that this is not just used by HUMINT agents located in North Korea, the United States has many HUMINT agents utilizing these applications all over the globe. This is a great example of the use of modern-day technology being used by HUMINT agents to communicate in a safe and secure manner. Having these applications on one's mobile device would not raise suspicion either as they are also used quite frequently by the general public. The use of social media is huge all over the world today and is utilized for HUMINT purposes even more today than the previous time period. However, it is still used in similar ways and because of this I will not go into depth on its more modern use.

6. Gaps in the Available Research:

As seen in the analysis above there are some gaps in the research that could not be answered or examined at the time that this dissertation was written. As I conducted my research, I ran into a few limitations that I expected to encounter. The first thing I would like to mention is that exact information about HUMINT activities and what specific models or type of technology were being

used still remains classified and is not made known to the public. If I had access to this kind of information, it would have allowed me to examine the question more effectively in regard to the growth of technologies. I would have liked to be able to examine what companies' technologies were being used during these periods of time. This would have furthered my argument of technological evolution as I would have been able to discuss more information. Also, there is a current shortage of available the information regarding the HUMINT activities of Russia and China from the 2016 to 2023 time period. This limits my findings of modern day HUMINT to be attributed to the United States when the case is that all three of these countries utilize HUMINT today. Being able to discuss HUMINT from all three countries in the modern world would have allowed me to make a stronger argument about how much modern HUMINT has changed and how it is conducted today. I would have liked to discuss the current situation with the war in Ukraine, but there is currently available information regarding the use of HUMINT as it is so modern, currently taking place at the time this dissertation was being written, it remains classified and most likely will for a period of time.

There is also the issue that I have no way to tell if these HUMINT events I have mentioned were the most influential events to answer the question. It is likely that due to the secretive nature of intelligence operations and HUMINT activities, I was not able to report on the HUMINT activities that had the greatest impact for these case study countries. I had to use the declassified information that was available to the public. I would have liked to mention only the most important HUMINT events that occurred during these periods of time. It is most likely that the most influential HUMINT events will remain classified for some time. For this, I suggest that perhaps due to the fact that most of the more recent HUMINT activities and operations remained classified, perhaps as time progresses scholars can reexamine the same question I have sought to answer. Perhaps when they

attempt to examine the HUMINT events of the current times and the past there will be more publicly available information as HUMINT activities and operations start to become declassified.

7. Conclusion:

As shown in the above analysis, this dissertation has examined that HUMINT has been heavily used from the Cold War to the modern day by the powerful nations of the United States, Russia, and China. To answer my question stated in the beginning of this dissertation, that question being "Has HUMINT become secondary and lost its value in the intelligence collection field, I believe the answer to be no". As the analysis has shown, HUMINT has continued to be used to collect intelligence even though it was initial use is dated back to the times of ancient Rome, Egypt, and China. As we can see above the activities of the HUMINT collection technique has not directly changed all that much when we look at its use throughout the years, Cold War to modern day, covered in this dissertation. This goes against what I expected to find, that HUMINT activities would in fact change vastly. I believed that HUMINT activities would in fact grow and change as the capabilities of technology have grown. The use of HUMINT activities has remained roughly the same with these kinds of activities involving the use of the recruitment of human sources, defectors and informants, the classic spy, the use of propaganda to spread misinformation, the relationships with the locals in a HUMINT operation's area of operation, and other the HUMINT activities mentioned earlier in this dissertation.

To answer my second and third questions, "Has HUMINT become more efficient thanks to the use of technological advancements and how has technology impacted the work of intelligence officers in the field?", the analysis shows that many, if not most, of the technologies did not lead to HUMINT becoming obsolete at all either, rather they have improved its capabilities as time has

progressed as well. As I expected, the technology used during these HUMINT activities has evolved and has become more advanced. Many of the technologies grew into new ones and evolved as time progressed, this is very apparent when we look at how many of the HUMINT activities mentioned were aided by the use of encryption technologies. I would actually argue that encryption technologies, for communication purposes, have proven to be the most used technologies and evolved the most from the Cold War period to modern day. These encryption technologies have evolved from basic encrypted telegrams and radio transmissions of the Cold War period all the way to the more modern use of common mobile phone applications, such as Signal and Whatsapp, that possess encryption capabilities. There is also the evolution of imagery techniques shown in the analysis. As mentioned during the Cold War, to be more specific the Penkovsky Papers, cameras were used, and they continued to be used as time progressed. There is an obvious evolution present when we look at the use of simple miniature cameras used in the Cold War to the updated use of surveillance cameras used to find possible Saddam Hussein hideout locations, which in the end was a success. Another imaging technique that came about was the capabilities of these imaging devices to possess thermal and night vision capabilities, used during the hunt for Osama bin Laden. There is also the increased usage of satellite imagery and aircraft reconnaissance that aided HUMINT agents.

Communication devices also evolved from the use of shortwave radios to the use of more mobile communication technologies such as covert earpieces, portable handheld radios, and mobile cell phones. These cellphones also radios grew to have encryption capabilities as well. I believe this was a major factor in the change of ease of HUMINT activities as the agent could now communicate while out in the field more easily.

There have also been a number of more advanced technologies that have not evolved but rather have been created as time progressed. The first to mention is the rise of biometric data systems that started to be utilized during the period of 1999 to 2015. This was a great technological advancement for the HUMINT field. As mentioned, this made the source verification and vetting process much vaster. There was also the implementation of the GPS systems during the United States War in Iraq. This technology is implemented in many modern-day tools such as mobile phones and even personal cars.

Electronic Countermeasures (ECMs), such as the electronic jammers, Communication jammers, and radio frequency detectors mentioned, have also come into the world around the same time as these biometric data systems and GPS. These ECMs allowed for HUMINT agents to remain undetected and keep a low profile while conducting their duties. Social media has also risen exponentially with apps such as twitter, Instagram, and Facebook becoming almost a necessity in the modern age. Today it is a rare occurrence to find an individual who does not have any form of social media presence in their lives. These social media applications have made it much easier for HUMINT agents to uncover potential sources of information and conduct OSINT as mentioned prior. Lastly, the rise of analytic data programs has greatly impacted the HUMINT field. With the mass amount of information that HUMINT agents today can uncover thanks to the rise of OSINT collection, they needed a better way to be able to analyze and store such vast amounts of information. These programs did such that with their pattern recognition capabilities that were mentioned prior.

As mentioned before, I hoped to shed some possible light on the idea of the possible future of HUMINT activities and operations. After the analysis of the Cold War time period, all the way to that of modern day I believe I can make a few points I expect to see in the future of HUMINT. I expect that HUMINT

activities will continue to use human sources such as spies, defectors, informants, and local information. As this has been used since ancient times, I do not see these sources becoming irrelevant any time soon. Besides, without the use of humans in HUMINT it could no longer be referred to as human intelligence. I also believe that the value of encryption technologies will become more important as the capabilities of cyber threats grow in the digital age. The technologies mentioned in this dissertation such as communications technologies and social media will also continue to grow. As shown in the analysis the need for communication technologies is vital and has continued to grow since the Cold War period. For this very reason I do not expect them to stay stagnant. As I mentioned before it is quite rare, and even suspicious, to meet an individual who does not have any form of social media. Social media is huge in today's day in age, people use it for hours multiple times a day. I believe that it will continue to grow and allow for more OSINT information and data to become available to intelligence professionals. There may even be a rise in the use of AI and HUMINT that will be interesting to see. AI technologies are growing at a rapid pace, I would not be surprised if it started to aid HUMINT in more and more ways as its capabilities evolve.

After all of these technological advancements I still do not believe that the use of HUMINT for intelligence purposes will ever become obsolete, even in this technological and digital world we live in today that is bound to keep changing and evolving. "I don't think we'll ever see a lessening of the need for human intelligence collection. At least not in the foreseeable future, any future I can see, Former Director of National Intelligence James Clapper" (Eggar, 2023). HUMINT will continue to be aided by technology as both adapt to the ever-changing intelligence world. Technology is bound to advance in these modern times and with it so will the use of HUMINT. It has proven the test of time as a viable and reliable source of information collection. As the research has shown

technology has not led to the demise of HUMINT, it instead has continued to aid HUMINT operatives in their operations.

Bibliography

Aclin, J., 2010 "INTELLIGENCE AS A TOOL OF STRATEGY." Edited by J. Boone Bartholomees. *VOLUME I: THEORY OF WAR AND STRATEGY*. Strategic Studies Institute, US Army War College, 2010. http://www.jstor.org/stable/resrep12114.22.

Aid, M.M. and Wiebes, C., 2001. Introduction on the importance of signals intelligence in the Cold War.

Akhmetov, A., 2020. *Digital Footprint Intelligence Report*, *Securelist English Global securelistcom*. Available at: https://securelist.com/digital-footprint-intelligence-report/99452/ (Accessed: 26 July 2023).

Albahar, M., 2019. Cyber attacks and terrorism: A twenty-first century conundrum. *Science and engineering ethics*, *25*, pp.993-1006.

An introduction to jammers and jamming techniques, 2019. *JEM Engineering*. Available at: https://jemengineering.com/blog-an-introduction-to-jammers/ (Accessed: 26 July 2023).

Baker, R.O., 2007. Humint-centric operations: Developing actionable intelligence in the urban counterinsurgency environment. *Military Review*, *87*(2), p.12.

Bărbulescu, C., 2016, November. THE ROLE OF OSINT IN REINVENTING INTELLIGENCE. In *INTERNATIONAL SCIENTIFIC CONFERENCE STRATEGIES XXI. The Complex and Dynamic Nature of the Security*

Environment (pp. 249-255). Carol I National Defence University Publishing House.

Barnes, T., 2020, The Fight against Russian “Illegal” Spies in Great Britain During the Early Cold War.

Blackstock, P.W., 1966. CIA and the Penkovsky Affair:“A New Disservice for All Concerned”. *Worldview*, *9*(2), pp.11-15.

Burkett, R., 2013. An alternative framework for agent recruitment: From MICE to RASCLS. *Studies in Intelligence*, *57*(1), pp.7-17.

Breen, C., 2019. *Espionage in ancient egypt*, *Espionage in Ancient Egypt, Further readings*. Available at: https://reference.jrank.org/security/Espionage_in_Ancient_Egypt.html#:~:text=The%20pharaohs%20of%20ancient%20Egypt,current%20espionage%20techniques%20and%20tactics. (Accessed: 24 July 2023).

Byman, D., 2014. Intelligence Functions: Human Intelligence (HUMINT).

Chang, J.P.K., 1995. *Propaganda and perceptions: the selling of the Soviet Union in the People's Republic of China, 1950-1965*. Harvard University.

Cohen, A., 2011. *The Russian military and the Georgia war: lessons and implications*. Strategic Studies Institute, US Army War College.

Collier, J., 2018. The story of the Berlin Tunnel: What the operations narrative teaches us about covert conflict in an ongoing Cold War.

Davidson, J., 2009. *Army’s Radio Inventory provides depth of versatile solutions to combat scenarios*, *www.army.mil*. Available at: https://www.army.mil/article/25032/armys_radio_inventory_provides_depth_of_versatile_solutions_to_combat_scenarios (Accessed: 25 July 2023).

DeKraker, A. *et al.*, 2021. *The Russo-Georgian War: Russian influence*, *The Russo-Georgian War: Russian Influence | Small Wars Journal*. Edited by C. Reno. Available at: https://smallwarsjournal.com/jrnl/art/russo-georgian-war-russian-influence (Accessed: 26 July 2023).

Del Vicario, M., et al., 2016. The spreading of misinformation online. *Proceedings of the national academy of Sciences*, *113*(3), pp.554-559.

Duns, J., 2013. *Dead Drop: TheTrue Story of Oleg Penkovsky and the Cold War's Most Dangerous Operation*. Simon and Schuster.

Eggar, M., 2023 *The relevance of HUMINT in the digital era*, *Lobo Institute*. Available at: https://www.loboinstitute.org/the-relevance-of-humint-in-the-digital-era/ (Accessed: 26 July 2023).

Faddis, K.N., Howard, J.J. and Stracener, J.T., 2011, August. Enhancing the usability of human machine interface on the handheld interagency identification detection equipment (HIIDE). In *2011 21st International Conference on Systems Engineering* (pp. 305-310). IEEE.

Fischer, B.B., 2023. Penkovsky, the Spy Who Tried to Destroy the World. *International Journal of Intelligence and CounterIntelligence*, *36*(1), pp.156-178.

Frąckiewicz, M., 2023. *AI and Data Imputation*, *TS2 SPACE*. Available at: https://ts2.space/en/ai-and-data-imputation/ (Accessed: 26 July 2023).

Fuchsberger, A., 2005. Intrusion detection systems and intrusion prevention systems. *Information Security Technical Report*, *10*(3), pp.134-139.

Gallagher, M., 2011. *Human intelligence in counterinsurgency: persistent pathologies in the collector-consumer relationship*. Small Wars Foundation.

German, T., 2018. Russia and South Ossetia: conferring statehood or creeping annexation?. In *The Ukrainian Crisis* (pp. 155-168). Routledge.

Georgia, C., 2008. *Russia endorses six-point plan*, *Civil.Ge*. Available at: https://old.civil.ge/eng/article.php?id=19069 (Accessed: 25 July 2023).

Gill, P. and Phythian, M., 2018. *Intelligence in an insecure world / Peter Gill, Mark Phythian.* Third edition. Cambridge ;: Polity Press.

Gill, R., 2023. *What is Open-Source Intelligence?*, *What is OSINT (Open-Source Intelligence?) | SANS Institute*. Available at: https://www.sans.org/blog/what-is-open-source-intelligence/ (Accessed: 24 July 2023).

Gillis, A.S., 2021. *What is a VPN? definition from searchnetworking*, *Networking*. Available at: https://www.techtarget.com/searchnetworking/definition/virtual-private-network (Accessed: 26 July 2023).

Gioe, D.V., 2017. 'The more things change': HUMINT in the cyber age. *The Palgrave handbook of security, risk and intelligence*, pp.213-227.

Govern, K., 2012. Operation Neptune Spear: Was Killing Bin Laden a Legitimate Military Objective?. *Targeted Killings: Law and Morality in an Asymmetrical World*, pp.347-373.

Haber, M.J., Rolls, D., Haber, M.J. and Rolls, D., 2020. Indicators of compromise. *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution*, pp.103-105.

Hagerty, E.J., 2016. Operation Whisper: The Capture of Soviet Spies Morris and Lona Cohen.

Hejase, H.J., Fayyad-Kazan, H.F. and Moukadem, I., 2020. Advanced persistent threats (apt): an awareness review. *Journal of Economics and Economic Education Research*, *21*(6), pp.1-8.

How to use the power of RF detectors in protecting your security, 2023. *Cellbusters*. Available at: https://cellbusters.com/what-is-an-rf-detector/ (Accessed: 26 July 2023).

Hristova, S., 2014. Recognizing friend and foe: Biometrics, veridiction, and the Iraq War. *Surveillance & Society*, *12*(4), pp.516-527.

Hulnick, A.S., 1999. *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*. Greenwood Publishing Group.

Hyatt, K. and Levenson, Z., 2023. *Social Engineering Impacts on Government Acquisition*. Acquisition Research Program.

Immerman, R.H., 2016. Intelligence and the Iraq and Afghanistan wars. *Political Science Quarterly*, *131*(3), pp.477-501.

Jamming Devices: Communication Jammers " phantom technologies, 2022. *Phantom Technologies LTD.* Available at: https://phantom-technologies.com/jamming-devices-in-the-security-of-communication/ (Accessed: 26 July 2023).

Jeun, I., Lee, Y., & Won, D. (2012). A practical study on advanced persistent threats. In Computer applications for security, control and system engineering (pp. 144-152). Springer, Berlin, Heidelberg.

Johnson, L.K., 1986. Making the intelligence “Cycle” work. *International Journal of Intelligence and Counter Intelligence*, *1*(4), pp.1-23.

Jones, I., 2010. *The human factor: Inside the CIA's dysfunctional intelligence culture*. Encounter Books.

Karnouskos, S., 2020. Artificial intelligence in digital media: The era of deepfakes. *IEEE Transactions on Technology and Society*, *1*(3), pp.138-147.

Kandiko, U.L., 2018. Cyber Intelligence: Reinventing the wheel. *Triarius 34 Content*, p.27

Kent, S., 2015. *Strategic intelligence for American world policy* (Vol. 2377). Princeton University Press..

Khokhar, A.Y., 2011. Operation Neptune Spear. *Strategic Studies*, *31*(3), pp.109-123.

Korteling, J.E. (Hans). *et al.*, 2021. *Human- versus Artificial Intelligence*, *Frontiers*. Available at: https://www.frontiersin.org/articles/10.3389/frai.2021.622364/full (Accessed: 26 July 2023).

Kovacevic, F., 2021. The Soviet-chinese spy wars in the 1970s: What KGB Counterintelligence Knew, part III, Wilson Center. Available at: https://www.wilsoncenter.org/blog-post/soviet-chinese-spy-wars-1970s-what-kgb-counterintelligence-knew-part-iii (Accessed: 25 July 2023).

Lallie, H.S., et al., 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, *105*, p.102248.

Language of espionage (no date) *International Spy Museum*. Available at: https://www.spymuseum.org/education-programs/spy-resources/language-of-espionage/ (Accessed: 26 July 2023).

Lawton, J., 2016. Intelligence Planning and Methods Employed: Operation Red Dawn-The Capture of Saddam Hussein. *Journal Article| Mar*, *16*(3), p.48pm.

Libicki, M.C., 2018, May. Drawing inferences from cyber espionage. In *2018 10th International Conference on Cyber Conflict (CyCon)* (pp. 109-122). IEEE.

Li, Z., Keel, S. and He, M., 2018. Can artificial intelligence make screening faster, more accurate, and more accessible?. *The Asia-Pacific Journal of Ophthalmology*, *7*(6), pp.436-441.

Llewellyn, J. and Thompson, S., 2020. Cold War espionage, The Cold War. Available at: https://alphahistory.com/coldwar/espionage/ (Accessed: 26 July 2023).

Lowenthal, M.M., 2022. *Intelligence: From secrets to policy*. CQ press.

Machiavelli, N., 2009. *Art of war*. University of Chicago Press.

Macrakis, K., 2010. Technophilic hubris and espionage styles during the Cold War. *Isis*, *101*(2), pp.378-385.

Maier, J.H., 1980. Information technology in China. *Asian Survey*, *20*(8), pp.860-875.

Maras, M.H. and Alexandrou, A., 2019. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. *The International Journal of Evidence & Proof*, *23*(3), pp.255-262.

Margolis, G., 2013. The lack of HUMINT: A recurring intelligence problem. *Global Security Studies*, *4*(2), pp.43-60

Mattis, P., 2012. The analytic challenge of understanding Chinese intelligence services. *Studies in Intelligence*, *56*(3), pp.47-57.

McCain, J., 2011. Bin Laden's death and the debate over torture. *Washington Post*, *11*.

McCarthy, J., 2007. What is artificial intelligence.

McLemore, C. and Lauzen, H.,2018. *The dawn of artificial intelligence in naval warfare*, *War on the Rocks*. Available at:

https://warontherocks.com/2018/06/the-dawn-of-artificial-intelligence-in-naval-warfare/ (Accessed: 26 July 2023).

Moisset, S., 2023. *How security analysts can use AI in Cybersecurity*, *freeCodeCamp.org*. Available at: https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/#:~:text=AI%2Dbased%20solutions%20can%20provide,sensitive%20data%20and%20critical%20systems. (Accessed: 24 July 2023).

Murray, W. and Scales Jr, M.G.R.H., 2004. The Iraq war: a military history. *Canadian Army Journal*, *7*(3/7), p.4.

Nelson, M.R., 1994. We have the information you want, but getting it will cost you! held hostage by information overload. *XRDS: Crossroads, The ACM Magazine for Students*, *1*(1), pp.11-15.

O'Leary, D.E., 2013. Artificial intelligence and big data. *IEEE intelligent systems*, *28*(2), pp.96-99.

Pastor-Galindo, J., Nespoli, P., Mármol, F.G. and Pérez, G.M., 2020. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access*, *8*, pp.10282-10304.

Phillips, D., 2011. *Six Point Ceasefire Agreement between Russia and Georgia* (pp. 1-30). The National Committee on American Foreign Policy.

Phillips, P.J., Martin, A., Wilson, C.L. and Przybocki, M., 2000. An introduction evaluating biometric systems. *Computer*, *33*(2), pp.56-63.

Pike, J. (no date) *Intelligence*, *FM 2-0: Intelligence - Chapter 10: Technical Intelligence*. Available at: https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap10.htm?utm_content=cmp-true (Accessed: 26 July 2023).

Riehle, K.P., 2020. Russia's intelligence illegals program: an enduring asset. *Intelligence and National Security*, *35*(3), pp.385-402.

Robb, C.S., et al., 2005. The commission on the intelligence capabilities of the united states regarding weapons of mass destruction: Report to the president of the united states. *Commission on Intelligence Capabilities Regarding WMD, Washington, DC*.Dantcheva, A., Elia, P. and Ross, A., 2015. What else does your biometric data reveal? A survey on soft biometrics. *IEEE Transactions on Information Forensics and Security*, *11*(3), pp.441-467.

Sano, J., 2015. The changing shape of HUMINT. *Intelligencer Journal*, *21*(3), pp.77-80.

Schaefer, B., Jones, N. and Fischer, B., 2014. Forecasting Nuclear War: Stasi/KGB Intelligence Cooperation under Project RYaN. *The Nuclear Proliferation International History Project, Wilson Center. URL: https://www. wilsoncenter. org/publication/forecasting-nuclear-war (accessed: 15.08. 2016)*.

Schwarck, E., 2018. Intelligence and informatization: the rise of the Ministry of Public Security in intelligence work in China. *The China Journal*, *80*(1), pp.1-23.

Scott, L., 1999. Espionage and the cold war: Oleg Penkovsky and the Cuban missile crisis. *Intelligence and National Security*, *14*(3), pp.23-47.

Scott, L., 2013. Human intelligence. In *Routledge Companion to Intelligence Studies* (pp. 96-104). Routledge.

Seelig, J., 2023. *What is cloud storage? explained by a cloud expert*, *Ridge Cloud*. Available at: https://www.ridge.co/blog/what-is-cloud-storage/ (Accessed: 26 July 2023).

Seskuria, N., 2021. *Russia's 'Hybrid aggression' against Georgia: The use of local and external tools*, *CSIS*. Available at: https://www.csis.org/analysis/russias-hybrid-aggression-against-georgia-use-local-and-external-tools (Accessed: 25 July 2023).

Shuster, S. (no date) *Putin's Secret Agents: Torture Allegations by Chechen dissident*, *Time*. Available at: https://time.com/putin-secret-agents/ (Accessed: 26 July 2023).

Spy Resources (no date) *International Spy Museum*. Available at: https://www.spymuseum.org/education-programs/spy-resources (Accessed: 26 July 2023).

Sridevi, G.M. and Suganthi, S.K., 2022. AI based suitability measurement and prediction between job description and job seeker profiles. *International Journal of Information Management Data Insights*, *2*(2), p.100109.

Stark, B., 2018. *The Ultimate Guide to Human Intelligence (HUMINT)*, *Intelligence101*. Available at: https://www.intelligence101.com/the-ultimate-guide-to-human-intelligence-humint/ (Accessed: 26 July 2023).

Steele, R.D., 2007. Open source intelligence. In *Handbook of intelligence studies* (pp. 147-165). Routledge.

Sterckx, R., 2018. *The Chinese spying game has a long history*, *Engelsberg ideas*. Available at: https://engelsbergideas.com/notebook/the-chinese-spying-game-has-a-long-history/ (Accessed: 26 July 2023).

The Berlin Tunnel (no date) *Central Intelligence Agency*. Available at: https://www.cia.gov/legacy/museum/exhibit/the-berlin-tunnel/ (Accessed: 24 July 2023).

Thompson, T.J., 2014. Toward an updated understanding of espionage motivation. *International Journal of Intelligence and CounterIntelligence*, *27*(1), pp.58-72.

Turner, M.A., 2014. *Historical Dictionary of United States Intelligence*. Rowman & Littlefield.

Warner, M., 2019. Wanted: A definition of 'intelligence'. In *Secret Intelligence* (pp. 4-12). Routledge.

Warner, M., 2012. Cybersecurity: A pre-history. *Intelligence and National Security*, *27*(5), pp.781-799.

Odni Home (no date) Home. Available at: https://www.dni.gov/index.php/what-we-do/what-is-intelligence#:~:text=Intelligence%20is%20information%20gathered%20within,U.S.%20national%20or%20homeland%20security. (Accessed: 26 July 2023).

USAICoE Command History Office, 2013. *Operation red dawn nets Saddam Hussein*, *www.army.mil*. Available at: https://www.army.mil/article/116559/operation_red_dawn_nets_saddam_hussein (Accessed: 25 July 2023).

Wedeck, H.E., 1945. Ancient spies. Classical World, 39, pp.31-32.

Wegerer, L., 2023. *Signal vs. WhatsApp: How are they different and which is right for you?*, *VPNOverview.com*. Available at: https://vpnoverview.com/privacy/apps/signal-vs-whatsapp/ (Accessed: 26 July 2023).

Weinstein, G., 2023. *Encryption: The necessary tool for U.S. National Security and the Intelligence Community*, *Forbes*. Available at: https://www.forbes.com/sites/digital-assets/2023/05/07/encryption-the-necessary-tool-for-us-national-security-and-the-intelligence-community/?sh=42c6a30d72f2 (Accessed: 26 July 2023).

Wheaton, K.J. and Beerbower, M.T., 2006. Towards a new definition of intelligence. *Stan. L. & Pol'y Rev.*, *17*

Wiesen, G., 2023. *What is a spy microphone?*, *Easy Tech Junkie*. Available at: https://www.easytechjunkie.com/what-is-a-spy-microphone.htm (Accessed: 26 July 2023).

Verstappen, S.H., 1999. *the thirty-six Strategies of Ancient China*. San Francisco: China Books & Periodicals.

Von Solms, B. and Von Solms, R., 2018. Cybersecurity and information security–what goes where?. *Information & Computer Security*, *26*(1), pp.2-9.

Yuill, J., Denning, D. and Feer, F., 2007, January. Psychological vulnerabilities to deception, for use in computer security. In *DoD Cyber Crime Conference* (Vol. 2007).