Tomi Lindfors

ENHANCING DETECTION & IDENTIFICATION OF HYBRID WARFARE FROM CYBER SECURITY PERSPECTIVE

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Lindfors, Tomi
Hybridisodankäynnin havaitsemisen ja tunnistamisen kehittäminen
kyberturvallisuuden näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2022, 57 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Lehto, Martti

Hybridisodankäynti on noussut viime vuosina pinnalle mediassa ja tieteellisessäkirjallisuudessa, kun länsimaat ovat huomanneet sen tuomat haasteet ja mahdollisuudet. Hybridisodankäynnille ominainen piirre on niiden alati muuttuva toimintatapa ja samanaikaisesti tapahtuvat vaikuttamisyritykset eri kohteisiin. Tämän takia hybridisodankäynnin havaitseminen on erittäin hankalaa. Usein kerättyjen tietojen määrä esimerkiksi taloudellisen vaikuttamisen havaitsemisessa aiheuttavat ongelmia analysointiresurssien riittämättömyyden kanssa. Anomalioiden eli hyökkäyksen merkkien löytäminen valtavista tietomääristä voi olla hankalaa, vaikka tieto etsittävästä kohteesta olisikin selvä. Tämä luo selkeän tarpeen hybridisodankäynnin havaitsemisen kehittämiselle sekä tämän tutkimuksen tekemiselle. Myös hybridisodankäynnin termistön haastavuus ja vaihtelevat käyttötarkoitukset ovat nousseet ongelmaksi keskustelussa eri toimijoiden välillä. Termien yhtenäisyys auttaa viestinnän selkeyttämisessä ja näin myös toiminnan tehostamisessa. Tämän tutkimuksen tarkoituksena on selventää hybridiuhkiin liittyvässä keskustelussa käytettyjä termejä sekä selvittää vähintäänkin mahdollisia alustavia jatkokehityskohteita hybridiuhkien havaitsemiseen liittyen kyberturvallisuuden näkökulmasta haastattelemalla hybridisodankäynnintutkimuksen ammattilaisia sekä kirjallisuuskatsauksen avulla.

Asiasanat: hybridi, hybridisodankäynti, hybridiuhat, Venäjä, hybridisodankäynnin havaitseminen, hybridivaikuttamisen keinot, hybridivaikuttamisen havaitseminen

ABSTRACT

Lindfors, Tomi
Enhancing Detection & Identification of Hybrid Warfare from Cyber Security Perspective
Jyväskylä: University of Jyväskylä, 2022, 57 pp.
Cyber Security, Master's Thesis
Supervisor(s): Lehto, Martti

Hybrid warfare has surfaced in recent years in media and scientific literature, as the western world has noticed its challenges and possibilities. Hybrid warfare and its operations are by nature constantly evolving and changing while attempting to cause the wished effect on the victim. This causes the complications behind the detection of hybrid warfare. Often the amount of data gathered for analysis can cause issues because of its size as the resources for detecting hybrid warfare are limited. Finding anomalies from such large data sets can be problematic even if the target of the analysis is well known to the analyst. This creates a need for research to improve the detection of hybrid warfare. The terms behind hybrid warfare are also used differently by different parties and could use unification. The unification of terminology also helps to clarify communications between organizations and can directly benefit operational efficiency. The goal of this research is to clarify the terms used in the discussion about detection of hybrid warfare and to find at least preliminary future research topics for it from cyber security research point of view.

Keywords: hybrid, hybrid warfare, hybrid threats, Russia, detection of hybrid warfare, means of hybrid influence, detection of hybrid influence

FIGURES

TABLE OF CONTENTS

1 INTRODUCTION

This thesis is conducted to research possibilities to enhance detecting hybrid warfare from cyber security point of view. The research views the issues within hybrid warfare and its detection from a western point of view, but the results can be applied by anyone in order to enhance their hybrid warfare detection capabilities. The topic of the research is currently interesting as hybrid warfare is a popular topic in media and in research circles and it is also often used as a term in different ways by different entities. Hence the need to clarify the terms used in discussion about detecting hybrid warfare. Another reason that makes this topic interesting to research is that the creation of efficient detection capabilities can be difficult even with more resourceful nations because of its complexity (MCDC, 2019, s. 25). The lack of capabilities in smaller countries makes them an increasingly attractive target for hostile nations to use hybrid warfare. It could be, that nations with more resources do not care for these smaller countries and the fact that they are being targeted by hybrid warfare, but there is a possibility is that the unrest and problems caused by the hybrid warfare can also spread and affect the neighboring and allied countries which are connected in social or communicational ways. (Braha, 2012, s. 1). Lastly, the cyber security point of view was chosen to bring completely new ideas to enhance detection of hybrid warfare. Hence the topic is useful and interesting for research purposes.

The research itself is conducted by reviewing literature and interviewing experts. Literature review is especially important in this thesis because the researcher does not have significant experience in this field. The first part of literature consists of multiple high-level reports and papers from the EU and Nato. The other significant part is the papers written by some of the most established experts in the EU such as some researchers working for the Hybrid CoE. Lastly the cyber-security papers provide the background for the cyber point of view.

The goals for this research are to:

- Explain terms and literature behind the detection of hybrid warfare from the cyber security point of view.

- Describe the current situation of detecting hybrid warfare and explain the difficulties of the topic and effects of improving it.

- Finding possible improvements and new possibilities for detecting hybrid warfare through literature review and interviews.

1.1 Theme, background and effects of the research

This thesis builds on the Multinational Capability Development Campaign Countering hybrid warfare project report. The Multinational Capability Development Campaign Countering will be referred as MCDC in this thesis from here. The main goal of this research is to research new ways and ideas to enhance the detection of hybrid warfare through analysis of previous material and papers regarding this topic and through interviewing experts from the field of hybrid warfare. The current situation in the detection of Hybrid warfare is that the usage of traditional military detection and early warning methods are questionable at best in context of hybrid warfare. The modern hybrid warfare methods change constantly and therefore require a completely new way of viewing and chewing through the data (MCDC, 2019, s. 25).

The research is of qualitative nature as the object of the research is to study the phenonium of detecting hybrid warfare. It is conducted with interviews and literature review.

The aim of this research is to research the literature written on detecting hybrid warfare and the literature about detection in cyber security academic literature. The next phase is to interview experts on the topic of detecting hybrid warfare and how to improve it. The last part of this thesis focuses on drawing conclusions from the material gathered from these sources and potentially crafting preliminary ideas for further research in this field.

The topic of this research is important and provides value for the following reasons. First, the main goal of this research is to develop topics to drive further development in the detection of hybrid warfare. This is done through expert interviews and literature review. The second goal of the research is to clear terms from hybrid warfare. As noted by Benson in the interview conducted during this research, the inefficacy in use of terms decreases the efficiency of communicating between analyzing or decision-making parties and inefficient communicating was one of the major key improvement points named by interviewed when asked about shortcomings in detecting hybrid warfare. (D. Benson, interview, 21.04.2022). By unifying and simplifying the terms in hybrid warfare, we can also increase the efficiency of detecting it. Lastly, it provides a bridge between cyber security research and hybrid warfare research. Previous research between these topics is largely based and focused on military sciences whereas this research focuses on the cyber security point of view. Taking the role of forerunner in this regard is difficult as the lack of exact material can create obstacles during the research but is a necessary evil which can also turn out to be rewarding.

1.2 Motivations for this research and the researcher's biases

One of the most significant motivations for this research for the researcher personally is the significant potential of discovering new ways to protect civilians and government entities from hybrid attacks by improving the detection systems. This motivation also stems from the fact that the researcher pursued a career in cyber security field in order to similarly help others. Cyber-attacks are of course one of the most significant ways of currently using hybrid methods. Hence the researcher's personal interest in especially cyber side of hybrid warfare. Hybrid attacks can be a strong tool which can be used to cause wanted impact on several countries with low risk of being caught. This can often happen without the victims even noticing the influencing attempts such as in the way of the "fake news" or other hybrid warfare methods. The researchers aim with this research is to improve the detection capabilities of hybrid warfare and increase the awareness of hybrid warfare for everyone. Through the newfound detection ways, nations can more easily protect their citizens from being influenced by hostile countries.

Another personal motivation for the researcher is the interest in hybrid warfare and the motivations behind using it. The concept of influencing silently and working in clandestine operations by exploiting multiple vulnerabilities of the target entity to accomplish leverage on the political or other interface is fascinating to the researcher. The similarity of hybrid warfare and cyber-attacks is also interesting to the researcher as cyber security is their main field of study and has largely been part of the researcher's career. The topic of detecting hybrid warfare has also relatively little research done, and it is an honor for the researcher to be in forefront of the research community.

Bias in research is defined by Pannucci and Wilkins (Pannucci & Wilkins, 2010) as "any tendency which prevents unprejudiced consideration of a question." They continue that in the context of research this means that there is an error in the process of conducting research which is realized with the researcher unknowingly or knowingly selecting one of the answers over another. It is almost impossible for qualitative research to be completely unbiased. Hence it is extremely important for the researcher to recognize and acknowledge his or her own biases and if possible, to mention them in the paper to inform the reader. The reader should take these biases into consideration when reading and interpreting the material. It is after all the readers task to understand the background of the source material. (Pannucci & Wilkins, 2010)

In this study the researcher has recognized the following biases which may or may not affect the process and result of this research. The researcher has a background in national security, has cooperated with the Finnish defense forces voluntarily through university courses and works and has also served the mandatory Finnish military conscription. The researcher is studying cybersecurity in University of Jyväskylä and is conducting this research for the university and its information sciences faculty. The researcher also works in the cybersecurity field. These attributes may have effects on the results of this research.

Of course, one of the most significant biases in this study is the of the researcher to the western countries. This has resulted in the adoption of certain pro-western countries viewpoints, and this can be seen as the study is focused on bringing down the barrier of entry especially for western countries to detect hybrid warfare. This will result in a study where countries such as China and Russia are often assumed a hostile role and the ones conducting the hybrid warfare, while the western countries are the defending ones.

The researcher has taken actions to recognize these biases and attempts to move around them as much as possible. The biases are listed here for the sake of transparency in this research.

1.3 Why was this research conducted?

Hybrid warfare is the new buzzword in the world of warfare right now. The term hybrid warfare is defined later in the thesis. Hybrid warfare is being used by state actors and smaller actors alike. It is extremely tempting for the adversaries to attempt Hybrid warfare methods, to use because of the relatively low risk of getting caught when comparing to the traditional military and other influencing methods (Bilal, 2021). For example, the Russian 2014 operation annexing of Crimea was conducted by using Hybrid methods (Bilal, 2021). This was an important piece in Hybrid warfare history because it made the term “Hybrid warfare” known for the main-stream media and a perfect example on why it is feasible for hostile actors to use these kinds of methods to influence their enemies. It becomes increasingly difficult to stop and prevent these Hybrid methods after they have been fully deployed as the operations are performed on multiple interfaces at the same time (MCDC, 2019).

For example, the annexation on Crimea is widely accepted in the west to be achieved by Russia with lowering the already low morale and trust of government of the Crimean citizens. This was achieved by combinational & simultaneous use of multiple Hybrid methods such as fake news and cyber-attacks (Bilal, 2021). With the strong base of Russian natives living in Crimea combined with the lowered trust in government institutions, the Russians deployed the now in-famous unmarked green men over the border to annex the Crimea. It is difficult for the west to apply correct level of international response against Russia as it is extremely difficult to prove without a doubt how much Russia participated in this annexation (Bilal, 2021). It is also important to understand that the Ukraine is not part of NATO nor EU which increased the difficulty of acting against Russia (Popli, 2022). This example is one of the motivations on why the detection and preventing Hybrid warfare should be preferably done before the adversaries have been able to completely deploy their hybrid methods. The detection capabilities must be improved so that the operations and influencing attempts can be stopped before they have begun (MCDC, 2019).

This research is conducted for the Jyväskylä University faculty of Information sciences and as such it needs a scientific background in cyber security. While the topic of hybrid warfare itself might seem as more of a military science related, the connections and applications to information systems and computer sciences are clear. The connection between detection of hybrid warfare and cyber security research comes from the term detection. Detecting cyber security is a richly researched part of the cyber security field and as such provides a great background for this research. The clear benefits of conducting this study for the information systems field and computer science fields are the following: Clearing multiple abstract terms which are linked to hybrid warfare and cyber security. Bringing military sciences and cyber security closer as fields and enabling increased cooperation with lowering the barrier of entry for cyber security related hybrid warfare research. Cyber information systems are critical to take into consideration in defending the critical infrastructure of a country.

Researching the detection of hybrid warfare increases the security and resilience of critical infrastructure. This creates a clear link between hybrid warfare research and cyber security where conducting this research has an immediate effect of increasing the security of critical infrastructure and therefore cyber security systems. The detection of hybrid warfare itself is also very closely related to cyber security as the actual detection is most definitely conducted on cyber security and is most likely to be AI-powered in the future. One of the objects of this study is also to provide a unique viewpoint from information systems researcher and cybersecurity specialist to the hybrid warfare research scene.

1.4 Literature review

The literature in this thesis is based heavily on military sciences and information systems & cyber security. The interdisciplinary of this thesis makes it difficult to find fitting literature which fits both the hybrid and information system research and cyber security. Hence there was extensive time spent on this part during the research and one of the reasons which makes the results of this thesis interesting for multiple parties. The literature for this thesis was chosen based on the research made at the beginning of the study. The search was made on Google & Google Scholar and various research search sites. The attempt of the search was to find works that were specifically about the detection of hybrid warfare. The exact keywords used in the search were "detection of hybrid warfare". The search turned out some extremely good results such as the Schmidts and MCDC authored papers. However, it became apparent to the researchers that the amount of literature which would be lacking in terms of the number of papers written on the topic.

The detection side of hybrid warfare has been relatively unresearched until now. The experts and western world have only now noticed that the usual ways of detecting threats and such hostile acts do not work on hybrid warfare operations as they are fought in multiple interfaces and are most often shrouded in (MCDC, 2019). The literature behind this research consists of hybrid detection related works. Hybrid warfare as itself is not indeed a new topic for research and it has been studied from multiple viewpoints and by multiple researchers. Some of these works have also noted the difficulties of detecting hybrid warfare but often that has been as a subtopic of the research. As a main research question of studies, it has remained relatively untouched until recent years.

As mentioned above, this research builds on Multinational Capability Development Campaign Countering hybrid warfare project report which is the most significant piece of research on the topic of detecting hybrid warfare. There is not a lot of previous material on detecting hybrid attacks. Other important works are J Schmidts papers along with others from Hybrid CoE of Helsinki. There are a lot of works on Hybrid warfare, which scratch the detection side of it also.

As the research was conducted for the Faculty of Information Technology in Jyväskylä University, the research must be based and relate to research on information systems and cyber security. Search for information system research papers related to detection was conducted also with the same methods as the earlier search. The problem which was observed immediately at the beginning of the search was that the number of papers written about detecting hybrid warfare and methods with information systems research as a viewpoint was zero. The goal of the search was then shifted to finding works with detection as the main topic of research. There were however papers that had cyber security as point of view but were military science literature. These papers were also used in the research.

The other significant literature for this thesis is the studies on warning intelligence. The literature on warning intelligence in the context of hybrid focuses on methods and topics which are related to warnings. These warnings can for example be created through intelligence data gathered usually by military or intelligence services. (Grabo, 2015)

The literature in this research and review was chosen based on its fitting on the research topic of detecting hybrid warfare specifically and the information systems and cyber security part of this research. The correct literature proved to be difficult to find as this topic remains relatively unresearched until last year's when the topic of detection started to come up combined with the topic hybrid warfare. Finding material on the information systems research combined with hybrid warfare proved to be impossible as there are no such works yet. The aim was then shifted to finding information systems research papers with topics related to hybrid warfare to gain general knowledge of the situation of the research on this field and cyber security papers with hybrid warfare as topic or vice versa.

The literature found during the literature review told the research multiple things about the research problem and the topic on hand. The research problem of detecting hybrid warfare proved to be as expected by the researcher an extremely difficult one. The literature review also proved the need for this thesis as the earlier works were unable to once and for all resolve the research problem. It also became apparent that there were no easy solutions for this problem as multiple high-profile researchers in the field were attempting to create solutions in, for example forms of frameworks to detect hybrid methods. One of the clearest points of connection between hybrid warfare and information systems research that rose during the review was of course cyber defense and the so-called APT actors. These papers, however, didn't prove to be enough source material on their own but will be used as a base in the coming full research.

The literature found during the literature review proved extremely useful for the researcher as the topic of this research was relatively unknown for him at the beginning of literature review. The material contained valuable information for the research in the form of different explanations for the terms.

The conclusions that can be drawn from this literature review are that this literature review helped the researcher in getting to know the terms in the topic detection of hybrid methods. The understating of the topic and the research problem in practice are of course necessary in order to conduct successful research.

1.5 Research questions and the scope of the study

The main research problem for this thesis is: The detection of hybrid warfare is continuously becoming increasingly difficult because the currently used military detection methods cannot effectively predict the operations of the enemy when it comes to hybrid warfare. These methods are not capable of following the typically continuously and covertly interchanging operations, methods and targets of hybrid warfare conducted by the enemy. The scope of this research was first restricted to focusing the study on improving the detection of hybrid warfare from cyber security research point of view. This scope was determined because of the resource and time limits of the research and to ensure that the research wouldn't expand to unnecessary lengths.

At the beginning of the research process, the research questions were set too wide and resulted in a need to revisit the questions during the study. This resulted in the following questions being formed from the research problem in order to create a more focused study that could be realistically completed with the resources that the researcher had in use.

The main question of the research is "How to improve detection of hybrid warfare, from cyber security perspective."

This is completed with two sub questions:

- Sub question 1: How to reduce the complexity of cooperating between multiple authorities and governments to enhance detection of hybrid warfare.

- Sub question 2: How to reduce the barrier of entry to start detecting hybrid warfare in countries with lesser resources.

2 RESEARCH FRAMEWORK

2.1 Research method

The qualitative case study was selected as the research method for this thesis because according to Arto Ojala (Ojala, 2016), it's a good method for gaining a deeper understanding of the object phenomenon being studied that might not be possible with a cross sectional study. In this research the case is the current situation of detecting hybrid methods in EU and other western/NATO countries and how to improve them through cyber security research.

According to Orlikowski & Baroudi (Orlikowski & Baroudi, 1990), the qualitative case study is the most used qualitative research method in information systems research. Yin describes the case study as a study that can be "exploratory, descriptive or explanatory" (Yin, 1994, s. 4). Yin's defines case study as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (Yin, 1994 s. 13).

2.2 Qualitative research

This research is of a qualitative nature. Qualitative research stands for collecting data in non-numerical form such as documents, photographs etc. (Merriam, 2002)

According to Polkinghorne (Polkinghorne, 2005) the qualitative research interview is the most used method of research in qualitative research. Writer of the popular qualitative research guide Sarah Merriam (Merriam, 2002) defines conducting qualitative research in her book "Qualitative Research: A Guide to Design and Implementation" as "understanding experiences and phenomenon. The questions which are asked in qualitative research are about understanding the behavior of people. The qualitative research aims to reach conclusions without resorting to measuring the variables of the study. The researcher's objectivity is in a significant role in qualitative research. (Merriam ,2002)

According to Myers & Avison, there are various ways to divide research methods into different groups. However, the most popular way is to divide them into quantitative and qualitative methods (Myers & Davison, 2002).

The difference in quantitative and qualitative research is that quantitative research assumes a world where objects, for example, are static or cannot change and can therefore always be measured and calculated mathematically. In reality, we exist in a world where some things are constantly changing and moving. Merriam gives an example of qualitative research in understanding and learning the interactions of a child's experiences in being placed in an orphanage. Such an event could for example be studied by following the feelings and involvement of multiple parties in this ordeal such as the child, orphanage or the social workers. The study could be conducted by following all three or single entities for different viewpoints and results. This would be impossible to measure or calculate mathematically. Hence the research community uses qualitative research methods to observe such phenomenon. (Merriam, 2002)

This research was conducted with qualitative methods because the object of study is a phenomenon. However, this study could have also been conducted with quantitative methods and with completely different questions and scopes. The scopes could have for example focused on the more technical side of detecting hybrid methods and using AI to detect anomalies. The possibilities of such a study will be discussed in the future section of this thesis.

This research is also of qualitative nature because the object of the research is to understand and improve the phenomenon of detecting hybrid warfare. As noted in the previous chapters, the qualitative research focuses on entities' experiences and comprehend the phenomenon of detecting hybrid warfare. In this research the experience is gathered from selecting a few professionals from the field of hybrid warfare. These people are experts in detecting hybrid warfare and it is this research's goal to gather material from said experts through interviews. The data is then analyzed and formed into information which can be used to create conclusions and theories. As the number of interviewees is small and the objective of the interviews is to dive deep into the experts' understanding of hybrid warfare and its detecting methods. (Merriam, 2002)

2.3 Data collection method

According to DiCiccoBloom & Crabtree, interviews are one of the most popular ways of gathering research material in qualitative research across research fields (DiCiccoBloom & Crabtree, 2006).

The choice of interview type for this research was the semi-structured and unstructured interview. In the semi-structured interview, the questions are designed beforehand, but there is room left for the interviewer to improvise by possible making furthermore detailed questions based on the interviewee's answers. DiCiccoBloom & Crabtree (DiCiccoBloom & Crabtree, 2006) note that in real life there are no completely instructed interviews, instead practically all unstructured research interviews are like guided conversations.

As Adams notes in "Conducting Semi Structured Interviews", the semi-structured interviews are superbly suited for certain situation such as asking open-ended questions and wanting to know the independent thoughts of everyone in a group or if the researchers is examining uncharted territory with unknown but potential momentous issues and your interviewers need maximum latitude to spot useful leads and pursue them. The reasons mentioned above are exactly why this type of interview was selected for this research. The data that was aimed to collect from the interviewees was mainly new ideas and research topics for the detection of hybrid warfare. This enabled the interviewer to dive deeper into the specific opinions and expertise of specific interviewees. (Adams, 2015)

The choice of the people being interviewed for this research was made based on their expertise in this field and former experience in research related to the research topic. Bloom & Crabtree note (Bloom & Crabtree, 2006) that the interviewees in qualitative research should be of similar backgrounds and should resemble each other in context of the research questions. All interviewees had background in the national security scene and most had military careers as well. The interviewees all had major experience with hybrid warfare related topics and hence contributed significantly to this thesis. Attempting to find interviewees proved to be difficult as there aren't a lot of experts on the topic of detecting hybrid warfare. As this topic is closely tied with the military, so are the interviewed. The nature of the military field is often secretive and hence finding interviewees on topics such as this can prove difficult. Especially if the questions could be interpreted as someone trying to gain knowledge about western hybrid warfare processes and systems with malicious intents. The target number of interviewed experts was set at five.

The interviewing of the experts was a significant source of material for this thesis. This was largely because even though the amount of research material and literature for hybrid warfare is significant, the amount material which is specifically about the detection of hybrid warfare is scarce. The interviews provided insight for the interviewer to the actual careers in the field of Hybrid warfare and to the research problems. The following experts were interviewed in this thesis:

- Aapo Cederberg – Cyber Watch Finland – CEO and founder
- Dr. Johann Schmid – Hybrid CoE – Director of COI S&D
- Dr. Josef Schroefl – Hybrid CoE - Deputy Director of COI S&D
- A hybrid warfare expert who chose to remain anonymous

- Dr David C. Benson – United States Air Force School of Advanced Air and Space Studies - Professor of Strategy and Security Studies

The interviews were conducted using Zoom. The preferable method in research interviews is usually to conduct the interview face to face, but because at the time of writing this thesis, the current COVID-19 pandemic situation made the Video conference interview the only feasible option. The interviews were conducted around 04.2021-04.2022. Between this time there were significant changes in the geopolitical climate of Europe which may have affected the opinions of the interviewed.

The following interview questions were formed from the research question, literature review and base material (DiCicco-Bloom & Crabtree, 2006). The goal of the interviews was to inquire with the interviewees on the topic of the thesis and to find completing material for the thesis. As mentioned in chapters above, this research has the following goals: Clear the terms of hybrid warfare and its detection, explain why the detection of hybrid warfare is so difficult, attempt to improve the current situation of detecting hybrid warfare by coming up with at least ideas and future research targets and possibilities. Lowering the barrier of entry for the detection of hybrid warfare for all western countries. With these in mind, the interview questions were formed with the intent of exploring the interviewees' expertise on detecting hybrid warfare. The questions were formed in a way that they attempt to fill the gaps in the literary background of this thesis. The interview questions were formed from these as follows:

- What does the term hybrid warfare mean to you? (To better understand the interviewed mindset)

- What kind of tasks the Hybrid CoE could improve and what new tasks do you see that Hybrid CoE could do when it comes to Detecting Hybrid warfare detection in EU. What is the shortcoming of an organization such as Hybrid CoE. What doesn't work? How would you fix these shortcomings?

- Let's say that you would be tasked with building and running an organization which would have a single task of detecting hybrid warfare through multiple interfaces (economic, military, political, etc.). What kinds of things would you take into consideration in such an event?

- What do you think are the currently largest shortcomings in the detection of hybrid warfare? How would you fix these? Where are the detection capabilities in the strongest positions?

- How would you decrease "the cost of entry" to detect hybrid warfare? Especially in the context of countries with lesser resources to spend on such matters as hybrid warfare detection. What kind of things should one think about if tasked with enabling detection of hybrid warfare for all western countries?

- Do you consider one of the interfaces used in hybrid warfare more important in the context of detection? If so, which one?

- How do you see improvements in AI creating new opportunities for detecting hybrid warfare?

- What do you think are the requirements for successfully implementing a detection system for hybrid warfare on EU level? What about on the national level?

- How would you further use civilians in the detection of hybrid warfare? How do you see the value in detection about civilian groups such as Bellingcat?

2.4 Data analysis

The hermeneutic analysis was chosen for analyzing the data collected from the interviews. Hermeneutic analysis refers to multiple methods of analyzing data which are all based on interpretation. It is often used in studies which contain information gathering by way of interview. A usual case is that the researcher is somewhat familiar with the material and attempts to focus on what the source of the information was exactly attempting to convey through their message. (Routio, 2007)

There are a couple of ways to do this such as the following according to Pentti Routio (Routio, 2007):

- Make a summary of earlier interpretations of the text, if there are any.

- Study the context from where the text originates, if it is known. This context can incorporate several distinct spheres of activity.

- Study other comparable texts, for example other works of the same author or the same group of artists.

Once the studies above have produced a number of fragmentary explanations or interpretations of the text, you have to estimate if they together give a picture complete enough. If some of the tentative interpretations seem not credible enough or insignificant, you should consider omitting them. (Routio, 2007)

The examples above, however, are focused on cases where the researcher is somewhat familiar with the material. Often the material and the context might be completely unknown to the researcher. This is the exact reason why the Hermeneutic analyzing method was developed. (Routio, 2007)

In the Hermeneutic analysis method, the researcher doesn't attempt to eliminate the person's biases and values. The research instead accepts that this kind of absolution is impossible and therefore recognizes his/her uniqueness and tries to translate the material with their own contortion. (Routio, 2007)

According to Myers and Avison (Myers & Avison, 2002, s. 11), The use of hermeneutic analysis in Information systems research attempts to understand the reasoning and thoughts of the organization or entity behind the source material. As the entity can often have a way of thinking which differs largely from researchers. The researcher must attempt to understand the complete picture and especially in the information systems context the differences and correlations between organizations and information systems. (Myers & Avison, 2002, s.11)

3 TERMINOLOGY AND RELEVANT ENTITIES BEHIND IDENTIFYING AND DETECTING HYBRID WARFARE

This chapter contains critical terms and entities which are crucial to understand to comprehend the concept of detecting hybrid warfare. It has been split into the following categories: entities, hybrid warfare terminology and lastly terminology that is related to both cyber security and hybrid warfare.

3.1 Entities

3.1.1 NATO

The North Atlantic Treaty Organization or NATO is an important entity when it comes to detecting and deterring hybrid warfare in western countries. NATO is a political and military alliance which consists of 30 countries from which 28 are in Europe. Hence the focus of NATO is largely also on European problems and hybrid warfare. (NATO, 2022)

NATO is heavily invested in cooperating with organizations and nations in the matters of detecting hybrid warfare. On their website, NATO reports that it: "NATO continuously gathers, shares and assesses information to detect and attribute any ongoing hybrid activity. The Joint Intelligence and Security Division at NATO Headquarters improves the Alliance's understanding and analysis of hybrid warfare. The hybrid analysis branch provides decision-makers with improved awareness on possible hybrid warfare." (NATO, 2022) NATO also has research agreements with the EU in the form of Hybrid CoE where the prominent research on everything about hybrid warfare in EU happens. This research also includes the detection of hybrid warfare. Even though NATO has its cooperation's with other entities when it comes to warfare, the participating countries have their own projects with other countries where they work to improve their understanding on warfare. A good example of this is the MCDC project. (Hybrid Center of Excellence)

3.1.2 European Union

The European Union or EU is a political and economic alliance which consists of 27 countries which are all located on the continent of Europe. (European commission)

The EU describes its role in responding to hybrid warfare as follows: The members of EU are mainly responsible for their own defense against hybrid warfare. The EU acts as coordinator between member countries in cases where there is a common threat against multiple member countries or where the target has value to multiple countries. An example of this could be a threat to the energy infrastructure. (European commission)

EU lists the following as main "pillars" to achieve the previously mentioned tasks: "enhancing situational awareness, boosting resilience in all critical sectors, providing for an adequate response and recovery in case of crisis and cooperation with like-minded countries and organizations, incl. the North Atlantic Treaty Organization." (European commission)

EU and its participating countries have multiple research agreements and cooperation's with other countries and entities such as NATO or United States. Some of the best examples of this are the MCDC (MCDC 2019) and the EU-HYBNET projects. Both projects have a large range of objectives when it comes to improving the capabilities and understanding of hybrid warfare in the EU. One of these objectives includes of course the detection of hybrid warfare and improving it. (EU-Hybnet)

3.1.3 Hybrid COE

The hybrid CoE is described as following organization on their page: "Hybrid CoE is an international, independent network-based organization promoting a whole-of-government and whole-of-society approach to countering hybrid warfare." What is Hybrid CoE - Hybrid CoE - The European Centre of Excellence for Countering Hybrid warfare

The Hybrid COE is one of the most critical players in the EU regarding Hybrid warfare. It was founded in 2017 and its headquarters are in Helsinki. The Hybrid CoE has a critical role in leading the research on Hybrid warfare related topics. The key task of Hybrid CoE is "to build participating states' capabilities to prevent and counter hybrid warfare". (Hybrid CoE)

3.1.4 Bellingcat/civilian groups

Bellingcat is an investigative journalism website that is known for its open-source intelligence and fact-checking work. The group came to the knowledge of larger public with the shooting of MH17 Malaysian airlines in the Ukraine by Russian backed separatists. The group helped to identify the key suspect in the incident through open-source intelligence and collaborative work. They are also known for the identification of suspects in the poisoning of Sergei and Yulia Shripal's in Salisbury. (Bellingcat)

The Bellingcat relates to hybrid warfare as its investigative work often relates to events which are heavily related to hybrid operations such as the MH17 Malaysian shooting. Another part of Bellingcat relation to hybrid warfare is its fact checking operations. Bellingcat is renowned for its ability to fact check information from mainly open source gathered intelligence. The group has. Information warfare is one important part of hybrid warfare which is often used in modern day hybrid war even without other means of affecting the victim state. This makes groups such as Bellingcat extremely valuable to entities trying to identify hybrid warfare. (Bellingcat)

The Bellingcat has caved way for other volunteering civilian groups that could one day help to recognize possible usage of hybrid methods that could otherwise be left undetected by the authorities. During the research interviews it became clear that all interviewed thought enabling the operation of these groups could very well enhance the identification and detection of hybrid warfare. Researcher's opinion is that the enabling of similar groups such as Bellingcat is a way for countries with lesser resources to spend on hybrid method detection to enhance their detection capabilities. These groups could help increase the general public awareness surrounding hybrid warfare and help gather open-source intelligence and analyze it through collaborative community work. This would in turn benefit authorities by providing them with additional analyzed intelligence at low cost. (Bellingcat)

3.2 Hybrid warfare terminology

3.2.1 Hybrid threats

Hybrid warfare is defined by Hybrid CoE as "an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level." (Hybrid CoE)

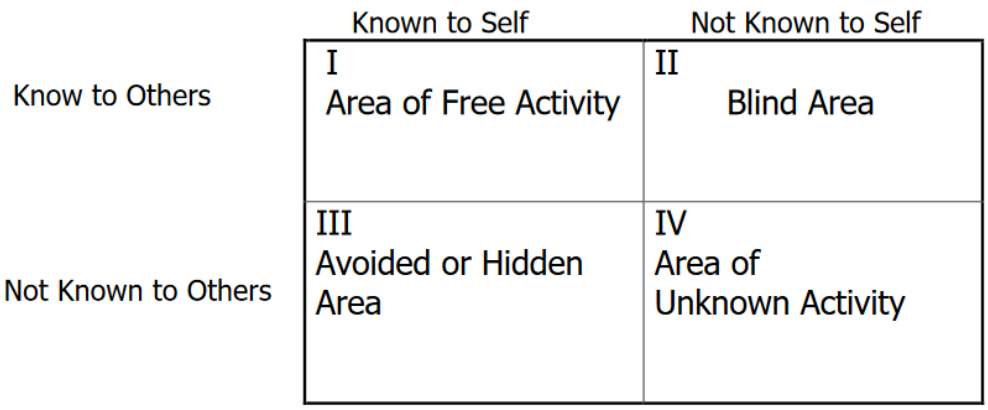
The term hybrid warfare is also commonly used in conjunction with the word hybrid warfare which can generally refer to multiple methods being used at once. In the context of hybrid warfare, it is often used to describe the methods used by adversaries in order to gain leverage on the target. In this thesis the focus is on hybrid warfare as they can be used better to describe detection of hybrid activities. (Hybrid CoE)

3.2.2 Unknown unknowns and Known unknowns

The terms unknown unknown and known unknown are often brought up in research papers of detecting hybrid warfare and detecting things in general.

They are necessary for a person to understand and to be able to comprehend the complexity of identifying and detecting hybrid warfare.

The terms Known unknown & unknown unknown were made familiar to the general public by United States Bush administration secretary of defense Donald Rumsfeld in 2002. (United States Department of defense, 2002) These terms first appeared in the Johari Window tool created by Luft & Inhgham in 1955(Luft, 1955). The Johari Window is used to provide enhancement and understanding of problems in group work (See Figure 1). It provides a possibility to self-reflect and enhances the understanding of areas that are known to you and not known to you and areas that others know or might not know for you to be able to focus on where it matters. (Luft, 1955)



	Known to Self	Not Known to Self
Know to Others	I Area of Free Activity	II Blind Area
Not Known to Others	III Avoided or Hidden Area	IV Area of Unknown Activity

FIGURE 1 The Johari Window (Luft, 1955)

In the context of detecting hybrid warfare, the MCDC describes the unknown unknowns and known unknowns as follows:

> *"One way to consider warning intelligence for hybrid warfare is to differentiate potential future hybrid attacks into two separate categories of 'known unknowns' and 'unknown unknowns'. Known unknowns refer to modes of hybrid attack that we know we may be unaware of. However, risk related to hybrid attacks may also exist where we are not even aware of its nature, our vulnerability to it, or even of our own ignorance to the threat. This is the field of unknown unknowns."* (MCDC, 2019)

The next Figure 2 is from the MCDC report 2019 and highlights the difference between monitoring known unknowns and discovering unknown unknowns.

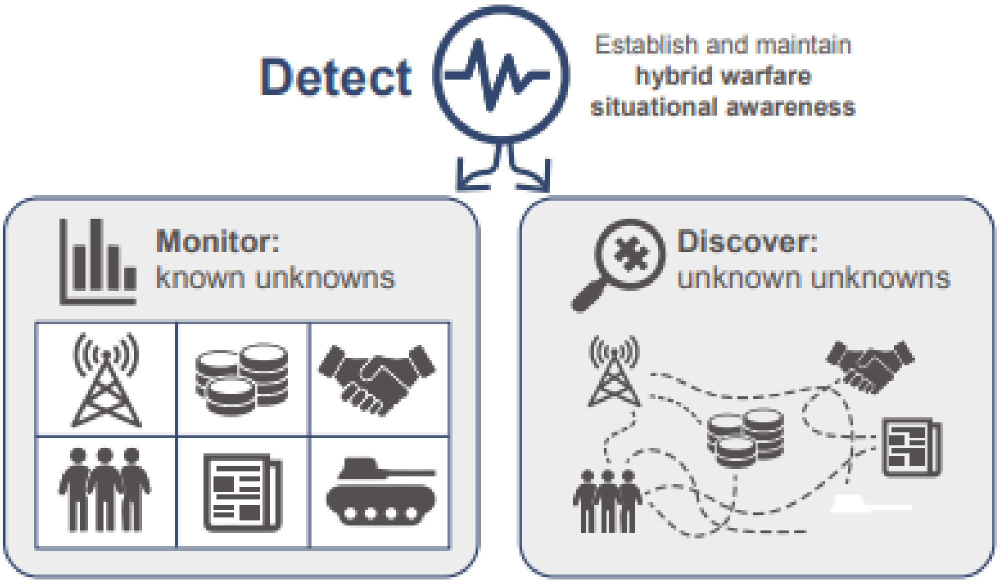

Detect
Establish and maintain hybrid warfare situational awareness
Monitor: known unknowns
Discover: unknown unknowns

FIGURE 2 Distinguishing between 'monitoring' and 'discovery' in warning intelligence for hybrid warfare (MCDC, 2019)

Other terms that are strongly linked to this topic are monitoring and discovery. Monitoring means the traditional way of attempting to detect known unknowns often by using indicators of known threats. The discovery, however, means attempting to identify previously unknown threats that have no indicators before the identification. These threats fall under the category of unknown unknowns that are extremely difficult to identify. These threats are not possible to be detected by traditional indicator-based means as no such indicators exist for the threat yet. (MCDC, 2019)

3.2.3 Warning intelligence

The term Warning intelligence is defined by C, Grabo as intelligence, which gives a warning signal or detects an upcoming hostile event such as traditional military attack. The warning intelligence is often more indicator based and uses the established baseline or" normal" of enemy movements in attempt to distinguish hostile activity (Grabo, 2015). The attack of Japanese forces in the United States pacific naval base Pearl harbor in 1941 in second world war is often mentioned in intelligence literature as an example on why warning intelligence is important part of national security. Predecessor to NSA (United States National Security Agency) the United States signal Intelligence Service (SIS) was able to decrypt the Japanese diplomatic communication systems cryptography named PURPLE. The SIS intercepted a large quantity of messages between Tokyo and Japan's diplomats in USA before the attack on Pearl Harbor. These messages contained information and signals that in hindsight highlighted and could have been used to prevent the attack. However, these signals were completely ignored by the United States and with the combination of misreading the Japanese intentions this resulted in the military disaster that the attack on Pearl harbor was for the United States. The incident also was one major driving factor for the forming of the CIA. The takeaway in context of Hybrid warfare and warning intelligence, is that even though the United States had the necessary warning intelligence to foresee the attack, they choose not to act as the intelligence couldn't provide a complete picture of the situation. This highlights the importance of a skilled analyst when it comes to warning intelligence and intelligence, which also applies it to detecting modern Hybrid warfare. (Vogel, 2012)

The warning intelligence is an important part of identifying Hybrid warfare and usage of Hybrid methods. In the context of Hybrid warfare, the warning intelligence could be for example a military intelligence report with information about a possible annexation or attack plan of an area by a hostile country or perhaps an intelligence report on economy which indicates many possibly strategic purchases of corporations with the intent of gaining leverage in that target country. However, according to MCDC in their report Countering Hybrid warfare, the traditional indicator-based activity is not as effective and usable in detecting Hybrid warfare as it has been against conventional military tactics. The detection of Hybrid warfare requires an entirely new approach that evolves beyond the traditional indicator-based warning intelligence. (MCDC, 2019, s.26)

3.3 Hybrid warfare/detection and information systems research related terminology

3.3.1 Cyber threats as a part of hybrid warfare

Cyber threats are an important part of the adversary's toolkit in hybrid warfare. Cyber threats can also be similarly difficult term to define as hybrid warfare as it is used differently by different organizations. United States National Institute of Standards and technology NIST defines cyber threats as follows: "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service." (NIST)

Cyber threats can be conducted by nation states, cybercriminals, hacktivists & terrorists. There are multiple means and ways of conducting cyber threats and various reasons ranging from monetary gains to attempting to influence target nations. The usage of cyber threats can be stealthy and efficient way to influence the target in various ways. One more recent example of cyber threats being conducted alongside other hybrid warfare was the Russian Cyber campaign launched on Ukraine critical infrastructure before beginning the invasion and war on Ukraine. (Kurmanau & Bajak, 2022)

According to Gunneriusson & Ottis (Gunneriusson & Ottis, 2013) cyber threats as part of hybrid warfare can be viewed in three different ways. First as a support force to traditional military such as Army or air force. Gunneriusson & Ottis (Gunneriusson & Ottis, 2013) provide one example of this as Iran was able to hijack a United States drone and control it to land on their soil.

Secondly it can be an instrument of hybrid warfare on its own as for example in the Stuxnet-worm was used to tamper and destroy the Iranian nuclear research facilities. (Malwarebytes).

Lastly it can be used in conjunction with other hybrid warfare to achieve wanted influence on target as seen in the previously mentioned Russia cyber campaign (Gunneriusson & Ottis, 2013).

3.3.2 Advanced persistent threat

Birth of the term "Advanced Persistent Threat" (APT) has been credited in the cybersecurity field to United States Air Force in 2006 (Nachaat & Belaton, 2021). There is a clear relation between APT groups and hybrid warfare is as the APT actors are often one of the possible entities being used by adversaries to conduct cyber operations, often as a part of a larger hybrid operations but also sometimes on their own.

The APT groups can be either related to national organizations such as intelligence services with national interests or criminal organizations with interests on usually money or hacktivism or terrorism. The line between these two groups of actors is blurring as multiple nations are backing these criminal organizations to create havoc and chaos in their countries of interest. The national APT groups often work for prolonged times in the same target with the single goal of gaining access to the target organization by any means necessary. (Nachaat & Belaton, 2021) The detection of APT groups is therefore also part of detecting hybrid warfare which makes it an important part of this research as it ties together the information system research and hybrid warfare. An active ongoing attack from certain nation state backed groups could also indicate that there could be other hybrid activities targeting the same organization or country.

The naming conventions of the APT-groups vary by the organization and for the sake of clarity in this research we use the Cyber security company Mandiant's naming convention which lists APT-groups with a simple "APT" and a number assigned for that group. It is one of the most known and used methods to name ATPs because of its simplicity. (Mandiant)

As a case example of an APT-groups as part of hybrid warfare, in the 2016 presidential elections of United States of America, the Russian based APT-groups took part in the attempted interference and affecting of the elections. The APT groups in question have been identified as APT28 & APT29. In the 2016 election hack both actors were identified and participants from both actors charged with conspiracy to hack into various computers held by the Hillary Clinton's election campaign. The participants have been identified by United States as employees of the Russian intelligence services SVR & GRU. (Symantec Security Response Team, 2018)

The group also attempted to infiltrate the election systems of USA likely to affect the result of the elections (United States Department of Homeland Security, 2016).

3.3.3 Security operations center

One major organizational entity related to detections in cyber security are the Security operation centers or SOC: s inside organizations. The cyber security company Checkpoint defines Security operations center or SOC as follows: "A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents." (Checkpoint)

Security operation centers often operate in tiers, and the specific contents of the tier vary on organization. Crowdstrike, one of the largest cybersecurity companies in the world defines the tiers as follows: where the first tier does the triage work which does the initial analysis for alerts and then does the possible prioritizing or escalation to next tier. The second tier is the incident responders who can conduct investigations on alerts and if needed do the necessary remediations. The last tier is the threat hunter, which works proactively to find threats that have slipped past the detections. There are also other relevant roles in SOC such as security engineer which works to integrate and develop the systems used by SOC analysts. (Crowdstrike, 2022)

3.3.4 Threat simulation

In cyber security context, organizations can conduct or purchase as a service a threat simulation in, for example a form of red team exercise in their environment in order to simulate the actions that a real attacker could possibly take in a real scenario. The information generated from the red team exercise is then in best case scenario used by the organizations cyber security team to enhance their security and to fill the gaps in detection and defenses that were noticed by a red team. There are also tools that provide similar functionalities to an actual red team, but the value of having real humans that have good offensive skills attempting to think like an attacker provides a good value to the organization. The red team exercises are often technically oriented, whereas the tabletop exercise is focused on improving the processes and policies of said organizations. (Harrington, 2022)

Another possibility for simulating threats in your operating environment is organizing or participating in a tabletop exercise. NIST defines a tabletop exercise as follows: "A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario." (NIST).

A tabletop exercise can provide information about the current situation processes and response capabilities of the target organization which can then be improved and possibly later tested again with a similar exercise. A tabletop exercise can also include red team operation as part of it or other sections which test and audit the technical capability of the target organization.

The United States Cybersecurity & infrastructure agency CISA lists possible scenarios that cover different areas of security that you could test. For example, there is a separate exercise for Industrial control systems and election system related cyber threats for United States organizations to run. (CISA)

3.3.5 Cyber threat modeling

The national Cyber Security Agency of Singapore defines Cyber threat modelling as an act that allows the owners to identify and map their systems throughout to ensure that they understand cyber threats they could potentially be facing. It increases the difficulty for an attacker to successfully complete as an attack can be stopped in different stages of it with a good usage of a threat model and understanding and hardening your own systems. By using a threat model, the owners can also see the blind spots of the system that could otherwise be forgotten. (CSA Singapore, 2021)

There are multiple different threat models that can be used. These models often take different points of view to look at the target and to identify its threats. For example, one of the most well-known cyber threat frameworks, the OWASP top 10 threat framework focuses on the specific web application threats that are commonly seen in web applications. By using this framework, the owner can map their web application and see if any of the most common threats are possible for attackers to exploit in case of an attack. If a threat is found the owner can then proceed to apply a remediation or fix to stop the threat from being exploited. (Sentonas, 2022)

Another well-known threat modelling framework is the MITRE ATT&CK Framework that is used to map possible the level of visibility the owner has to the vulnerabilities and threats in target system and to provide an easy way to understand the current defensive capabilities. It can also be used for example to map the capabilities of EDR tools and level of detection in SOC. It is often used as a sales point by vendors providing tools for detecting cyber threats (Sentonas, 2022). By using the MITRE, a SOC can start filling the gaps in detections to ensure a throughout detection capability. The ATT&CK framework is designed for multiple operating systems and dives deep into specific techniques to teach the system owners what an attacker could potentially exploit in their system. (Poston, 2021)

3.3.6 Detections in cyber security

The act of detecting in cyber security refers to identifying or discovering a possible threat or an indicator of an attacker. To be able to detect an attacker, the defender must have visibility to their environment which in the cyber environment comes through tools and logging. Through these the defenders can look for anomalies and attempt to identify the attacker and malicious activity from the regular activities. Typically, the attacker deploys malicious software of some type onto the victim systems which the defender then attempts to detect. (Rapid7)

There are different types of detection that are used to detect malicious actions on systems. Previously malicious actions were detected by indicators and signatures such as known malicious filenames or hashes. This method worked for a while, but the attackers were able to conjure malware that changes its indicators constantly to avoid detection. To counter this, the push has been for detection tools to be able to use heuristic detections to detect malicious activity based on actions and routines that are known to be associated with malicious behavior. (F-secure)

4 HYBRID WARFARE AND IT'S DETECTION

4.1 What is hybrid warfare

For us to truly understand the term Hybrid Warfare and modern warfare and how it has evolved to this point we must go back to its origins and how it has evolved. Warfare that could be considered hybrid has been conducted throughout history. However, the term hybrid warfare as a somewhat loose is relatively new and has only been used in scientific and military literature from 2007 onwards.

It was first used by Frank Hoffman in his work Conflict in the 21st Century: The Rise of Hybrid Wars. Hoffman defined Hybrid warfare as follows: "Hybrid Wars incorporate a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder." (Hoffman, 2007).

It also has various other definitions which vary significantly by the source but in my opinion the most accurate description was made in the "Understanding Hybrid Warfare" article, the "Hybrid Warfare" is explained as a something of an unclear concept but still something western countries recognize as significant problem. The baseline assessment of MCDC countering hybrid warfare describes the Hybrid warfare as the following: "The synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects" (MCDC, 2017).

One of the implied reasons for the article and framework is indeed to clear up some of the confusions behind the use of the term hybrid warfare. The "distinct attribute" of Hybrid Warfare is in the attackers focus on multiple methods of power in order to maximize the effect on the target. The attacker attempts to identify and exploit specific vulnerabilities such as internally divided countries to reach a desired goal. The term hybrid warfare is also a bit problematic as it contains the word "war" it tends to indicate that there is a physical military altercation connected to it. However, that isn't always the case. (MCDC, 2017)

According to Schmid, J from Hybrid CoE (Schmid, 2019) "All war is hybrid, but there is also a specific hybrid way of conducting war." Schmid says that the most significant difference between hybrid way of conducting war is the center of the gravity, which is not located in the military domain.

Schmid (2019) defines Hybrid Warfare to the following three key characteristics and their hybrid orchestration can be used to identify The Hybrid warfare:

1. Focusing the decision of war/conflict as such primarily on a broad spectrum of non-military centers of gravity. These can include political will, the economy, culture, psychology, legitimacy, or morale, for example. Hence, success in hybrid warfare does not necessarily require a military victory.

2. Operating in the shadows of various interfaces such as between war and peace friend and foe, internal and external security, civil and military domains, state, and non-state actors. This blur traditional lines of order and responsibilities, hereby creating ambiguity and avoiding attribution in order to paralyze the opponent's decision-making processes. this, in turn, limits the adversary's options to respond and attacks his most critical vulnerabilities at such interfaces in a non-linear way, while avoiding being confronted by his strengths.

3. Utilizing a creative combination, hybrid orchestration and the parallel use of different civil and military, regular and irregular, open as well as covert means, methods, tactics, strategies, and concepts of warfare, thereby creating 'ever-new' mixed hybrid forms. In short: combining the tailored use of hard power with a broad spectrum of soft power elements by the creative use of smart power.

The Figure 3 below visualizes the characteristics of Hybrid Warfare described by Schmid.

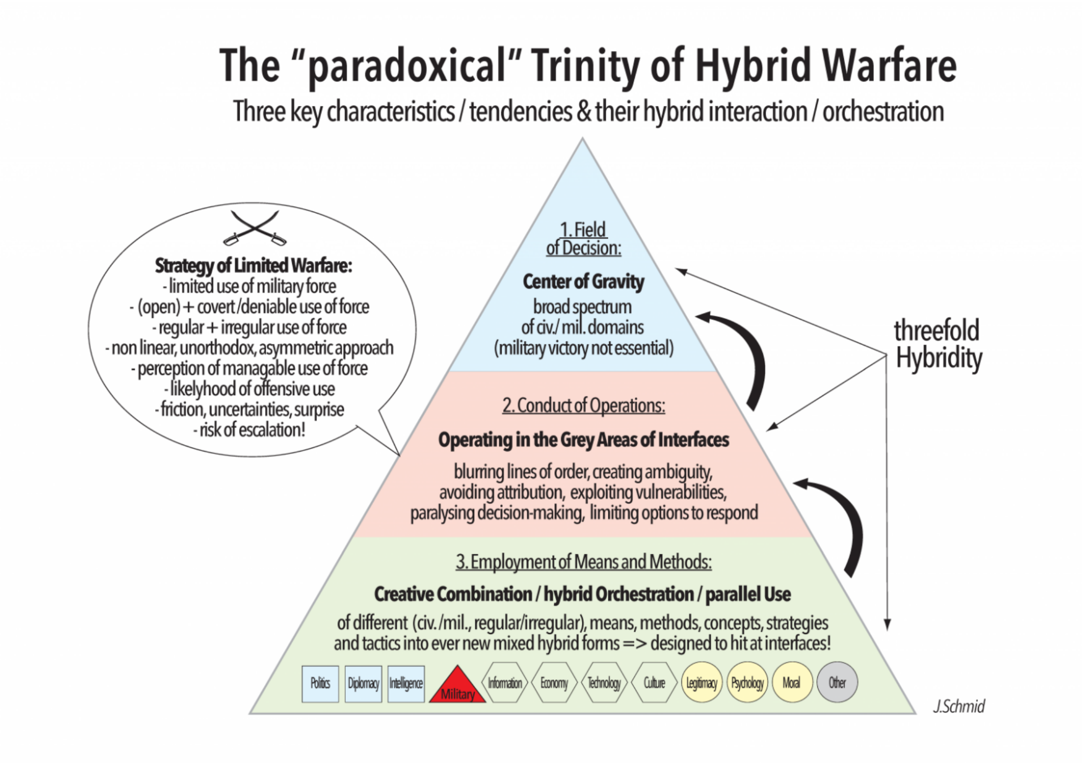

The "paradoxical" Trinity of Hybrid Warfare
Three key characteristics / tendencies & their hybrid interaction / orchestration
Strategy of Limited Warfare:
- limited use of military force
- (open) + covert/deniable use of force
- regular + irregular use of force
- non linear, unorthodox, asymmetric approach
- perception of managable use of force
- likelyhood of offensive use
- friction, uncertainties, surprise
- risk of escalation!
1. Field of Decision:
Center of Gravity
broad spectrum of civ./ mil. domains
(military victory not essential)
2. Conduct of Operations:
Operating in the Grey Areas of Interfaces
blurring lines of order, creating ambiguity, avoiding attribution, exploiting vulnerabilities, paralysing decision-making, limiting options to respond
3. Employment of Means and Methods:
Creative Combination / hybrid Orchestration / parallel Use
of different (civ./mil., regular/irregular), means, methods, concepts, strategies and tactics into ever new mixed hybrid forms => designed to hit at interfaces!
Politics
Diplomacy
Intelligence
Military
Information
Economy
Technology
Culture
Legitimacy
Psychology
Moral
Other
threefold Hybridity
J.Schmid

FIGURE 3 The paradoxical trinity of hybrid warfare (Schmid, 2019)

The reasons mentioned above also highlight the extremely complicated and difficult situation of accurately detecting and predicting the usage of hybrid warfare methods.

The researcher's opinion on the term Hybrid warfare is that the Hybrid warfare is very closely related to cybercrime/war as in both are the modern evolutions of old methods that use modern covert, clandestine and stealthy tactics to achieve an objective, which could for example be political leverage or obtain materials. The same objectives used to be achieved through warfare or by robberies, which both were high risk and high reward activities. These days you can launch a hybrid campaign on a target, and it might take years to even detect that such activity was going on. Therefore, the detection of hybrid warfare is such an important topic to research right now.

The specific methods for hybrid warfare identification and detection are classified and vary on a national basis with different levels of resources and capabilities to use to conduct the identification and detection of hybrid warfare. The following chapters attempt to describe the current situation of detecting hybrid warfare as it is discussed in the academic literature and important western publications such as NATO research papers and contain tools & models & terminology and how they relate to current situation of detecting hybrid warfare.

Even if specifics of each nation detecting & identifying hybrid warfare are classified, it is revealed in and often discussed in academic military papers etc. That the currently and in recent history actions which could be considered war have been detected using certain known indicators which the defenders know as a mark that a war has started etc. These indicators could for example be something such as the enemy combatants passing your border to enter your country without permission. However, the problem with these traditional indicators is that as Frank Hoffman noted in his work (Hoffman, 2016) it is difficult to define what war is as adversaries often operate on the so-called gray zone in order to avoid confrontation and detection. Hoffman lists as an example the actions of China on the South China Sea where they seem to be attempting to change the existing borders by using maritime security forces and fishing boats. These acts are easily deniable by China and hence allow them to continue operate without the fear of triggering armed response as they would have in total war. The significant problem according to Hoffman here is, that there haven't traditionally been any other distinctions than war and peace. Hence when the adversaries operate on the gray zone the western countries have been unable to generate answers and have been paralyzed in their tracks. (Hoffman, 2016)

As Hoffmans example shows, the traditional and currently used hybrid warfare do not function on necessary levels to identify and detect hybrid warfare as the threats themselves haven't been identified yet and are hence called unknown unknowns. Hence the need for new approaches for the western countries to be able to detect adversaries. The current approaches to this will also be covered in later chapters.

4.2 CHW1-model

The CHW1-model is a significant scientific framework product in the field of hybrid warfare. The name CHW comes from Countering Hybrid warfare (See Figure 4). It was created by the Multinational Capability Development Campaign (MCDC). Established in 2013, The Multinational Capability Development Campaign series is a multinational force development initiative designed to develop and assess non-material (non-weaponry) force development solutions, through collaborative multinational efforts, to meet present and future operational needs associated with conducting joint multinational and coalition operations. It contributes to multinational capability development by identifying and evaluating potential solutions to coalition and multinational capability gaps (MCDC, 2013).

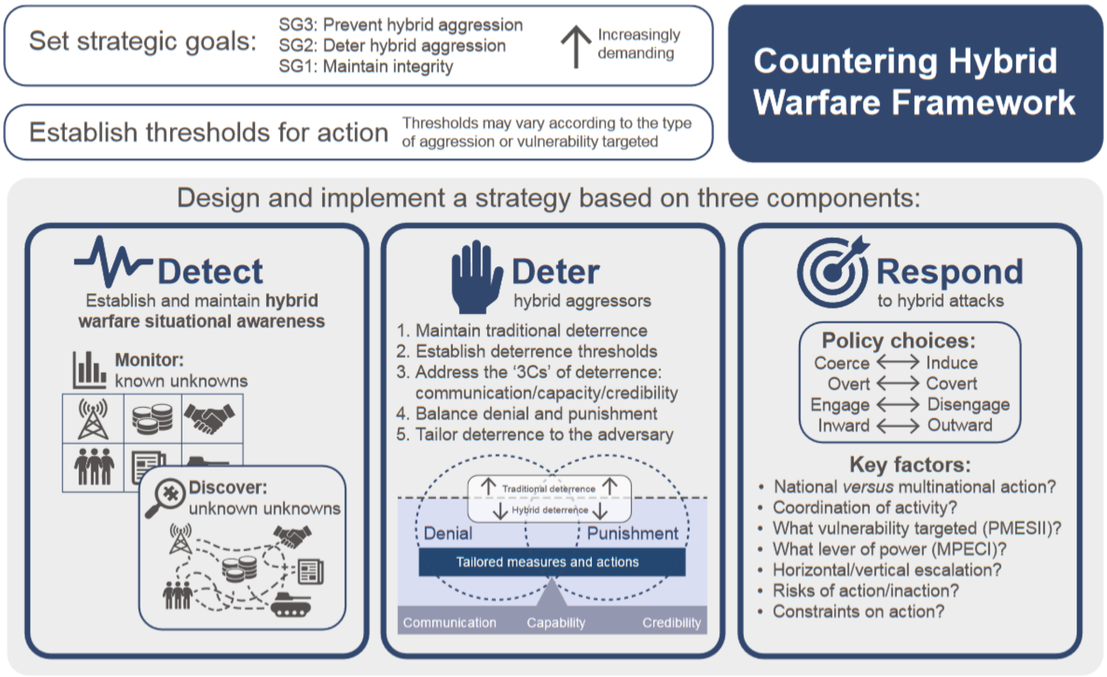

Set strategic goals:
SG3: Prevent hybrid aggression
SG2: Deter hybrid aggression
SG1: Maintain integrity
Increasingly demanding
Establish thresholds for action
Thresholds may vary according to the type of aggression or vulnerability targeted
Countering Hybrid Warfare Framework
Design and implement a strategy based on three components:
Detect
Establish and maintain hybrid warfare situational awareness
Monitor: known unknowns
Discover: unknown unknowns
Deter
hybrid aggressors
1. Maintain traditional deterrence
2. Establish deterrence thresholds
3. Address the '3Cs' of deterrence: communication/capacity/credibility
4. Balance denial and punishment
5. Tailor deterrence to the adversary
Traditional deterrence
Hybrid deterrence
Denial
Punishment
Tailored measures and actions
Communication
Capability
Credibility
Respond
to hybrid attacks
Policy choices:
Coerce ⟷ Induce
Overt ⟷ Covert
Engage ⟷ Disengage
Inward ⟷ Outward
Key factors:
• National versus multinational action?
• Coordination of activity?
• What vulnerability targeted (PMESII)?
• What lever of power (MPECI)?
• Horizontal/vertical escalation?
• Risks of action/inaction?
• Constraints on action?

FIGURE 4 MCDC Countering Hybrid Warfare Framework (MCDC, 2019)

The CHW1 is a concept model which can be used to visualize the hybrid warfare and its complexity in an easily understandable way through the usage of instruments of power and vulnerabilities and synchronized combination of these to achieve the target objectives. According to the MCDC (2019), the model is focused on state-actors but is agnostic to the type of aggressor. The model was made based on the following characteristics. (MCDC, 2019):

- The combined use of multiple instruments of power to achieve asymmetry through targeting an expanded range of vulnerabilities.

- A synchronized attack package that exploits both horizontal and vertical axes of escalation.

- An emphasis on creativity and ambiguity to achieve synergistic effects (including in the cognitive domain).

The CHW1-model describes how it is possible for the adversary of Hybrid Warfare to use a wide scale of instruments to achieve the desired effect. These instruments are then targeted towards specific vulnerabilities in the targeted system. The figures below are also from the CHW1-model and showcase the instruments and the vulnerabilities they are being targeted to. (MCDC, 2019)

The instruments of power in the CHW1-model are described as Military, Political, Economic, Civil and Information. Shortened as MPECI.

The target vulnerabilities can be categorized in the CHW1-model as Political, Military, Economic, Social, Infrastructure and Information. Shortened as PMESII. (MCDC, 2019)

These categories are further explained in the Figure 5 below.

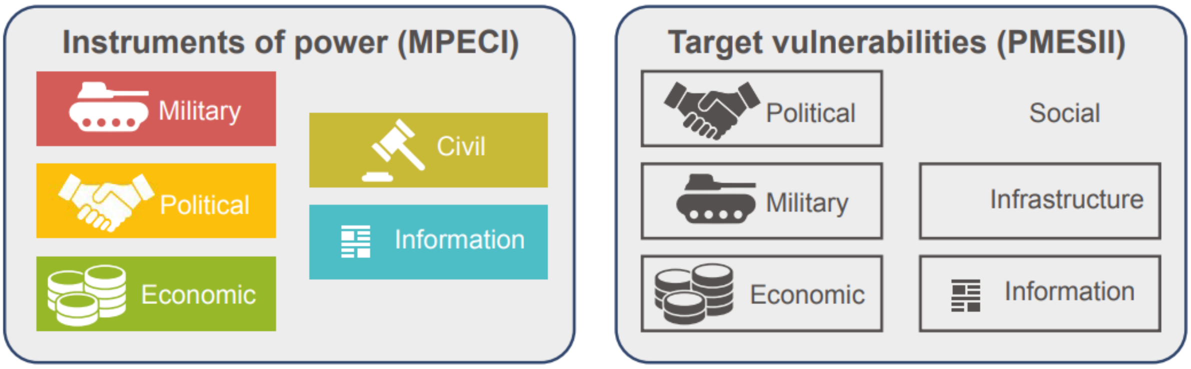


FIGURE 5 MPECI instruments of power and PMESII target vulnerabilities (MCDC, 2019)

The synchronized vertical and horizontal escalation characteristic to hybrid warfare is illustrated in the Figure 6 (MCDC, 2019).

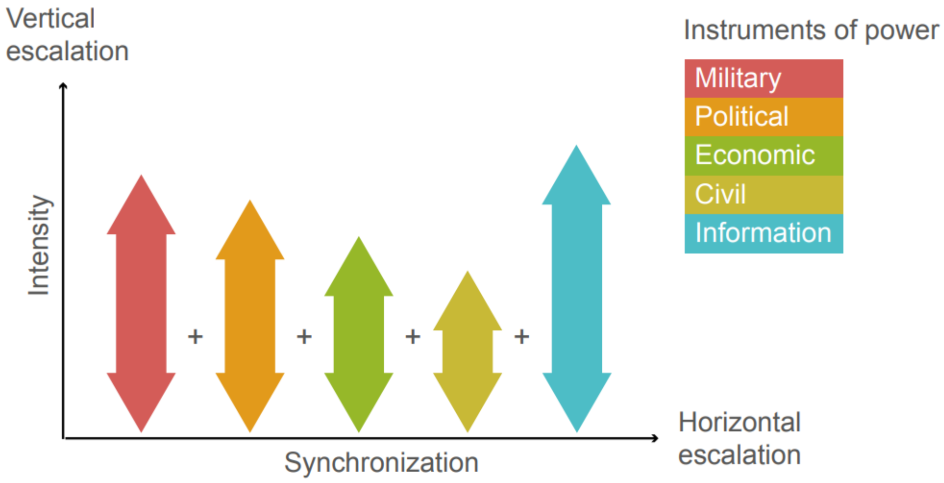


FIGURE 6 The synchronized vertical and horizontal escalation characteristic to hybrid warfare (MCDC, 2019)

The following Figure 7 is the last one from the framework, and it is used to visualize a hybrid attack and to showcase the combination of different instruments of power to gain horizontal escalation. According to MCDC (2019), “the figure is based on the following elements”:

- Critical functions and vulnerabilities,
- Synchronization of means (horizontal escalation),
- Effects and non-linearity.

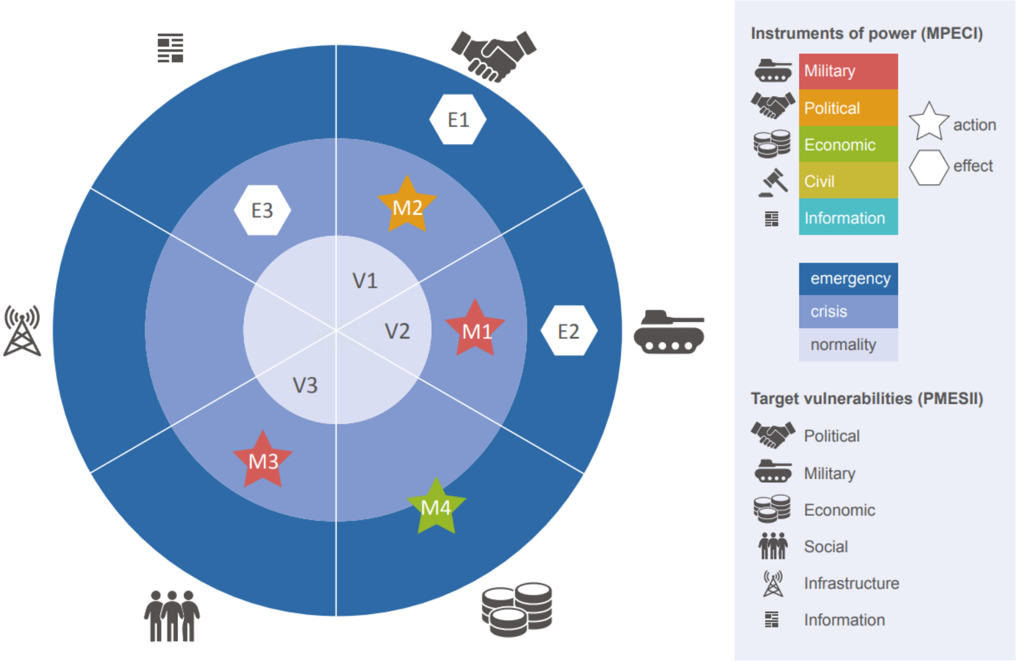


FIGURE 7 Visualizing hybrid warfare (MCDC, 2019)

The CHW1-Framework describes accurately the difficulties of detecting Hybrid warfare because of its seemingly irregular and complex combination of methods. The combination allows clandestine and covert operations to be used to hide the origin of the attacker. This causes the problems in detecting hybrid warfare and is also the most significant motivation of this thesis. (MCDC, 2019)

As mentioned above the authors incorporate the three elements showed above to describe hybrid warfare as: “The synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects.” (MCDC, 2019)

4.3 Current attempts to solve problems in detecting & identifying hybrid warfare

The following case studies are from the MCDC 2019 report which aims to prove the possibilities of detecting hybrid warfare in practice in current day environment. Another part is the previously mentioned problems and fixes to them. The following Figure 8 shows what kind of approach the studies have taken to find a solution and where the approach falls in the monitoring known unknowns and discovering unknown unknowns' matrix. (MCDC, 2019)

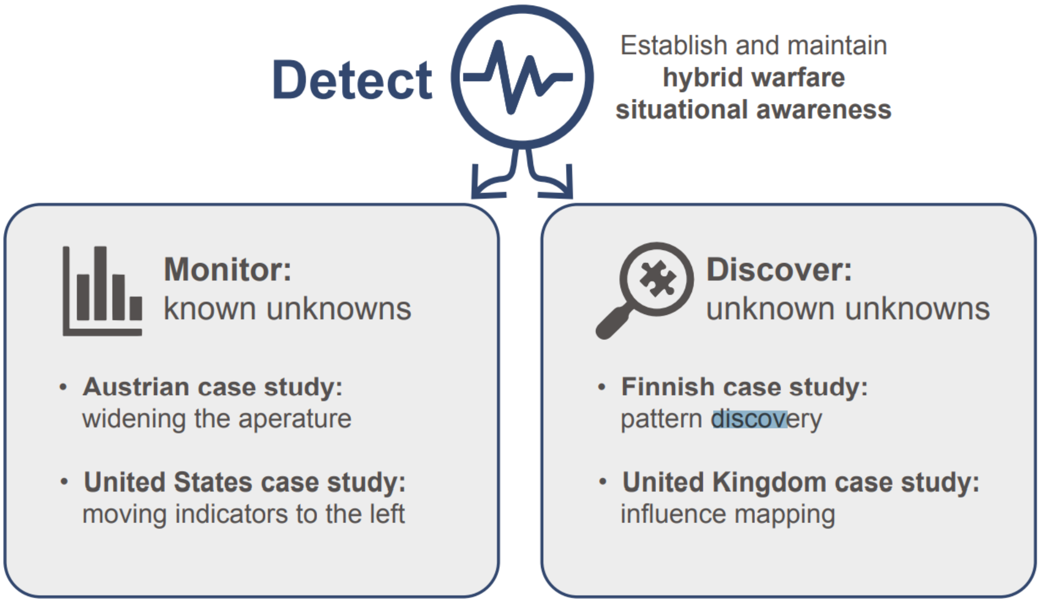

Detect
Establish and maintain hybrid warfare situational awareness
Monitor: known unknowns
• Austrian case study: widening the aperature
• United States case study: moving indicators to the left
Discover: unknown unknowns
• Finnish case study: pattern discovery
• United Kingdom case study: influence mapping

FIGURE 8 Distinguishing between 'monitoring' and 'discovery' in warning intelligence for hybrid warfare (MCDC, 2019)

4.3.1 Austrian solution to detecting hybrid warfare.

Austrian military has attempted to increase the scope of their hybrid warfare detection methods to better match the complexity of modern hybrid warfare when compared to traditional indicator-based detection methods. One of the ways this was done was that the Austrian military used Clausewitz "center of gravity"-theory. In practice this means, that the Austrian army can anticipate potential hybrid warfare better with the usage of COG analysis when considering the possible targets of hybrid warfare. The MCDC (MCDC, 2019) lists the detection process in the following four parts:

- Identifying national critical vulnerabilities,
- Linking them to assumptions or hypotheses of adversary objectives and capabilities,
- Developing new warning indicators linking the two,
- Deriving actions, effects and conditions required to counter these threats (in a whole nation approach).

According to the MCDC (2019) study the civilians are also in crucial role in detecting hybrid warfare as they provide the much-needed expertise from different fields and practical skills which can then be applied to create indicators to identify and detect hybrid warfare.

4.3.2 United States solution to detecting hybrid warfare

The United States military has another approach to detecting hybrid warfare where the focus is on hybrid warfare being the known unknown and trying to develop indicator-based warning systems. (MCDC, 2019)

In this approach the United States decided to focus more on the gray zone/non-military hybrid methods performed by adversaries. The spectrum used by the United States to determine the phases of conflict in hybrid warfare is the "Spectrum of Conflict in Unconventional Warfare", which was created by Hoffman in 2016 to represent the difficulty of determining hybrid warfare (See Figure 9) (Hoffman, 2016).

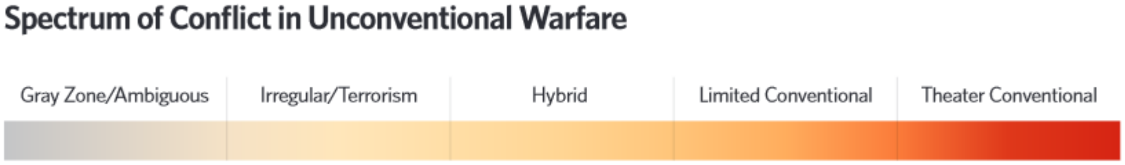


FIGURE 9 Spectrum of Conflict in Unconventional Warfare (Hoffman, 2016)

There are similarities to the Austrian military's approach, but instead of finding additional vulnerabilities and places to monitor hybrid methods, the United States decided to focus on attempting to enhance their warning intelligence to detect threats and methods happening under certain level of Hoffmans spectrum which stay in the gray area etc. The United States Army Special Operations Command or short USASOC has identified a significant need to enhance the capability of them being able to identify threats especially on the left side of Hoffmans spectrum. (MCDC, 2019)

USASOC has identified the hybrid warfare to be a significant problem for their warning intelligence especially in the gray area of conflict as they haven't historically been relevant for the military and are hence not understood and developed well enough in the military for them to efficiently identify and detect. The US military community has noted that there is a need for a whole new type of intelligence collection to be able to fulfill the needs to create warning intelligence to detect these threats. (MCDC, 2019)

4.3.3 Finnish solution to detecting hybrid warfare

Finland has taken a totally different approach to detecting hybrid warfare from traditional ones used by United States & Austrian militaries. In this approach Finland is focusing on the unknown unknowns which, as mentioned previously are known to be difficult to detect with traditional indicators. For that reason, Finland aims to shift from reliance on traditional indicators to detecting anomalies in data. (MCDC, 2019)

Quick action and response unit has been set straight under the Prime minister office in Finland to allow possibility to respond immediately to new potential threats. The team consists of specialists from different fields such as economics to be able to identify threats on all of them. (MCDC, 2019)

Traditionally these kinds of threats wouldn't be possible to detect with only specialists from national security related agencies. This approach needs a deeper understanding of additional specialists from different fields such as politics and economics in order to be able to detect and identify anomalies. Another main point of this method is to enhance the communication government branches and agencies and private sector to come as one nation to detect threats against Finland and its allies. (MCDC, 2019)

4.3.4 United Kingdom solution to detecting hybrid warfare

UK has also taken the similar approach to detecting hybrid warfare as Finland. UK MOD has developed a tool called "hybrid activity monitoring tool" to detect and identify hybrid warfare. It functions by grinding through open-source data to generate leads of potential hybrid warfare. The aim of the tool is to enhance the level of understanding of hybrid warfare for decision makers by attempting to clarify to them what kind of hybrid activity is happening currently and on which vulnerability they are being targeted at. The possible vulnerabilities in the tool are categorized as in the CHW1-framework. Political, Military, Infrastructure, Information, Economic & Social. The findings are scored based on their level of influence and impact. This score is then compared to baseline which reflects a normal environment where there are no active threats. (MCDC, 2019)

5 IMPROVING THE DETECTION OF HYBRID WARFARE FROM THE CYBER SECURITY PERSPECTIVE

This chapter goes through the methods and ideas to improve the capability to detect hybrid warfare on countries of any sizes which were formed during the research and how the previously mentioned research questions were answered. As mentioned before, the main sources for the ideas were of course the extremely rich material source from interviews and the literature behind the detection of hybrid warfare. The methods mentioned in this chapter can be used one by one or by combining multiple methods at the same time. In the early phases of developing hybrid detection capabilities, starting with small steps and single methods can be more efficient. A lot of these ideas cross-over each other and are based on possible points of improvement that were found during the research.

During the literature review and interview it came apparent that it wouldn't be easy or feasible in this study and with the level of access there was into the actual practicalities of nations to detect hybrid warfare to focus on attempting to dive deep to improve the practical detection processes. Instead of blindly throwing possible solutions to the practical workings of the detection systems in place, the choice was made to focus more on the visible parts which were known to the researcher such as the cooperation between different entities, while still maintaining the cyber security research point of view.

5.1 Cooperative effort with public to enhance the detection of hybrid warfare

One of the ideas that was drawn during the initial literature review phase was the increasing the amount and level of education on hybrid methods in EU & national level. The thought behind this idea is that it would be an easy and public way of reporting possible hybrid methods.

This topic was also brought up during the interviews as an interview question. The interviewed were asked the question: "How would you further use civilians in the detection of hybrid warfare? How do you see the value of civilian groups such as Bellingcat in the context of detecting hybrid warfare?" As a response to this question, every interviewed viewed this topic similarly and agreed that educating the public could provide useful information and wouldn't hurt the detection of hybrid warfare and that using civilian groups such as Bellingcat could provide valuable information that could otherwise be left out. (D. Benson, A. Cederberg, J. Schmid, J. Schroefl, Anonymous expert Interview 2021-2022)

According to The Center of European Policy (CEPA, 2021), to increase the public's knowledge about hybrid warfare, the topic should be introduced into multiple levels of education to ensure that understanding is built from early on. The Center for European policy analysis has recognized the low level of understanding of the public on hybrid warfare related concepts and its affection to decision making on hybrid related policies. (CEPA, 2021)

The increasing education level could also prove to be useful as it could increase the amount of civilian participation in hybrid warfare countering in forms of civilian groups such as Bellingcat or perhaps in a way of a human alerting/whistleblowing system. Both could potentially increase the detection capability of hybrid warfare, especially for countries with lesser resources to spend on the actual operative detection system. For example, there are currently civilians acting as military boat enthusiasts that spot and report military boat movement on social media (Farooq, 2022). With government backed training and increased public understanding a similar approach could provide significant data to analysts on other platforms when attempting to identify hybrid warfare.

A significant part of cyber security field tooling and information on threats comes from the community and its participation is generally seen as a good thing by employers during interviews for jobs. There are also volunteering groups such as the CV19 assisting companies which have fallen victims to a data leak or other cyber-crime (Cyberv19).

A similar open-source approach could be possible in the context of hybrid warfare with enough support from the government. The open-source based software could also benefit countries with lesser resource to spend on detecting hybrid warfare.

Ukraine has also adopted cooperation with civilians into their military tactics. A group of Ukrainian volunteers have developed an application for Android devices, which allows civilians to report incoming air threats such as enemy missiles, aircraft or drones. This information is then moderated and fed to the military intelligence and air defense. The application has already participated in successfully stopping Russian air attacks. (Sabbagh, 2022)

A similar approach could also be taken in the detection of hybrid warfare where the civilians would have an easy and fast way to feed information to the security officials about suspicious or potential indicators of hybrid warfare. This data could then be fed to the entities that are relevant in detecting and preventing hybrid warfare to enhance decision making.

5.2 Increased cooperation between EU states

During the interviews, every single one of the interviewed emphasized the importance of cooperation between western countries.

As noted by Cederberg in our interview, the problem with improving the detection of hybrid is the complexity and variety of interfaces and methods it is conducted with (Cederberg, Interview, 20.07.2021). Even though there are multiple different organizations in the EU which focus on hybrid methods, there isn't a single organization which is tasked with detecting hybrid warfare and improving the detection capabilities through research. Cederberg also noted that he feels that the lack of an organization with operative power and capabilities is significantly hindering the detection of hybrid warfare. An organization with a single task of detecting hybrid warfare could. An organization such as this could immensely increase the detection capabilities of countries with lesser resources as operative power and research knowledge could be shared with all participating countries. This would in general raise the publics general awareness of using hybrid methods and would hence straight affect the detection of hybrid methods. (Cederberg, Interview, 20.07.2021)

This chapter discusses a solution, where the usage of similar organizational structure across Europe on national level could enhance the communication between different actors and enhance the detection of hybrid methods. There could also be the effect of standardizing the collected data to enhance the data sharing process even further. This could also serve as a framework for countries with lesser resources to improve their hybrid method detection capabilities.

The following means were listed by the interviewees (D. Benson, A. Cederberg, J. Schmid, J. Schroefl, Anonymous expert, Interview, 2021-2022) as an answer to one of the interview questions on creating such an organization:

- Establishing standardized country specific baseline for detecting anomalies.

- Yearly revisiting of identifying hybrid vulnerabilities.

- Collection of hybrid intelligence data through multiple ways.

- Focusing all research about the detection of hybrid methods on a single organization to increase efficiency

- Participating in providing education to the public and other EU countries in order to enhance EU wide hybrid detection capabilities

Previously mentioned education of the public would be one of the main tasks for this organization, but it is something that could prove to be difficult to implement as hybrid warfare is not a simple concept to comprehend as shown earlier in this thesis. The education from enhancing the detection point of view should consist of the students learning about the ways hybrid warfare can be conducted on multiple interfaces and how a citizen can identify and report them. Holding public forums and seminars about hybrid more often. There seminars should especially be held in universities and other public places where anyone can attend.

The idea for this came from the interviews and literature which noted that there were problems mentioned between cooperations of different entities while attempting to detect hybrid warfare. The idea to draw from cyber security related researcher's previous background in the cyber security field. The security operations center model is explained in previous chapters.

During the interviews the following points came up from Cederberg's when asked about which things he would consider when discussing the civilian groups questions and their usage in hybrid warfare detection and usage of AI in detection of hybrid warfare. (Cederberg, Interview, 20.07.2021) The organization should contain experts from every possible hybrid method or attack interface or target areas. The experts should also be from different geological parts to gain as many different viewpoints as possible. There should be cooperation with other teams that are attempting to solve this problem to create an exhaustive system that can detect multiple interfaces at once. The tool should be able to detect the unknown unknowns and to do this by finding anomalies from the data. This team should also have AI-experts and others who have the skillset to develop tools to detect hybrid methods. The team should work with a single goal in mind. Creating a hybrid detection system based on AI. It could be that building an AI-based detection system is the only actually efficient way of detecting the constantly changing hybrid methods. The other ideas listed here work as mere mitigators of the problem. Every day the humankind generates more and more data (Marr, 2018) for which in turn causes there to be more data to be analyzed in terms of hybrid warfare. This highlights the importance of AI and efficient establishing of baselines similarly as in cyber security.

The idea of a joint task force is by no means new one. Although there are multiple articles about such ideas being mentioned in the literature of hybrid warfare, the joint forces in these papers would have focused on reacting and deterring to threats. Instead, the idea listed in this chapter focuses only on detection side of hybrid warfare and aims to solve its issues. Some of the papers did however, mention detecting hybrid warfare and why it is relevant to take into consideration while designing such joint task force. For example, Sean Monaghan (Monaghan, 2019), mentions in his paper discussing the topic of Joint Task Force and that increasing the cooperation between government organizations would be one of the keys to increasing the efficiency of detecting hybrid warfare. Just as the interviewed in the conducted interviews, Monaghan also thought that the responsible organizations should be able to analyze the data that was fed to them from all interfaces of hybrid warfare such as political or economic. He also noted that to be able to achieve such capability, a special training would be required for the analysts and that it couldn’t be achieved without close cooperation between relevant entities. (Monaghan, 2019)

5.3 Data standardization and cooperation of government entities in detecting hybrid warfare

The cooperation and its importance and shortcomings are highlighted multiple times in hybrid warfare literature and the interviews. The common consensus is that there is room for improvement to cooperating between relevant entities in hybrid warfare detection. (Monaghan, 2019)

There could also be the effect of standardizing the collected data to enhance the data sharing process even further. The data standardization means creating a standard on which the data that is received from multiple sources in multiple formats is then transformed to, so that the data can then be more easily digested by different systems and users (Egnyte, 2022).

Data standardization is important because it helps with problems such as bad data quality, data errors & removing unnecessary data. In information systems research and cyber security, the threat intelligence is often shared with certain standards such as TAXII to enhance information sharing between different parties (Connolly, Davidson, Schmidt, 2014). For example, different tools and products such as antivirus or endpoint detection & response can ingest natively data that is formatted in certain way such as the TAXII (Connolly, Davidson, Schmidt, 2014). There are also tools in Cyber Security field that’s only purpose is to standardize the threat intelligence so that it can be more easily digested and shared with others such as MISP (MISP, 2022). A similar approach should be taken when it comes to sharing the warning intelligence generated by nations. Standardized data could be ingested on national level faster which in turn would allow the governments to respond faster to hybrid warfare.

5.4 Tabletop exercises and threat simulation

When asked the following question: How would you decrease “the cost of entry” to detecting hybrid warfare? Especially in the context of countries with lesser resources to spend on such matters as hybrid warfare detection. What kind of things should one think about if tasked with enabling detection of hybrid warfare for all western countries? Some of the people interviewed mentioned that was that the value of holding tabletop exercises or like simulate possible threat activity on friendly targets. (Benson, Cederberg & Schmid, Interview, 2021-2022)

The interviewed were also unanimous in that the most important parts the exercise could improve were cooperation between different entities and finding new possible vulnerabilities to detect. The participants should include specialists from all government branches and agencies to be able to completely test and identify the weak points in cooperation and detecting hybrid warfare. The barrier to conducting these exercises should be set as low as possible so that every nation could start improving their hybrid warfare understanding as early as possible. (D. Benson, A. Cederberg, J. Schmid, J. Schroefl, Anonymous expert Interview 2021-2022)

It could be an interesting topic for future research. The research could for example focus on how efficient is using tabletop exercises for hybrid warfare training is and how could that efficiency be improved.

This idea of hybrid warfare tabletop exercise has already been taken into practice at-least in the following places in Austria where the Hybrid CoE developed hybrid warfare exercise was taken into practice successfully. The exercise was conducted on two levels, first being on the practical hands-on specialist level and the second on national political decisions making level. According to Austria the exercise highlighted the importance of clear communication between ministries in the event of being targeted by hybrid warfare. (Hybrid CoE, 2022)

Entities such as such as the Friends of Europe thinktank that have previously conducted similar exercises with participants from NATO and other relevant organizations. (EU monitor, 2019)

Just as with detection side of hybrid warfare, there isn’t much academic research that has been conducted on using tabletop exercises in training for hybrid warfare. However, there is some research that has focused on a single target vulnerability of hybrid warfare. Oleksandr Sukhodolia (Sukhodolia, 2018) for example, researched usage of tabletop exercises as a tool for improving resilience of critical energy infrastructure. The exercise was a success, and the tool helped the participants to understand their main issues. The cooperation between public and private sector was listed as the main point of improvement to increase the resilience of national critical infrastructure. The exercise also highlighted the need for an efficient management on multiple levels, both on national and on lower levels so that there can be progress. (Sukhodolia, 2018)

6 CONCLUSIONS AND DISCUSSION & FUTURE

The main objectives for this research were to find at least initial future research points and find if there is a room for improvement in detecting and identifying hybrid warfare. The second main objective was to clarify the terms relevant to identifying and detecting hybrid warfare. These objectives were viewed from the researcher's cyber security background.

This research contributed to the academic world by clarifying the terminology behind hybrid warfare and by bringing future research ideas to continue the research and by coming up with initial ideas for enhancing the detection of hybrid warfare and it can be used for as a base for future research and as a guide for implementing the improvements of detecting hybrid warfare. The cybersecurity point of view was implemented to gain a different point of view from the common military hybrid warfare research. This provided interesting and unique viewpoints and improvement ideas as hybrid warfare from cybersecurity point of view has little previous research available. However, this also caused issues during the research and literature review because of little to no material in a field where finding fitting literature can be difficult. This required the researcher to do extensive research on both topics and their literature and go the extra mile to correlate and combine the literature from both topics to gain academically valuable information.

During the research, multiple other issues also surfaced that affected the practicalities and the results of the research. The most significant limitations for this study were the researchers' own resources to spend on the project, scope of discussions, lack of previous studies in the research area and small interview sample size. These issues affected the research and how it was conducted and its results.

Previous academic work on improving the detection of hybrid warfare has been, as previously mentioned, low in numbers. The detection of hybrid warfare is a contemporary and evolving topic with little current research material to use. Especially in the literature review phase of this project, the literature for detection of hybrid warfare was difficult to find. There were some research paper's that were glancing the subject of detecting hybrid warfare, while still mainly focusing on other topics. This made it difficult to collect and correlate data from the literature as simply there wasn't enough material for each topic available. It also made it difficult to present information in readable and understandable way for the reader. As a solution for this, the previously mentioned MCDC countering hybrid warfare project has been a major source of information for this thesis. The amount of important information that the report contained and how easily it was presented was unmatched. This cleared a significant amount of previously mentioned issues where the material was simply nonexistent. The MCDC Countering Hybrid Warfare report contained significant amount of information on the topic that wasn't available anywhere else. The information was also excellently tied together which made it easy to be analyzed and used. Because of the reasons mentioned the literature base of this research was mostly tied to the previously mentioned MCDC report and has therefor had a major impact on the results and the research itself.

Secondly, the lack of researcher's resources resulted in a limited number of interviewed and the depth of discussion in interviews. With a larger pool of resources there could have been more interviews and more time for literature review. The research could have dived deeper and asked more complex questions from a larger group of interviewed experts. This could have resulted in better discoveries and valuable information that could have translated to better practical enhancement ideas. Having more resources could have enabled the research to be more technically oriented, which would have enabled the researcher to use their entire skillset to conduct the research, whereas now the technical cyber security side wasn't utilized to the fullest.

Lastly, the researchers lack of previous studies in the topic of detecting hybrid warfare affected setting the scope of the research and amount of time it took to finalize the research. With better previous understanding of the topic, the scope could have been set to focus on a more specific area of detecting hybrid warfare.

Because the level of classification of the topics discussed in this paper is generally high, the exact practices behind each country detecting and identifying threats are unknown. It is possible that some of the methods mentioned in this paper are already applied and in use by countries with more resources to spend on researching identification and detection of hybrid warfare. However, recommendations and improvement points found in this study can be useful especially for countries with lesser resources to spend in researching hybrid warfare related topics. This research has also brought together the field of information sciences. All the enhancement ideas mentioned in chapter 5 can be applied to straight to practice. The enhancement ideas in this paper were also meant to reduce the barrier of entry to start detecting hybrid warfare for countries with lesser resources. This goal was achieved at least partly as all these ideas have a possibility of being applied to practice with the minimal resources required.

This research has focused on enhancing the cooperation between different entities and other such high-level things to improve the overall level of being able to detect hybrid warfare. For this research the decision was made to look to solve the issue of detection from cyber security and information sciences point of view. The results correlate with those of previous researchers of the topic while also providing new ideas from the new point of view.

As mentioned in the previous chapters, the results of the interview and this research correlate with the findings of others in hybrid warfare. Because of the lack of research in detecting hybrid warfare, it is difficult to find literature that for comparing results as a lot of the articles and papers in hybrid warfare research only partly discuss detection of hybrid warfare. However, it has been possible to compare some of the results and studies such as in the case of Sukhodolia's (Sukhodolia, 2018) critical infrastructure tabletop exercise where the correlation could be made that with the results that are similar to the ones achieved in this research.

The second main objective for this research was to clarify the terms of hybrid warfare as they are often used differently. The difficult of understanding terms of hybrid warfare is one of the reasons which makes it more difficult for different organizations to efficiently communicate matters of detecting hybrid warfare. This turned out to be a difficult issue to solve and obviously requires further work in the form of correlation between the relevant organizations. This research introduced multiple solutions to this issue. Mainly, the unification of terminology of the detection of hybrid warfare through a framework that could be then used by all western organizations. This would enhance information sharing and result in more efficient communication. Another solution this research presented was collection of data in the form of literature view and interviews and unifying those in the previous chapters while still describing the difficulties and why those terms are difficult to determine.

The last objective of this research was to find at least initial research topics for future researchers. This objective was achieved as planned as this research has opened multiple opportunities for future researchers to continue and further research multiple topics and their applications into real world practice. Researching these topics could have a capability to significantly improve the western capabilities to detect hybrid warfare. Just as with this research, the mentioned possible future research topics can be approached from multiple angles. One of the possible point of views is the technical aspect and how to implement the ideas such as the application into reality.

The following separate questions rose during the research that could benefit the research community if researched further:

- How to enhance identification of critical vulnerabilities on state level

- What area of identifying and detecting hybrid warfare is the weakest and where should the potentially spare resources be focused?

- What would be the most efficient way for nations to start detecting hybrid warfare from scratch

- How to efficiently identify unknown unknowns from large datasets? How to filter the “noise” from data to generate only true positives?

- Would a mobile application designed for reporting possible hybrid warfare indicators be useful. How should such application be designed?

REFERENCES

Adams, W. (2015). "Conducting semi-structured interviews." *Handbook of practical p rogram evaluation* 4 2015: 492-505.

Bellingcat. About Bellingcat.
https://www.bellingcat.com/about/

Bilal, A. (2021). Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote.
https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Braha D. (2012). Global civil unrest: contagion, self-organization, and prediction. *PLoS One*. 2012;7(10):e48596. doi:10.1371/journal.pone.0048596.

Bryman, A. (2016). *Social research methods*.
https://books.google.fi/books?hl=fi&lr=&id=N2zQCgAAQBAJ&oi=fnd&pg=PP1&ots=dpNsDTK7oc&sig=8fzp-x3cgJbm69a5b2SZ88rNFrU&redir_esc=y#v=onepage&q&f=false

Center for European Policy Analysis (CEPA). 6.2021. Page 2
Hybrid Warfare of the Future: Sharpening NATO's Competitive Edge
https://cepa.org/wp-content/uploads/2021/07/Hybrid-futures-two-pager-v2.pdf

Checkpoint. What is a Security Operations Center (SOC)?
https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/

CISA. CISA Tabletop Exercise Packages
https://www.cisa.gov/cisa-tabletop-exercise-packages

Citation: Tian J, Xie H, Hu S and Liu J (2021) Multidimensional Face Representation in a Deep Convolutional Neural Network Reveals the Mechanism Underlying AI Racism. *Front. Comput. Neurosci.* 15:620281. doi: 10.3389/fncom.2021.620281 s. 9/9

Coffey, L. (2019). How to Defeat Hybrid Warfare Before It Starts.
https://www.defenseone.com/ideas/2019/01/how-defeat-hybrid-warfare-it-starts/154296/

Connolly, J. Davidson, M. Schmidt, C. (2014). The Trusted Automated eXchange of Indicator information (TAXII™).
https://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_May_2014.pdf

Crowdstrike, (2022). What is a Security Operations Center (SOC) ?
https://www.crowdstrike.com/cybersecurity-101/security-operations-center-soc/

CSA Singapore. (2021). GUIDE TO CYBER THREAT MODELLING https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf

Cyberv19. Our mission
https://cyberv19.org.uk/our-mission-cyber-volunteers/

DiCicco-Bloom, B and Crabtree, B. (2006) "The qualitative research interview." *Medical education*: 314-321.

Egnyte. (2022) Data Standardization: How It's Done & Why It's Important
https://www.egnyte.com/guides/life-sciences/data-standardization

Eu monitor, 11.2019. Hybrid warfare readiness: a tabletop exercise - Main contents
https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vl0acwbk3utr?v=1&ctx=vg9piqcfmzzz&tab=2&n=4

EU-Hybnet. Project overview.
https://euhybnet.eu/about/

European Comission. Hybrid threats. https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_fi

European Comission. The European Union What it is and what it does.
https://op.europa.eu/webpub/com/eu-what-it-is/en/

Farooq, U. (01.2022). Giant chessboard: Istanbul ship-spotters monitor moves for war. Aljazeera
https://www.aljazeera.com/news/2022/1/24/giant-chessboard-istanbul-ship-spotters-monitor-moves-for-war

F-secure. Detection, A quick guide to detections - what they are, how they work and how to read them
https://www.f-secure.com/v-descs/articles/detection.shtml

Gentry, J & Gordon, J. (2019). Strategic Warning Intelligence: History, Challenges, and Prospects. Strategic Warning Intelligence: History, Challenges, and Prospects - John A. Gentry, Joseph S. Gordon - Google-kirjat

Grabo, C. (2015). Handbook of Warning Intelligence, Rowman and Littlefield (complete and declassified edition), page 113

Gunneriusson, H. & Ottis, R. (2013). Cyberspace from the Hybrid Threat Perspective
https://www.jstor.org/stable/26486843

Harrington, D. (2022). What is Red Teaming? Methodology & Tools. https://www.varonis.com/blog/red-teaming

Hoffman, F. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, Virginia: Potomac Institute for Policy Studies. p. 29 https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Hoffman, F. (2016). The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War, Heritage Foundation. https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_ESSAYS_ HOFFMAN.pdf

Hoffman, F. (2016)The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War. https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_ESSAYS_HOFFMAN.pdf

Hybrid Center of Excellence. EU and NATO welcome Hybrid CoE https://www.hybridcoe.fi/news/eu-and-nato-welcome-hybrid-coe/

Hybrid Center of Excellence. Hybrid threats as a concept. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Hybrid CoE, 6.2022. National exercise with a focus on hybrid threats piloted in Austria https://www.hybridcoe.fi/news/national-exercise-with-a-focus-on-hybrid-threats-piloted-in-austria/)

Kennan, F. (1948). The Inauguration of Organized Political Warfare. https://digitalarchive.wilsoncenter.org/document/114320

Kevkhishvili, M. (2022). Top it skills in demand. https://www.comptia.org/blog/top-it-skills-in-demand

Kurmanau, Y & Bajak, F. (2022). Cyberattacks knock out sites of Ukrainian army, major banks. https://apnews.com/article/russia-ukraine-technology-business-europe-russia-e791990f60841b599f664c34f58403de)

Kurmanau, Y. & Bajak, F. (2022). Cyberattacks knock out sites of Ukrainian army, major banks. https://apnews.com/article/russia-ukraine-technology-business-europe-russia-e791990f60841b599f664c34f58403de

Luft, J. (1955). The Johari Window, A Graphic Model of Awareness in Interpersonal Relation.

https://static1.1.sqspcdn.com/static/f/1124858/28387950/1617395004320/THE+JOHARI+WINDOW.pdf?token=s2jPPOU5Bhj3lUTndZkdnY55A3s%3D

Malwarebytes. What is Stuxnet?
https://www.malwarebytes.com/stuxnet

Mandiant. Advanced Persistent Threats (APTs).
https://www.mandiant.com/resources/apt-groups

Marr, B. (2018). How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read.
https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=7cfa519e60ba)

MCDC, (2013). Multinational Capability Development Campaign (Public site) https://wss.apan.org/public/MCDCpub/default.aspx

MCDC. (2019). MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

Merriam, S. (2002). "Introduction to qualitative research." *Qualitative research in practice: Examples for discussion and analysis* 1.1 : 1-17.

Metz, C. (2021). Who Is Making Sure the A.I. Machines Aren't Racist?
https://www.nytimes.com/2021/03/15/technology/artificial-intelligence-google-bias.html

MISP. (2022). MISP features and functionalities
https://www.misp-project.org/features/

Mitzen, J & Schweller, R. (2011). Knowing the Unknown Unknowns: Misplaced Certainty and the Onset of War. Security Studies - SECUR STUD. 20. 2-35. 10.1080/09636412.2011.549023. (PDF) Knowing the Unknown Unknowns: Misplaced Certainty and the Onset of War (researchgate.net)

Monaghan, S. (2019). Countering hybrid warfare. *Prism*, *8*(2), 82-99.

Multinational Capability Development Campaign. (2019). Multinational Capability Development Campaign (MCDC) public site.
https://wss.apan.org/public/MCDCpub/default.aspx

Myers, M & Avison, D. (2002). *Qualitative research in information systems: a reader*. Sage, 2002.
https://www.academia.edu/download/49332780/Qualitative_Research_in_Information_Syst20161003-25845-701hjd.pdf

Nachaat, M & Belaton, B. (2021). SBI Model for the Detection of Advanced Persistent Threat Based on Strange Behavior of Using Credential Dumping Technique. *IEEE Access*, 2021, 9: 42919-42932. P. 1
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9380629

Nato. (2022). NATO's response to hybrid threats
https://www.nato.int/cps/en/natohq/topics_156338.htm

Nato. (2022). What is NATO?
https://www.nato.int/nato-welcome/index.html

NIST. Tabletop Exercise
https://csrc.nist.gov/glossary/term/tabletop_exercise

Ojala, A. (2016). "Business models and opportunity creation: How IT entrepreneurs create and develop business models under uncertainty." *Information Systems Journal* 26.5: 451-476.

Orlikowski, W & Baroudi, J. (1990). Studying Information technology in organizations: Research Approaches And Assumptions.
https://archive.nyu.edu/jspui/bitstream/2451/14404/1/IS-90-04.pdf

Pannucci, CJ & Wilkins, EG. (2010). Identifying and avoiding bias in research. *Plast Reconstr Surg*. 2010;126(2):619-625. doi:10.1097/PRS.0b013e3181de24bc
Identifying and Avoiding Bias in Research (nih.gov)

Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. Journal of Counseling Psychology, 52(2),
137−145

Popli, N. (02.2022). How NATO Is Responding to Russia's Invasion of Ukraine. Time.
https://time.com/6151115/nato-russia-ukraine-article-4/

Poston, H. (2021). Top threat modeling frameworks: STRIDE, OWASP Top 10, MITRE ATT&CK framework and more
https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride-owasp-top-10-mitre-attck-framework/

Rapid7. Threat Detection.
https://www.rapid7.com/fundamentals/threat-detection/

Routio. P. (2007). Finding Information in Texts,
http://www2.uiah.fi/projects/metodi/140.htm#herm

Sabbagh, D. (2022). Ukrainians use phone app to spot deadly Russian drone attacks. https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo

Schmid, J. (2019). COI S&D Conception Paper: Hybrid Warfare – a very short introduction. ISBN: 978-952-7282-20-5

Schmid, J. (2019). Hybrid Warfare on the Ukrainian battlefield: developing theory based on empirical evidence. Journal on Baltic Security, 2019; 5(1): 5-15

Schmid, J. (2019). The Hybrid Face of Warfare in the 21st Century. https://www.maanpuolustus-lehti.fi/the-hybrid-face-of-warfare-in-the-21st-century/

Schmid, J. Thiele, R. (2020). Hybrid Warfare – Orchestrating the technology revolution. https://www.ispsw.com/wp-content/uploads/2020/01/663_Thiele_Schmid.pdf

Sentonas, M. (2022). CrowdStrike Achieves 100% Prevention in Recent MITRE Engenuity ATT&CK Evaluation Emulating Russia-based Threat Groups https://www.crowdstrike.com/blog/crowdstrike-achieves-100-percent-prevention-in-mitre-engenuity-attack-evaluation/

Sukhodolia, O. (2018). Training as a tool of fostering CIP concept implementation: Results of a table top exercise on critical energy infrastructure resilience. *Information & Security: An International Journal*, *40*(2).

Symantec Security Response Team. (2018). Subverting Democracy: How Cyber Attackers Try to Hack the Vote. https://symantec-enterprise-blogs.security.com/blogs/election-security/election-hacking-faq

The European Centre of Excellence for Countering Hybrid Threats – What is Hybrid CoE
What is Hybrid CoE - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats

Thiele, R. (2020). Artificial Intelligence – A key enabler of hybrid warfare.
https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf

United States Department of Defense. (2022). DoD News Briefing - Secretary Rumsfeld and Gen. Myers.
https://archive.ph/20180320091111/http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636

United States Department of homeland security. (2016) GRIZZLY STEPPE – Russian Malicious Cyber Activity.
https://www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

United States National Institute of Standards and technology NIST. Cyber threats.
https://csrc.nist.gov/glossary/term/cyber_threat

Vogel, R. (2012). 'The Intelligence failures involved in Pearl Harbor', *Journal of the Australian Institute of Professional Intelligence Officers*, vol. 20, no. 2, pp. 44-51.