Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Social and Educational Sciences
Department of Sociology and Political Science

Jørgen Danielsen

The Security Politics of Hybrid Operations

An inductive, deductive and empirical approach to a nascent field of research

Master's thesis in Political Science
Supervisor: Gunnar Fermann
May 2023

NTNU
Norwegian University of Science and Technology

Jørgen Danielsen

The Security Politics of Hybrid Operations

An inductive, deductive and empirical approach to a nascent field of research

Master's thesis in Political Science
Supervisor: Gunnar Fermann
May 2023

Norwegian University of Science and Technology
Faculty of Social and Educational Sciences
Department of Sociology and Political Science

NTNU
Norwegian University of
Science and Technology

Acknowledgments

It is with great pleasure and a great personal sense of accomplishment that I present this Master's thesis. This product is the culminative representation of five years of hard work, dedication and intellectual exploration into the study of political science.

Undertaking the study of this thesis, into a nascent and fairly untheorized field, has been demanding, and at times exhaustive. The resulting product presented in this paper could not have been accomplished without the mentoring, support and supervision from a number of individuals.

First and foremost, I will express my deepest gratitude to my supervisor, Gunnar Fermann, Professor with the Institute for Sociology and Political Science with NTNU. His support, expertise and insights have been instrumental to the completion of this thesis and could not be sufficiently emphasized. His guidance and mentorship have inspired me to move beyond my past expectations and strive for excellence in my work.

Apart from Fermann, several others have provided me with invaluable guidance and help, both academically and socially. I would like to extend my most sincere appreciations to Eskil Grendahl Sivertsen with the FFI, and Ole Felix Dahl with the Norwegian Defence Ministry, which have provided me with a deeper understanding of information operations and Russian signaling. I would also like to thank the Royal Norwegian Air Force and NATO Air Command for access to additional data on Russian air activities.

Finally would I like to present my gratitude to my fellow students, which have been of great support during the years of study. Especial thanks to Patrick Schjølberg, Maja Auglend and Nora Lunde. I would also like to thank Stine Reitan, who have been a great team-player while writing about similar theories and overlapping fields of research.

Trondheim, May 2023

Jørgen Danielsen

Abstract

Hybrid Warfare became a highly popularized term after the Russian annexation of the Ukrainian peninsula, Crimea, in 2014. Despite its relatively recent revisit, the concept is by many scholars considered to be as old as war itself. Technologies developed over the last decades, such as social media platforms, and our increasing dependence on software systems for everyday activities make us vulnerable in different ways than previously. Adversaries may exploit these vulnerabilities and relocate the battlefield from the military to civilian spheres of society. How may states pursue such hybrid efforts to enhance their foreign policy strategies? This thesis has sought to grasp the concept of hybrid operations, inductively introduce new concepts that seem fit for further analysis as elements of such operations and integrate this concept into the frames of foreign policy analysis The design and methodology applied to manage such a task have been Eckstein's plausible probe design, a design feasible for early framework development, as it features both inductive and deductive analysis to be tested in a benign environment. In such, the empirical observations are believed to provide us with a deeper understanding as to whether the early structures of the concept is sufficiently feasible for wide-spread testing for generalizable results and conclusions, or if the framework does not hold adequately, make use of the lessons learned from the pilot-testing to suggest proper improvements for future adjustments to the framework. The thesis concludes that the framework presented does provide an understanding for the phenomenon through an analysis of foreign policy, but that it would benefit from an inclusion of variables at the individual and societal level to sufficiently explain the application of hybrid efforts.

Sammendrag

Begrepet "Hybrid Warfare" ble sterkt popularisert etter den russiske annekteringen av den ukrainske halvøya Krim i 2014. Til tross for at begrepet nylig har fått ny oppmerksomhet, betraktes konseptet av mange forskere som like gammelt som krig selv. Teknologier utviklet de siste tiårene, som sosiale medieplattformer, og vår økende avhengighet av programvaresystemer for daglige aktiviteter gjør oss sårbare på andre måter enn tidligere. Motstandere kan utnytte disse sårbarhetene og konflikten flyttes fra den militære slagmarken til sivilsamfunnet. Hvordan kan stater benytte slike hybride metoder for å styrke sine utenrikspolitiske strategier? Denne avhandlingen har søkt å forstå konseptet hybride operasjoner gjennom å induktivt introdusere nye begreper som virker egnet for videre analyse som elementer av slike operasjoner, og integrere dette konseptet inn i rammen av utenrikspolitisk analyse. Designet og metodologien som er anvendt for å håndtere en slik oppgave, har vært Ecksteins «Plausible Probe Design», et design som er fordelaktig for tidlig utvikling av rammeverket, da det innebærer både en induktiv og deduktiv analyse som skal testes i et vennligsinnet miljø. De empiriske observasjonene antas å gi oss en dypere forståelse av om de foreløpige strukturene i konseptet er tilstrekkelige for omfattende testing for generaliserbare resultater og konklusjoner, eller om rammeverket ikke holder tilstrekkelig, slik at erfaringene fra pilot-testingen kan brukes til å foreslå forbedringer for fremtidige justeringer av rammeverket. Avhandlingen konkluderer med at det presenterte rammeverket gir en dypere forståelse for fenomenet gjennom en analyse av utenrikspolitikk, men at det ville ha nytte av å inkludere variabler på individ- og samfunnsnivå for å tilstrekkelig forklare anvendelsen av hybride midler.

Table of content

List of Figures:

Part 2: Inductive reasoning of hybrid operations

Part 3: Deductive reasoning of hybrid operations

Part 4: Researching plausible cases of hybrid operations

Abbreviations:

A2/AD	Anti Access Area Denial
AO	Area of Operation
AOR	Area of Responsibility
C2	Command and Control
C4ISR	Command Control Communications Computers Intelligence Surveillance Reconnaissance
DDoS	Distributed Denial of Services
DOS	Denial of Services
EU	European Union
FPA	Foreign Policy Analysis
GIUK	Greenland-Iceland-United Kingdom
NATO	North Atlantic Treaty Organization
SMP	Social Media Platform
SOF	Special Operations Forces
SPM	Scope of Political Maneuver
Theatre	Theatre of War
UW	Unconventional Warfare

Part 1

An introduction to hybrid operations

1.0 Introduction

Hybrid Warfare became a highly popularized term after the Russian annexation of the Ukrainian peninsula, Crimea, in 2014. Despite its relatively recent revisit, the concept is by many scholars considered to be as old as war itself. Technologies developed over the last decades, such as social media platforms, and our increasing dependence on software systems for everyday activities make us vulnerable in different ways than previously. Adversaries may exploit these vulnerabilities and relocate the battlefield from the military to civilian spheres of society. How may states pursue such hybrid efforts to enhance their foreign policy strategies?

Hybrid Warfare, or hybrid operations, suffer from being subject to no clear and generally accepted definition. However, an aggregated definition would be:

> The synchronous or simultaneous use of conventional and unconventional measures by states or non-state actors. These measures are often applied in an effort "short of open conflict", facilitating covert action, leaving its originator with some level of plausible deniability.

Hybrid Warfare is a fairly broad concept, to this day, more or less used as a describing term for all untraditional ways of conflict. This has led the term to be subject to widespread use, which widens the scope for what we would consider measures of hybrid operations. The research field of hybrid Warfare is relatively nascent, and only a handful of studies set forward to grasp the concept's core fundamentals or provide a wider understanding of the phenomenon. Much of this problem is related to a siloization within the research field. The concept of hybrid Warfare draws on various domains, such as the cyber, information, political, economic, and military domain. The various domains and instruments included causes much of the research to be centred within each of these, leading to minimal in-depth research on the simultaneous or synchronous use of these instruments in a joint effort. Many studies providing empirical analyses of hybrid operations tend to take the understanding of the phenomenon as a given, which is a severe problem given the limited knowledge of its core fundamentals.

Hybrid Warfare is by many considered an integrated part of "Next Generation Warfare" concepts. The ever-developing nature of the concept makes it highly relevant for research, which is critical for states to respond to such acts in a suitable manner, but also to manage to project power by using such measures themselves. The topic is also interesting because of its deficiencies in research. The latter allows for contributions to be made on a conceptual level.

This thesis sets out to solve some of the issues in the existing literature by contributing to the deeper aspects of hybrid operations. Its primary purpose is to integrate theories of hybrid operations into a framework suitable for the study of foreign policy, by using Eckstein's *plausible probe research design*. To efficiently achieve such, great parts of this thesis are allocated to provide the reader with a comprehensive understanding of the phenomenon, this part separately to be considered a contribution to the field of its own. Further, the concept will be prepared for integration into the existing theories of security politics within foreign policy analysis and subsequently also tested empirically in a pilot study to assess the sustainability and robustness of the framework.

This thesis will be divided into five main parts. Part 1 will provide the introductory section to this thesis, as well as the research problem, research design and methodology chosen for this paper.

In Part 2 of this thesis, I will conceptualize and prepare hybrid operations for a study of foreign policy analysis. Part of this work is based around establishing existing concepts and theories of the phenomenon and compiling these into coherent and overarching frames for further dissemination. Part 2 is intentionally a large section of this thesis, as such overarching, yet in-depth analysis of the phenomenon is hard to find in the existing literature and is crucial to sufficiently provide an understanding of the concept in the subsequent parts on deductive reasoning and empirical testing. In addition to the existing concepts, I will adapt new concepts adapted from traditional military doctrine that could be reinvented into a hybrid context. Further, the existing literature falls short of sufficiently producing arguments on the various intensity of hybrid operations, and central terms are used either interchangeably or with little substance to explain the boundaries between these. To sort for this problem, I will produce and illustrate arguments that provide a clear and understandable overarching taxonomy of hybrid operations and a stronger argument for when and how to apply the correct terms to each observation of hybrid efforts.

Part 3 will introduce the induced concepts and arguments to theories of foreign policy analysis and present a brief overview of FPA as it is today. Finally, as hybrid operations undeniably are tools of security politics, I will seek to apply structural theories of realism, both offensive and defensive, to provide a theoretical foundation for empirical testing of the phenomenon.

In Part 4, the framework of concepts and theories will be tested empirically towards a benevolent case in the Plausible Probe research design format. The design involves empirical testing of a preliminary framework in a benevolent testing environment to see if the framework is sufficiently bolstered for widespread testing or if changes and development must be made. The presumed benevolent environment for this specific pilot study is the Russo-Ukrainian war, which has been ongoing with various degrees of intensity since 2014. For simplicity, I have divided this war into two separate cases: the Russian hybrid operation in Crimea from February 2014 until the annexation in March the same year and the Russian full-scale invasion in 2022. The decision to split the war into two cases based on the intensity of these periods leads to methodological complications, which will be further discussed later. However, the temporal or autocorrelative problem it poses provides important arguments critical to the understanding of the functionality and mechanisms of hybrid operations.

In the final part of this thesis, Part 5, I will conclude with the findings of the thesis and the robustness of the framework developed, as well as provide suggestions for possible modifications to the framework and future research in the field of hybrid operations and hybrid warfare.

1.1 Research question

Hybrid warfare, in combination with theories of foreign policy, opens a series of possible research propositions within the field of political science. Whereas research questions are intended to both factor as a directing guidance for the paper, it is also supposed to serve as both inclusive and exclusive simultaneously (Maxwell, 2005, p. 67). As established while doing initial research for this thesis, the field of hybrid warfare separately is conducted in various directions. Nevertheless, it is somehow siloed to a degree where overarching studies, combining the knowledge gathered from sub-studies of the concept, is at a minimum and, in many cases, outdated regarding the technological development and the eternal nature of change and development of the concept of hybrid warfare.

The combination of Hybrid Warfare theory and theories of foreign policy analysis limits the possible approaches to the phenomenon. Therefore, for this paper, I have decided to look deeper into why states apply hybrid operations strategies, either as stand-alone operations or as integrated parts of multi-domain traditional warfare. Moreover, how do the attributes of hybrid warfare feature key elements of theories within foreign policy analysis? To answer these questions, this paper will be guided by the following proposition:

> **Generalized Research question:**
>
> *How may we approach, theorize and research the security politics of hybrid operations?*

In addition to the generalizable research question, this paper seeks to answer a specific question related to the empirical case study to the end of this analysis. As will be discussed in the following chapter, there are methodological limitations to the generalizability in this study. As the phenomenon is only publicly recognized in a handful of cases empirically, a generalizability of the findings in the empirical analysis would be impossible. Rather than generalize, the findings would serve as a single-case result of the questions raised by the overall analysis and serve as lessons learned for future research into the field. A second, more specialized research question would serve to adequately narrow down the analysis for the scope and extensiveness allowed for this format. The specialized proposition would be:

Specialized:

How may the framework of hybrid operations for theories of foreign policy analysis explain Russian use of hybrid methods during the conflict in Ukraine in 2014 and 2022?

The specialized research question is directed at the empirical testing of this thesis and serves to cover the scope of this section; to test and verify the functionality of the framework built in the parts previous to the case study. It does not seek to find generalizable answers, hence, the empirical findings will provide answers for either the robustness of the framework, or questions directly related to Russian hybrid warfare strategies.

1.2 Methodology and research design

The plausibility probe:

The *plausibility probe* is a search design introduced by Harry Eckstein (1975). The research design features a *fitting case strategy*, whereas limited time and resources for uncertain projects may be resolved by a pilot study, "a sort of trial test of a given theory on a particular case" to analyze the initial validity of a theory or concept (Moses & Knutsen, 2012, p. 138). Eckstein maintains that "At a minimum, a plausibility probe into theory may simply attempt to establish that a theoretical construct is worth considering at all, that is, that an apparent empirical instance of it can be found" (Gomm et al., 2009, p. 141). Fermann (2022, p. 215) asserts that "by turning the epistemological argument 180 degrees, we may also use the probability probing reasoning as a vehicle for developing more solid theoretical generalizations".

As far as Eckstein's theory is centred around the initial testing of theories and their validity, it mainly concerns the testing of theory from a deductive perspective, top to bottom, rather than testing inductive propositions. Jack S. Levy introduces inductive plausibility probe as a theory-building design that allows researchers to "sharpen theoretical arguments, or to refine operationalization or measurement of key variables, or to explore the sustainability of a particular case as a vehicle for testing theory before engaging in costly and time-consuming research efforts" (Levy, 2008, p. 6). Levy further argues that the plausibility probes thus are considered generally nomothetic by orientation, "since the analyst probes the details of a particular case in order to shed light on a broader theoretical argument" (ibid).

The proposition by Fermann (Ibid) will be the process for the research design of this paper. The format of the master thesis does not allow for extensive analysis, both deductively and inductively, to be tested empirically due to the frames and limits of the format. Additionally, initial research into the field has revealed a lack of coherent and overarching theories to be built, which do not allow for simple theory testing without a proper inductive approach to generate a framework of its own. The design of this master thesis will seek to inductively maintain a grasp of the various interpretations of hybrid operations, introduce taxonomies and concepts, and introduce a coherent understanding of the phenomenon, not from a perspective of war or conflict studies, but from a political scientifical approach, by understanding how this instrument may be used by states towards other states. To reaffirm hybrid operations as an instrument of foreign policy strategies, I will deductively approach the concept from a theoretical perspective of systemic theories of political realism to understand how we may

understand the concept and its application by existing systemic theories of foreign policy and international politics. *The emphasis in this thesis is on the inductive section*, mainly because there is a massive need for clarification on the concept, not extensive research into the various instruments of hybrid operations, but the concept as an overarching mode of coercive power projection. After the inductive and deductive framework for analysis is put forward, I will proceed with empirical testing with a "benevolent" case study in a suitable environment. As Levy (2008) argues, illustrative case studies would also fit into the plausibility probe research design. Illustrative case studies are often "quite brief, and fall short of the degree of detail needed either to explain a case fully or to test a theoretical proposition" and would instead aim to "demonstrate the empirical relevance of a theoretical proposition by identifying at least one relevant case" (Levy, 2008, pp. 6-7). The latter is critical to this thesis, as the format does not allow a broader scope than an illustrative case study if the emphasis and dominance of the inductive analysis should hold.

The empirical analysis will be conducted as a comparative study of two cases: The Russian annexation of Crimea in 2014 and the full-scale Russian invasion of Ukraine in 2022. Although these are tested as two cases in this study, the two cases are highly intertwined and suffer from a series of methodological deficiencies and biases, such as high correlation, both because of the similarities in the cases but also because of the temporal problem of these cases happening merely eight years apart. However, there is no doubt that the 2014 case led to a hype around hybrid operations as a concept, and the scarce availability of attributed cases of hybrid operations makes it the ideal case-option for this study.

1.3 Case-specific Methodology and Problems.

For initial comments, I must once again restate the purpose of this empirical section. For a theory-testing paper, this case choice would suffer from an obvious selection bias. It must therefore be understood that it is a meaning behind the choice of cases and that the analysis is merely for initial assumptions and further framework development.

Methodologically it must be acknowledged that although treated as separate cases, these campaigns are part of one ongoing conflict and will thus be subject to various biases while analyzed. One apparent type of bias concerning these cases is the autocorrelation problem, which will be further discussed below.

1.3.1 Autocorrelation and temporal problems concerning the case selection.

Jakobsen & Mehmetoglu maintains that assumptions may be breached "if the observations are dependent on each other" and that such connection among cases implies a methodological error of autocorrelation (Jakobsen & Mehmetoglu, 2022, p. 167). There is little doubt that the cases are highly correlated and, in many instances, should be considered one case rather than separated. On the other hand, there is a clear separation of periods concerning the intensity, which makes it interesting to divide the periods into different campaigns. Thus, it would be scientifically compelling to explain the two cases as methodological counterfactuals regarding the choice of methods, but the high degree of autocorrelation appearing in plain sight makes such an attempt ill-fated.

It is evident that, as discussed in the inductive part of this paper, hybrid campaigns bear both the upsides and downsides of being prone to an element of surprise. Once a hybrid operation is launched and detected, the adversary will seek to minimize damage and mitigate vulnerabilities. This makes it hard for an actor utilizing hybrid means to revisit prior battlespaces using the same tactics and instruments as previously. The concrete examples of how this works, in reality, are seen in these very two cases.

Carnegie Endowment does, in their 2022 report, state that "Ukraine's national internet and IT infrastructure, even before the war, was resilient in many ways" and quotes Emile Aben that "researchers have identified low market concentration at multiple levels and the relatively high number of interconnect facilities, meaning there are no obvious choke points, or individual networks whose loss would have a crippling effect on the internet in Ukraine" (Bateman, 2022, p. 40). This means that the 2014 campaign resulted in significant mitigations

made by Ukrainian state and private entities to reduce digital vulnerabilities, which directly affected the success of Russian cyber operations during the 2022 campaign.

OECD maintains that although the flow and disruption caused by Russian disinformation campaigns significantly increased after Russia's invasion in February 2022, measures were taken after 2014 to maintain information dominance and create information resilience:

> "Ukraine's response to the Russian disinformation threat has built upon progress made in strengthening the information and media environment since 2014 and in establishing mechanisms to respond directly to information threats. These include efforts to provide accurate information, ensure that media organisations can continue operations, and policy efforts to combat the threats posed by Russian state-linked media" (OECD, 2022, p. 2).

Correspondingly, the OECD maintains that equal measures were taken by actors outside the theatre, disrupting Russian attempts to influence global opinions on the war. As the above sections also include Russian macro-level attempts to apply hybrid measures against non-theatre involved actors, it is essential to maintain that the 2014 campaign and corresponding utilization of the information domain, as well as succeeding information campaigns, have led to a form of predictability of Russian choices of methods, and thus make such utilization less effective and therefore produce less utility. The OECD maintains that:

> "Internationally, governments rapidly recognised the disinformation threat in the context of Russia's largescale aggression against Ukraine. In response, they have highlighted narratives and tools used by the Russian government, sanctioned media and personalities, and supported media environments domestically, as well as in Russia and Ukraine. International organisations similarly executed fact checking and debunking programmes, as well as provided cross-organisational mechanisms for information sharing and technical support" (OECD, 2022, p. 2).

1.3.2 Selection Bias

The research design for this study, Eckstein's Plausible Probe, encourages empirical testing in a "benevolent" environment. This inevitably means that the empirical observations selected for the analysis are chosen on its merit as a "likely" case for dissemination. This leads to a selection bias of observations (King et al., 1994, pp. 139-140). This bias is accounted for in the analysis, as the primary objective is of the analysis is to test the framework, not to produce generalizable conclusions, although conclusions on the specific case might still be drawn.

Part 2

Inductive reasoning of hybrid operations

Conceptualizing and theorizing the foreign politics of hybrid operations.

The inductive part of this thesis seeks to provide a clear understanding of the previous research on hybrid operations and introduce a couple of new concepts found in traditional military doctrine, which will be adapted to a hybrid context. The inductive framework will provide the necessary background knowledge to sufficiently provide a foundation for a preliminary framework for adapting the hybrid doctrine for the security politics of political science theory. Following this, I will introduce terms, develop typologies, and determine the boundaries and borderlines of related terms.

2.0 Literature review

2.1 Existing literature within the field of Hybrid Warfare

Hybrid warfare became popular following the publishment of the so-called "Gerasimov Doctrine" in 2013, a journal article by the Russian Chief of the Armed Forces, General Valery Gerasimov. Gerasimov laid forward a series of notions on "Next Generation Warfare", a concept adopted as Russian doctrine. The concept brought forward the use of force beyond military capabilities and became even more relevant after the Russian annexation of Crimea, an operation by many considered a text-book example of the Gerasimov-playbook.

However, Hybrid warfare is no new concept. Most literature emphasizes that hybridity in operations has occurred since the earliest encounters of military conflict. However, the birth of Hybrid warfare as a theoretical and doctrinal concept is much more recent.

Frank G. Hoffman did in 2007 publish an article on behalf of the Potomac Institute of Policy Studies, "Conflict in the 21st Century: The Rise of Hybrid Wars". The article has become one of the main articles in the study of Hybrid warfare as a concept and may be the cornerstone in establishing the phenomena as a concept. It is impossible to write a study on the concept without referring to Hoffman, which has become evident while researching the topic. The article brings forward the phenomena as a military concept, which Hoffman maintains incorporates *"a range of different modes of conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion and criminal disorder" (Hoffman, 2007, p. 14)*, a definition of which most subsequent attempts at grasping the phenomena is building on in some form. Hoffman focuses mainly on the initial study of

this new form of combined warfare but makes no effort to determine how the conventional and irregular tactics are carried out.

The Hoffman article has inspired a series of new articles and studies into the phenomena, many of which attempt to specify how Hybrid warfare manifests itself in real-life operations. One such scholars are John Chambers (2016. Chambers' article is written in the aftermath of the Russian annexation of Crimea and is characterized by the experiences of that operation. Chamber's attempts further build on the foundations of Hoffman and seeks to explain how the phenomena may materialize in future conflicts, how vital the after-action reports are for the resilience against such tactics, and how we need to adapt to overcome hybrid challenges in the future. Chambers maintains that Hybrid warfare is the bridge between conventional and irregular warfare, which "combines the aspects of the two types of warfare in a single space and time" (Chambers, 2016, p. 8). One of Chambers' primary objectives is to establish awareness of the greyzone. The greyzone as a concept is often used in literature, but few studies make such an attempt to provide a theoretical definition of the phenomenon. Chambers establishes the greyzone as an *operational environment*, a set of conditions, circumstances and influences that affect the ability to employ capabilities and make decisions (Chambers, 2016, p. 13). This paper will describe the greyzone in further detail in the following chapters.

In 2017, a multinational research group, MCDC, produced a report on behalf of the UK government (Cullen & Reichborn-Kjennerud, 2017). The report is set to understand the phenomenon and produce generalizable frames for how the concept unfolds, based on empirical findings from previous encounters, such as the previously mentioned case of Crimea, but also others. The report is one of the most coherent and detailed reports on hybrid warfare after the Hoffman report, but whereas others, such as Chambers (2016), focus on how western military doctrine needs to be altered to face tomorrow's adversaries, the MCDC report is instead focusing on the defensive aspect, how to build resilient societies, and how to minimize damage and mitigate vulnerabilities. As such, the MCDC report does, in addition to the fundamental theory on hybrid operations, contribute to the fields of risk management and counteractions against hybrid operations with a defensive approach.

Another important contributor to the theoretical aspect of the field is Sverre Diesen, on behalf of the Norwegian Armed Forces Research Establishment, FFI (Diesen, 2018). Diesen's work is centred around how Hybrid warfare enables the escalatory process between peace and full-scale military conflict. The article is directed mainly towards Norwegian interests and

includes a scenario of low-intensity Hybrid warfare against Norway. The scenario and its theoretical foundation is more specific than the literature previously presented and specify different instruments of hybrid operations. It is fair to remark that such elements had been part of studies previous to that of Diesen but in a much less theoretical and systematic form. Diesen further expands on the framework leading back to Hoffman, but whereas former studies focus mainly on the combination of conventional and irregular or unconventional warfare, Diesen distinguishes between kinetic and non-kinetic operations and thus further specifies the actions on an operational level. One of the less discussed contributions from Diesen is the distinction made on the instruments between the operational domain and the operational intent (Diesen, 2018, p. 15).

The distinction between the instruments, the gateway and the environment or the intention by which the action takes place is fundamental in the studies coming in the time after 2015. Much effort is put into the research and analysis of instruments by which Diesen, amongst others, consider means of Hybrid warfare, being sabotage, cyber operations, influence campaigns etc. These studies are often siloed, which would be a describing term for the following research on the area. With the development and importance of the cyber domain in both military operations and society in general, numerous studies have been conducted to grasp how states and non-state actors may employ malicious operations in the cyber domain to disrupt the general society, produce chaos, and coerce both private businesses and government bodies to alter their preferred policies, and by such maintain some form of coercive power towards those entities.

2.2 Critisism and insufficiencies with existing literature of Hybrid Warfare

The studies on cyber operations, influence operations and other hybrid instruments are siloed to the level that there is a lose and incoherent agreement on how these are distinguished and separated. Some scholars and establishments consider operations in the information domain, such as propaganda and influence campaigns, as cyber operations, even though cyber is merely the facilitating gateway for such actions. However, the intentions and resulting utility returns are happening in another domain. This makes it difficult to produce coherent, agreeable terms, concepts, and theory that is extensive enough to provide an in-depth picture of Hybrid warfare as an overarching concept of coercive power, both on the conceptual, theoretical, and specific operational levels.

An extensive number of such siloed studies will be employed in this paper to attempt to provide an in-depth study of the concept. These studies are often conducted by research establishments such as the previously mentioned FFI, its Swedish counterparty FOI, and a series of governmental and private entities within the fields of these domains. An inclusion of the details in the operations is completely necessary to fulfil this paper's primary objective – to merge the concept and theories of Hybrid warfare with theories on foreign policy.

Although hybrid warfare as a term and concept is a popular area in conflict and war studies literature, there exist intrinsic weaknesses in the existing knowledge of the concept, at least of what is disseminated for public reading. One of the most evident and widespread problems is the lack of a common understanding of the concept. Even official research, such as the MCDC article series, struggled to agree on a common definition of the phenomenon. Although most articles define the concept within somewhat similar frames, mainly alterations of the Hoffman definition, there exist variations in our understanding. Further, the understanding of the terms "hybrid warfare", "greyzone operations", and "hybrid operations" are inadequately distributed throughout the academia. Hybrid warfare as a term is often used as the universal concept for events of hybrid nature, and there is no distinction between the environment and the frames within these events take place. There is also a problem regarding how hybrid warfare normatively should be placed within military doctrine. Some scholars define hybrid operations as irregular or unconventional warfare primarily because the tactics differ from what we observe in traditional conventional warfare. Others, such as some of the scholars described in the section above, describe hybrid warfare more as a combination of the existing variations of warfare. This fact has made it evident for this paper to revisit the fundamental definitions of war, warfare and conflict, to place each term in its correct "environment" and hierarchical place.

The most relevant insufficiency in contemporary studies of hybrid warfare is the lacking bridge between war-studies and studies of foreign policy and international politics. Most reports are descriptive and seek to understand the concept of hybrid actions. However, few, if any, reports set out to explain why states utilize hybrid measures, under which conditions, against what kind of adversaries, and how these states decide on instrument-choices in foreign policy. Why should a state carry out power projection through hybrid warfare when it could use conventional methods only?

3.0 Theories of hybrid warfare

3.1 Definitions and terms

Hybrid operations and hybrid warfare could be considered one of the biggest "hypes" of security studies over the last decade and became especially prominent for the study of international conflicts after the Russian annexation of Crimea in 2014, which this paper seeks to study.

The terms "hybrid warfare", "hybrid operations", and "greyzone operations" are often used synonymously, but previous research has revealed that these terms must be distinguished and put in their proper context (Danielsen, 2022). The fundamental core of hybrid warfare is hybrid operations. Hybrid operations bear no distinct common definitions, and efforts to produce such has been proven challenging (Cullen & Reichborn-Kjennerud, 2017, p. 8). However, most studies agree on the fundamental principle of hybrid operations being *the combination of synchronized efforts of both conventional and unconventional means of power* (Cullen & Reichborn-Kjennerud, 2017; Diesen, 2018, p. 8).

What does this definition of hybrid operations mean? The definition speaks to the employment of various means in a coordinated and synchronous effort. These means are both conventional and unconventional, of which hybrid operation in its very base is distinguished from conventional military operations.

Conventional military operations are often considered the traditional ways of warfare in which identifiable military forces of one state engage the military forces of another country. Conventional operations are by US military doctrine defined as:

> A form of warfare between states that employs direct military confrontation to defeat an adversary's armed forces, destroy an adversary's war-making capacity, or seize or retain territory in order to force a change in an adversary's government or policies. The focus of conventional military operations is normally an adversary's armed forces with the objective of influencing the adversary's government (US Army, 2008, p. 4).

Conventional warfare is often conducted in contemporary operations as coordinated efforts across the air-, cyber-, land-, maritime- and space-domain, termed *Multi-Domain warfare* (Perkins, 2017, p. 7). These could either be carried out to serve strategic objectives independently within the theatre of war or be integrated into *Joint Operations*, which could be exemplified as air support to land operations or maritime support to extract or infiltrate either land- or air assets (US Army, 2022, p. 19).

Unconventional warfare, on the other hand, is typically considered as military efforts outside the regular spectre of conventional operations. These could be asymmetrical efforts such as guerilla warfare, sabotage operations, or terrorism. Although various unconventional warfare efforts are asymmetrical by nature, not all unconventional operations are asymmetric (US Army, 2008, p. 3).

The US Army (2008, p. 3) defines unconventional warfare (UW) as such: *"Operations conducted by, with, or through irregular forces in support of a resistance movement, an insurgency, or conventional military operations".* The definition suffers from being framed in a perspective of army doctrinal efforts. However, it explains the efforts of small specialized groups, such as special operations forces (SOF), special mission units (SMU) or special intelligence elements conducting clandestine operations on enemy territories, such as sabotage operations, terrorist operations, renditions of essential enemy personnel, or other operations conducted by covert efforts in support of a greater strategic effort. The US Army definition is inherited to its domain and fails to recognise various other efforts as part of UW. Such efforts could be cyber-operations, foreign direct investments, influence operations, information warfare, and election interference (Cullen & Reichborn-Kjennerud, 2017; Diesen, 2018; Larson et al., 2009).

Although Diesen (2018) acknowledge the definitions of hybrid warfare as the combined efforts of conventional and unconventional means, he instead distinguishes between the means as kinetic or non-kinetic efforts (Diesen, 2018, pp. 7-8). Diesen defines kinetic efforts as irregular operations seeking to cause the adversary loss of personnel and material without seizing, gaining, or holding territorial control. Conversely, he refers to non-kinetic efforts as operations seeking to manipulate the situational awareness of the enemy without the involvement of lethal action (Ibid).

3.2 Plausible deniability and attribution – the key aspects of covert action.

The next concept in need of clarification is plausible deniability and covert actions. Hybrid operations can be based on both overt and covert action (Diesen, 2018, p. 15). The difference lies in the attributionality of the action. As covert operations are the most related applications of hybrid measures, at least in popular media, plausible deniability has been a popular term in such discourse. Operations, if carried out as covert action per se, allow decision-makers to deny involvement or sponsorship in the event. Cormac and Aldrich (2018) distinguish between plausible and implausible deniability, whereas the difference lies in the actual degree of plausibility.

Attribution, on the other hand, refers to two phenomena. The first is attributionality, or in other words, how exposable the originators of the operation are. The other relates to attribution as the instrument of foreign policy, where states hold other states accountable for actions made (Kolb, 2017, p. 71). In such matters, attributions are often followed by other foreign policy instruments, such as sanctions, diplomatic efforts or war in extreme cases.

Further discussions on ambiguity and the degrees of plausible deniability and implausible deniability will be further discussed in subchapter 3.3.4.

3.3 The layers of hybrid operations

In a previous work, I have discussed the various layers of hybrid operations. Hybrid operations are complex and consist of several layers of means and operational environments. In addition to these dimensions, hybrid means may be applied with various intensities, of which the effect is likely to vary (Danielsen, 2022, pp. 10-11).

3.3.1 Domain and intent

The lowest levels of hybrid operations are the means and instruments applied: "Operational intent" and "Operational domain". These levels are adaptions from the specific distinction made by Diesen (2018, pp. 14-15). The terms distinguish between the intended action and the domain by which such action is operated. This could be exemplified by election-interference, as seen in the 2016 presidential campaign in the US (Mueller, 2019). Election-interference itself is the intended action. To accomplish results of interference, a series of actions must be made. These could be related to, for instance, information and influence operations (polarization and disinformation, propaganda etc.) or sabotage by either physical operations (SOF, special intelligence activities, proxies etc.) or cyber (Denial of services or data manipulation). The complexity is evident and makes it difficult to understand the connection between domain and intent. It also emphasizes that various domains might facilitate the same operational intent, and these could be employed singularly or by synchronized efforts, defined by several simultaneous attacks through various domains, employed to serve the same target.

Recall at this point the definition of hybrid operations as *the synchronous application of hybrid means*. This implies that the application of one single hybrid instrument does not invoke the use of the term *hybrid operation* unless other hybrid means are employed simultaneously or against the same target over a longer or shorter timeframe, which could be considered part of the same operation. In cases where only one hybrid instrument is employed in an operation, the operation should be defined by its domain (e.g., Cyber-operation) rather than by the term hybrid operation.

Hybrid operations serve to establish the phenomenon in which *several operations through a variety of domains are employed in a joint and synchronized effort to facilitate strategic objectives against the same target or objective*. If these conditions are not met, the operation will remain at the stand-alone domain level, as described in the previous paragraph.

Both hybrid and domain-specific stand-alone operations could then be deployed into various *operational environments*. The US Army defines the operational environment as "A

composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander" (US Army, 2021a, p. 74). More simplistically, the operational environment could be understood as the situational understanding by the antagonist and protagonist parties of the conflict, which affects the choices of actions and strategies. This leads to a discussion over definitions and conditions over which the term "war" comes to use. For example, could a conflict be defined as a war if the state attacked does not recognize the attack as an intentional hostile act by another state actor?

2.3.2 When do hybrid operations qualify as acts of war?

The infamous Carl Von Clausewitz does, in his book "on war" state that "*war is thus an act of force to compel our enemy to do our will*" (Clausewitz et al., 2007, p. 13). This definition is very similar to the generally accepted loose definition of power, as the *ability to make an entity do something it otherwise would not have done*. By the definition of Clausewitz, war is merely the general application of power to force our will on another entity. Although Clausewitz includes "act of force", it does not define how or by what means force is applied. A more specific understanding of warfare is presented by Hedley Bull (cited in Vasquez, 2009, p. 24):"War is organized violence carried on by political units against each other". Bull introduces two new concepts into the definition; organized violence, which could be understood as a detailed variation of Clausewitz's "act of force", and "political units", which details the actors of Clausewitz's "enemy" and plays on another famous citation of Clausewitz, as war being the continuation of politics by other means (Clausewitz et al., 2007, p. 28). These definitions alone, however, favour the definition of *warfare,* which could be understood as the act of hostile activities within the frames of the conditions above. It does not necessarily adequately define the situational understanding, or societal environment of "war", in which acts of warfare are employed. One problematization here is whether a situation could be defined as a "war" if the situational understanding is not shared by both parties of the conflict. This problem is relevant for the next problematization.

International law "regulates" how and the conditions under which inter-state war should occur. The application of conventional military power in offensive operations thus appears clear and obvious as acts of war and makes it easy to define and observe both by the attacked state and third-party actors. However, hybrid warfare facilitates covert operations, of which actions do not clearly indicate intent or hostility. Many of these actions are also indirectly legal by law in democratic countries. Examples of such actions by hybrid means could be

influence-operations or disinformation. Many national constitutions offer widespread rights to freedom of speech, by which introductions of alternative truths and support of specific political perspectives do not necessarily violate national law (Veibäck et al., 2021, pp. 18-19). These actions, intended to manipulate the enemy to abide by our will, do not directly comply with the definitions by Clausewitz and Bull, as the actions are no use of force by direct terms, nor organized violence.

3.3.3 Plausible deniability and the greyzone

The covertness of these measures prohibits the antagonist state from being recognized as the originator of the hostilities, thus, from being recognized as violating the United Nations Charter 2.7, in which the ratifying states are prohibited from intervening or interfering in domestic affairs in other signatory states (United Nations, 1945, p. 3). In other words, as long as plausible deniability holds, the acts are not legally considered "acts of war", although the actions clearly serve to fulfil objectives that violate Article 2.7. Other acts by hybrid means, such as sabotage of infrastructure, assassinations of strategic personnel, denial of services etc., serve similar objectives as the above example of information operations, being to limit political options and scope of manoeuvrability to such degree that the remaining course of action aligns with the strategic objectives of the antagonist. As previously mentioned, detecting such actions as intended and hostile is challenging and blurs the lines between war and peace. If international law is not officially recognized as violated, and the affected state does not recognize the events as intentional acts of hostility, could the situational or "operational environment" thus be considered one of war?

This specific situational understanding, of which social construct could be understood as an operational environment, is often defined as the *greyzone*. A generalization of the definition of greyzone by the Swedish armed forces research establishment (FOI) could be understood as such*: a condition between war and peace where states and non-government actors seek to influence a state's interests, freedom of manoeuvrability and capacities* (Veibäck et al., 2021, p. 18). Hence, the operational environment the greyzone represents is not to be characterized as war, nor warfare in the term's legal form. In situations where hybrid measures are deployed into an environment that fulfils the definition of the greyzone, such application of means should rather be defined as either hybrid operations or stand-alone domain operations deployed in the greyzone, not as warfare. This inherently mean that the term warfare is limited to conditions recognized as war.

3.3.4 Implausible deniability

As the previous conceptualization describes the application of covert action where plausible deniability holds, a conceptualization deems necessary for the situation where such deniability does not hold. Cormac and Aldrich (2018) define such as a state of *implausible deniability*. They argue that thinking of all covert actions as secret by intent is a mistake. Thus, a lack of secrecy does not necessarily constitute a failure of covert action (2018, p. 478). Implausible deniability itself, in addition to the other features of hybrid operations, "allows states to communicate resolve, while not escalating crises into open warfare" (Cormac & Aldrich, 2018, p. 488). This does not necessarily favour the hostile actor, but also the defending actor, as seen during the cold war, as "parties had a shared interest in maintaining the fiction of secrecy in order to avoid pressure to escalate" (ibid). Cormac and Aldrich define this situation as a "tacit collusion", the situation where both parties favour from the implausible nature of the actions, and such collusion allows risk management and off-ramps to de-escalate tense situations.

The situations of implausible deniability often lead the aggressive party to, contrary to orthodox consensuses on plausible deniability have it, choose non-acknowledgement than outright denial (Cormac and Aldrich, 2018, p. 489). This plays on the popular phrasing in covert action, where the involvement is neither confirmed nor denied. Cormac and Aldrich maintain that acknowledgement and denial exist at the end of a continuum, not as binary absolutes (ibid).

This implausible deniability is one of the main features leading to the evolvement of the operation, from operating within greyzone conditions, to an environment of *hybrid war*. By its name, hybrid war could be defined as an operational environment in which hostile acts are recognized as such, and cross the threshold from peace to war. In legal terms, this threshold is easily observed in treaties and conventions, such as Article 5 of the NATO treaty. While a nation observes hostile military action on its territory, such acts violate its inherent right to sovereignty, thus invoking the proclamation of war. Hybrid warfare, however, does not necessarily involve a straight-out proclamation of war from any of the involved parties.

3.3.5 Defining hybrid warfare.

I choose to define hybrid warfare as *a hybrid operation conducted in an operational environment – a state of nature, where the intensity or nature of the actions, which previously could be defined as in the greyzone, has evolved into a state where actions are detected and understood as hostile, and/or plausible deniability evolves to implausible, leading to an open conflict between to parties.* To describe a hybrid operation as *warfare* does not necessarily demand a declaration of war. A situation could be described as hybrid warfare if the actions previously defined as in the greyzone are illegal by law when recognized as intentional, and plausibility no longer holds, and it evolves past the threshold of conflict. This inherently means that it is not only the choice of methods or intensity which leads an operation to evolve from operating within the boundaries of the greyzone to hybrid war – it could simply be whether such actions are detected as an act of aggression. Cormac and Aldrich maintain that "hybrid warfare forms a timely example of implausible deniable operations creating exploitable ambiguity" (2018, p. 490).

The ambiguity allows the aggressive actors to project power and reach strategic objectives in a way that allows legal deniability but, at the same time, appears so implausible that there is little doubt about the origin of such actions. The latter enhances the aggressor's abilities of deterrence by hybrid means – whereas receiving states and their populations are being noticed by the abilities of the aggressor to deploy hybrid means to fulfil strategic objectives yet maintain plausibility to such a degree that the actions presented are yet to present consequences for the antagonist. To exemplify, Cormac and Aldrich maintain that recent actions (the annexation of Crimea and election interference in the US) prove Russia's ability "to generate a situation where it is unclear whether a state of war exists – and if it does, who is a combatant and who is not" (Cormac and Aldrich, 2018, p. 490). They further elaborate that *the exposure of operations, that although unacknowledged still pose such implausibility about its origin, effectively blurs the line between war and peace, and more specifically, between what is to be recognized as civil unrest, or that of external intervention* (ibid). Moreover, the lack of hard evidence of external aggression makes it difficult for supranational bodies, such as the UN or NATO, to intervene and place responsibility. Yet, even more effectively, the problem of attribution and enforcement of Article 5 of the NATO-treaty undermines the entire purpose of the organization (ibid), which could lead to a lack of confidence, internal unrest, or, ultimately – the disintegration of the organization in its present form. Undoubtedly, these

consequences could lead to serious strategic victories for Russia or any other actor favourable to such degradation or disintegration.

3.3.6 Multi- and full spectrum warfare

Multi-domain warfare is another operational environment worth mentioning for both cases to be discussed in the subsequent case study in part 4 to this thesis. Multi-domain warfare is often considered coordinated joint operations by land, sea, and air forces for military purposes (Fraioli, 2022). This is what we generally consider conventional warfare, as such military operations in contemporary warfare are most likely to be carried out in some kind of joint effort (US Army, 2022, p. 13). Whereas wars previously were fought as straight-out land-battles or sea-battles, most land and sea-operations of contemporary military operations are strictly dependent on some air support, either to provide close air support against surface targets or to secure friendly surface elements from hostile air threats (US Army, 2022, p. 20). Many consider the maintenance of air superiority as an indisputable necessity to risk putting "boots on the ground" – the involvement of land forces in the theatre. *While hybrid operations are deployed simultaneously as conventional military forces, or hybrid warfare escalates to include conventional elements to such a degree that it supersedes the way we traditionally see conventional elements as part of hybrid operations, we should rather consider the conflict as traditional warfare – thus as multi-domain.* The domains employed by the hybrid operation would, in such cases, complement the traditional domains of conventional warfare – land, sea, air, and, more recently, space and cyber. As far as the operational environment is considered a social construct – a result of not only our situational awareness and understanding of such but also our choice of how to recognize it, there is several ways to explain and conceptualize the various states between peace and war, and through various levels of intensity.

For simplistic purposes, this paper maintains that the only escalating level following multi-domain warfare is *full-spectrum warfare* – or in popular terms, "all-out war". This includes the use of strategic or tactical nuclear weapons, in addition to the domains of multi-domain warfare.

3.3 The instruments of hybrid operations

The means, efforts or instruments of hybrid operations refer to the variety of efforts included within the spectre of hybrid operations, discussed at length in the previous subchapters. Some of these are mentioned as examples in the above definitions of various terms within the concept. The multinational project "MCDC" do in their publication "Understanding Hybrid Warfare" include a variety of domains in which hybrid efforts might be deployed. The MDCD refers to this spectre as MPECI - Military, Political, Economic, Civil and Information (Cullen & Reichborn-Kjennerud, 2017, p. 9). Within these domains, various instruments might be employed to serve either kinetic- or non-kinetic objectives. For this thesis, I have reformulated the MPECI scale to form the most discussed and analyzed domains of operation, which I will discuss further.

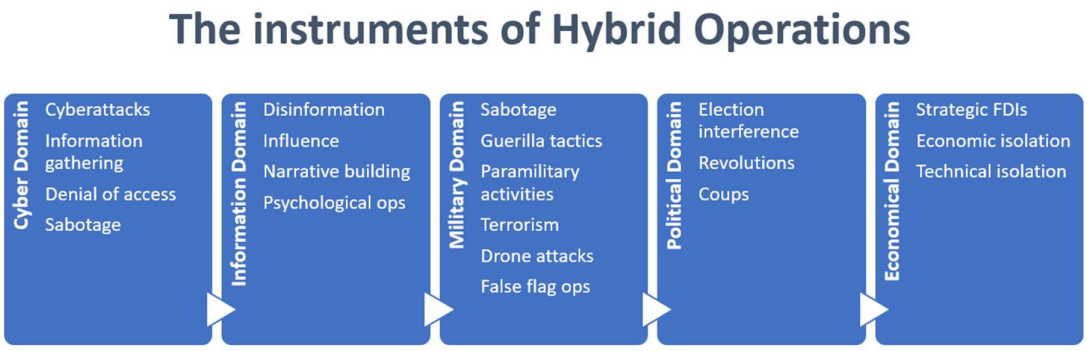


Figure 3.1: The Instruments of Hybrid Operations

The Cyber domain

The Cyber domain includes all forms of operations that seek to exploit software systems. Cyber operations could be of various technological origins and deployed in several architectural designs, such as DDoS, Malware, Phishing etc. The purpose and intent of these operations are, however, in most cases related to similar outcomes; disruption, denial, exploitation and gathering.

In 2007, a dispute between Estonian and Russian authorities regarding Soviet war memorials in Estonia escalated into a hybrid conflict. During the dispute, Estonia suffered numerous cyber-attacks, targeting most government websites, political parties, media organizations, and banks (Haataja, 2017, pp. 160-170). The attacks disrupted access to websites, services and communication channels, as well as slight interruptions to mobile networks and emergency

service lines (ibid). The scale of the attack led Estonian authorities to attribute the attack back to Russia, despite the lack of substantial evidence (Chen, 2010, p. 2).

Another well-known example of cyber operations is the US-Israeli Stuxnet attack. In 2012, a joint US-Israeli cyber operation, *Operation Olympic Games,* was carried out to reduce or halt the Iranian nuclear programme. Farwell and Rohozinski (2012) state that "the lesson is that cyber weapons may offer non-kinetic ways to disrupt an operational capability of an adversary" and that "it is significant that Iran has not suggested the use of Stuxnet constituted an act of war". The operation practically fulfilled US and Israeli strategic objectives of reducing the military capabilities of the emerging regional power, Iran.

Cyber operations are one of the most driving elements of the hybrid portfolio, much because the infrastructure and communication solutions in our modern societies are built upon software solutions. In contemporary societies, everything is powered by software-based infrastructure. One of the scenarios analyzed by the Norwegian Directorate for Civil Protection is a possible cyber operation that disrupts financial institutions and economic infrastructure. Such a scenario will be analyzed in more profound terms in the next chapter.

The military domain

Within the military domain, special operations, guerrilla warfare, sabotage and insurgency could be employed (US Army, 2008, pp. 3-4). Several contemporary conflicts involve the use of military elements for hybrid warfare. The Russian annexation of Crimea, using “little green men”, is one of the prime examples. However, the Hezbollah-Israeli conflict, which by many is characterized as hybrid by nature (Hoffman, 2007, p. 35; Kaunert & Wertman, 2020; Vaczi, 2016, p. 48), also involves elements of military characteristics, such as guerilla warfare and insurgency. One of the most theorized concepts of military contributions to hybrid operations, however, is the use of special operations forces. These are highly trained professional units, prone to covert action, and serve to fulfil a variety of tasks. However, physical sabotage and renditions, or small-scale kinetic operations, remain the primary tasks for SOF-elements in hybrid operations (Diesen, 2018, p. 14)

Drone operations have been introduced as a potential new tool in the military domain of hybrid operations. Drone technology has come a long way since its first introductions, and lessons learned from the current conflict in Ukraine show the great potential of small, civilian drones, modified to drop grenades and other small ordnance on enemy positions

(Benjaminsen, 2022). Drones may also efficiently be used to disrupt operations in critical infrastructure, such as airports (Steen, 2022), and did cause great media coverage after being observed over Swedish nuclear power-plants (Ringstrom, 2022), and Norwegian off-shore installations (Baisotti et al., 2022), and efficiently led to increased security measures to be made around such objects.

False flag operations are special intelligence activities conducted to deceive, confuse and enable narrative control. Concrete, false flag operations are carried out as activities under the cover of being conducted by another state, group or entity (Martin, 2023). False flag operations could either be conducted to diminish and reduce trust and confidence in governmental institutions, or as an enabling element, if followed by actions of aggressive behaviour. For the latter, the false flag activity would provide a pretext and an element of legitimacy for the following activities of the antagonist. For example, before the Russian full-scale invasion of Ukraine in February 2022, President Biden accused Russia of planning to carry out a false flag operation to create a pretext and an excuse for the subsequent invasion (Alba, 2022).

The political domain

The political domain could serve objectives of manipulation, influence, and suppression. Giannopoulos et al. (2021, p. 32) maintains that "the tools of this domain target democratic processes, political organizations, and persons". These efforts could be accomplished through election interference, colour revolutions and coups. The latter two concepts could be achieved by overt political support, economic subsidies to benevolent political groups, or direct involvement through special intelligence activities, such as paramilitary operations (US Army, 2008, p. 5; 2021a, p. 105). The orchestration of revolutions could be introduced as one of the least risk-related methods for regime change in foreign countries (Fridman et al., 2019, p. 33). Allegations have been made that the US was "involved in a coup" against the Russia-backed Ukrainian president, Viktor Yanukovych, in 2014 (RadioFreeEurope, 2015), and that Western countries had been "meddling" in Ukraine during the Maidan revolutions (Chiacu & Mohammed, 2014). The United States has, for instance, been known for carrying out various activities in Latin America, leading to political coups, and enhancing U.S influential control in the continent (Thyne, 2010, p. 449).

The economic domain

The economic domain is becoming increasingly vulnerable and sensitive, much because of the ever-increasing degree of economic integration and transnationality. These vulnerabilities

could be related to foreign direct investments, integration of foreign infrastructure, manipulations of energy markets, economic sanctions, or multi-domain civil incursions, such as cyber-attacks into banking markets or financial infrastructure, of which the general public is denied access to financial assets over a shorter or longer timeframe (DSB, 2019, p. 200; Giannopoulos et al., 2021, p. 29).

The information domain

Some of the most applied tools of hybrid means are within the spectre of what some existing literature would name "information warfare" (Farwell, 2020; Waltz, 1998). These operations include influence operations, propaganda and disinformation (Fridman et al., 2019, p. 1; Giannopoulos et al., 2021, p. 32). The general concepts within such campaigns are manipulation, deception and demoralization (Hutchinson, 2006, p. 217). Whereas influence operations are covert by nature, propaganda is more overt and serves as an alternate information option by a known actor. Disinformation shares some of the same attributes of propaganda but is more covert and seeks to cause confusion around the objectively observable truth (Bergh, 2020, pp. 7-8).

FFI defines influence operations as an agent's coordinated attempt to influence meanings and situational awareness with people and groups outside their judicial control without these being aware of the agent's involvement (Bergh, 2020, p. 7). The last few decades have introduced a new digital dimension with social media platforms (hereafter SMPs) such as Facebook, Twitter, Instagram and TikTok. The most crucial attribute found in SMPs is that all content is in a universal format. Therefore, any content, either from a friend, or a malicious influence operation, will appear universally equal to the end-user (Bergh, 2020, p. 10), and thus make it difficult to differentiate between friendly and malicious content. Another problem with SMPs is related to the algorithms that decide what content to be distributed to the end user. The algorithms are machine-learned processes intended to produce what the end-user is most likely to be interested in watching based on their previous behaviour, user data which is stored in the application. These algorithms, however, may be altered by being "fed" large packages of content. Agents pursuing influence operations will thus be able to alter the initial automatic algorithms and distribute their malicious content to end-users (Bergh, 2020, p. 17). TikTok has become one of the most used SMPs over the last couple of years, and the increasing risk of users utilizing the application as their primary resource for information gathering, combined with the close ties between Chinese companies and Chinese authorities, has

introduced a risk of manipulation through controlled and manipulated algorithms showing benevolent content, and hiding unwanted content by the Chinese state (Slotten, 2022).

Disinformation and misinformation are other modes of operation within the information domain. These terms are often used synonymously but must be understood as separate concepts. FOI defines misinformation as "information initially processed as valid but that is subsequently retracted or corrected" (Svenonius, 2022, p. 15). Disinformation, on the other hand, is defined as the intended distribution of "false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit" (European Commission et al., 2018, p. 3; Svenonius, 2022, p. 15).

Although misinformation not necessarily could be attributed as intentional, the *continued influence effect* may, in some cases, produce a so-called "belief perseverance effect", which means that the perceived misinformation will continue to have an effect, even after it is definitively corrected (Svenonius, 2022, p. 15-16). Further research also shows that retractions and corrections rarely have the effect of eliminating reliance on the misinformation and that it is "difficult to readjust the beliefs of people previously exposed to the misinformation".

It is essential to differentiate between the various modes of information operations. For example, influence operations could be directed at narrative-shifting in favour of the agent (Bergh, 2020, p. 8), but it does not necessarily involve disinformation or misinformation, albeit merely presenting a one-sided perspective of a case. However, disinformation is often "planted" within content distributed through influence operations in SMPs, as it will enhance the narrative while end-users that believe and incorporate the information share and distribute this content out of their own will (ibid).

3.4 How to measure hybrid efforts?

Having clarified the modes of operations, its instruments and the operational environments, the current section needs to clarify how hybrid efforts are to be observed. In the previous subchapters, meaningful distinctions have been made to distinguish hybrid operations from adjacent phenomena, such as single-domain irregular operations or traditional unconventional warfare. What remains is to argue ways of measuring the strength and intensity of hybrid measures applied in foreign policy strategies.

3.4.1 Intensity

In conventional military combat, the intensity of the military efforts is generally determined through the number of troops involved in direct combat, casualties, number of air sorties or artillery strikes or similar. Because hybrid operations are different from traditional warfare, new ways of determining the intensity of the efforts must be established. There could be several ways of determining such intensity, but the illustration below will provide an option for interpreting and understanding the intensity of such operations.

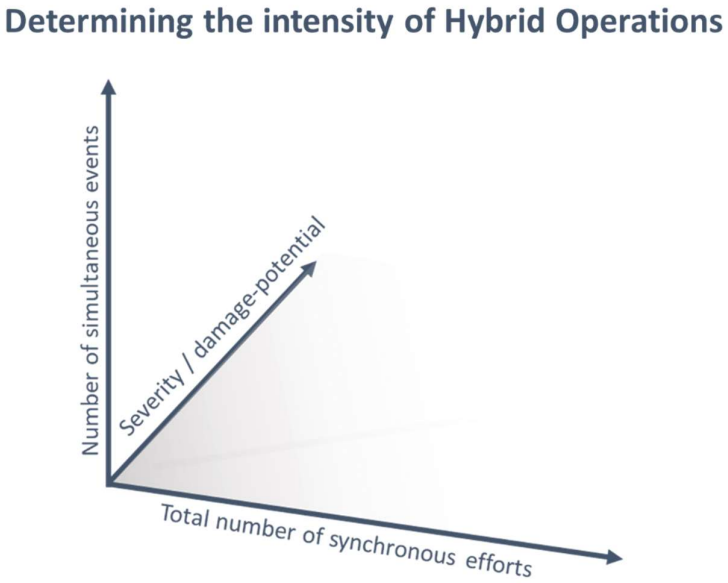


Figure 3.2: Measuring Intensity of Hybrid Operations

The figure above illustrates the intensity of operations through three axes: The number of simultaneous events, damage potential, and the total number of synchronous efforts. These categories define three different methods of interpreting intensity. First, the number of simultaneous events determines how many events occur at any given moment. The synchronous element of hybrid operation does not necessarily demand an overlap of all events

in time and space so long as these events can be linked to the same operation within a limited time and geographical span. Thus, the intensity throughout an operation could vary and be determined by the number of efforts in action at any given time. The second category of intensity is related to the severity of the measures taken at any given time. For example, actions related to sabotage of critical infrastructure may lead to civilian casualties and could, as such, be interpreted as more intensive than influence- or disinformation campaigns. Other events that could be amplifying for intensity are, for instance, special operations targeting essential personnel for the maintenance of state stability (such as military leaders or politicians) or special intelligence activities, such as false-flag operations or orchestrated demonstrations.

The last category describes the grand total of efforts laid forward in the operation. This number varies from the first category because rather than identifying simultaneous efforts, it seeks to provide a number of total events taking place during the operation in its entirety. This way of measuring intensity will most likely be more valuable when conducting comparative analyses of several operations and campaigns.

3.4.2 Timespan and types

In addition to intensity, we can apply additional variables to provide an overall awareness of each operation for comparative purposes. As described above, the intensity variable should most likely make its primary efforts to explain the totality of the operation. Severity and damage and a curve diagram of variations of simultaneous efforts could also be of high value when comparing operations. In addition to intensity, I see it fit to compare the following two variables: Timespan and Type. The timespan is as simple as it seems: the operation's endurance. However, it is vital to be aware that an operation could have an unclear start and end. An operation leading into open conflict could, for instance, “start” before the open conflict reveal itself because known or unknown (depending on intensity and covertness) enabling efforts could occur before the main efforts. It is also likely that measures of hybridity could endure after the end of an open conflict for strategies of legitimacy and damage control.

The last variable to efficiently be able to measure hybrid operations comparatively is type. The type of operation could be interpreted in several ways. The type could be related to the highest strategic achievement of the operation, for instance, regime change or policy change, or whether it was a stand-alone hybrid operation (not as an integrated part of a traditional

campaign) or if it served as enabling and/or supportive to a traditional campaign. In addition, we can distinguish between hybrid operations as greyzone operations or hybrid warfare in open conflicts. More about the distinction between operational environments is to be found in the chapter on layers of hybrid operations and the initial framework for understanding this phenomenon. Lastly, I believe it could be valuable to differentiate between operations based on what measure or instrument that was most prominent during the operation.

3.5 The asymmetry of hybrid operations and its implication on the security dilemma

Like conventional operations often prove disproportional or asymmetric, hybrid operations feature similar disproportionalities in their nature of operation, which needs to be discussed. As with conventional warfare, hybrid operations lean on two premises for competitiveness – capabilities and vulnerabilities. From a military perspective, capabilities might be exemplified by strategic bombers, long-range rocket artillery, or similar attributes to combat power. Vulnerabilities, on the other hand, could be related to the territorial defence of uneasily defendable terrain or technical vulnerabilities with military hardware, such as easily destroyable tank turrets.

3.5.1 Strategic advantages and asymmetric vulnerabilities.

Hybrid operations base themselves around the same axes; capabilities and vulnerabilities. Whereas economic theory introduces competitive advantages between economies, the security politics of hybrid operations might offer similar ideas to differentiate between the potential for capability-building amongst states. An optimal strategy of hybrid nature is more specifically centred around what I will name *strategic advantages* and *asymmetric vulnerabilities*. Strategic advantages represent the capability-based spectre of the operations. Strategic advantages are most effective while such attributes are considered what economic theory names a competitive advantage – a set of attributes that make the production of certain products cheaper or more available compared to the counterpart (Holden, 2016, p. 373). This analogy is also used by Schneider (2019, pp. 847-848) while describing how the invention of a capability will introduce a vulnerability (or a competitive disadvantage) for those with insufficiencies related to the development of such capabilities. Competitive advantages within the hybrid doctrine could be the sole development of specific tactics or capabilities or the possession of comparatively larger capacity or highly skilled personnel to carry out such tactics. Highly digitalized countries would, for instance, have a greater potential to produce capabilities within the cyber domain, since human capital is predisposed within that field.

Asymmetric vulnerabilities, on the other hand, represent points of vulnerability that are exclusive to the enemy. Such vulnerabilities are only relevant if these could be exploited by the capabilities of the aggressor. Examples of asymmetric vulnerabilities could be heterogenic societies resilient to internal polarizations or the lack of adequate cyber security capacities.

3.5.2 Responses to hybrid threats

There is scant literature or doctrine establishing a proper way to respond to hybrid threats, apart from public attribution. Although NATO decided to include hybrid threats to Article 5 of the Atlantic Treaty (NATO, 2023), it is highly unlikely that hybrid attacks in unconventional domains would lead to a response by conventional military measures. A likely assumption would be that hybrid operations would be countered by symmetric means, which allows us to analyze how risk is involved in capability-building. It could be argued that operations within the frames of the greyzone complicate decision-making and raise the bar for escalatory retributions beyond the threshold of conventional inter-state conflict. In other words, it is unlikely for states exposed to hybrid operations to produce conventional kinetic counterstrikes by military means. This assumption is drawn from two premises; inattributionality and plausible deniability complicate the legitimatization of hard power retributions, and the disproportionality of countering non-kinetic operations (such as disinformation campaigns) with military kinetic operations, such as air strikes or artillery.

3.5.3 The security dilemma and hybrid operations.

The security dilemma problematizes how misperception and fear lead to escalation and securitization, which leads the adversary to escalate correspondingly, leading to an arms race in which none of the parties experiences increased security (Baker, 2019, pp. 1251-1252; Jervis et al., 2003, pp. 316-317).

The security dilemma is as relevant to hybrid operations as to any capability of coercive power. However, as established early in this thesis, hybrid operations heavily rely on capabilities and effects that are pursued covertly and under various degrees of plausible deniability, some to the extent that there will be challenging to differentiate between intended and unintended action. This axiom of hybrid operations makes it the wild card of coercive measures, as its capabilities or the extent of such is difficult to observe by the other states in the system. This could lead to two outcomes; states will not pursue strategies of capability-building of hybrid means because the existence of such capability with their adversaries is unclear – or states will pursue capability-building precisely because of the uncertainty, as the initial proposition assumes. However, the unobservable nature of these capabilities will make it difficult for any to present academic results as to whether the security dilemma holds for hybrid capabilities as it does for conventional ones. Moreover, even when utilized, there will still exist an uncertainty as to the variety of the state's capabilities and the size and utility level of such.

3.5.4 Diminishing returns on hybrid measures and the security paradox

There is a limit on how much resources might be put into action before the outcome of operations would see diminishing utility. The logic is simple: As seen in the section on the instruments of hybrid operations, we can observe that both the cyber domain and the information domain are driven forward by resource-efficient strategies that employ automatization and digital aids. After developing a substantial capability base, there will be a saturation of resources, and the following effect will be what economists would describe as diminishing returns on utility.

An attribute possibly leading to a diminishing effect of the arms-race-like phenomenon of the security dilemma is what academics within the cyber domain field name "the security paradox". The security paradox's outcome is fairly similar to the security dilemma – an escalation and development of capabilities would efficiently lead nowhere. Schneider (2019) addresses this paradox. As a state gain increased digitalized technological capabilities, the level of vulnerability will increase accordingly. Schneider cites Richard Danzig:

> Digital technologies . . . are a security paradox: even as they grant unprecedented powers, they also make users less secure . . . their concentration of data and manipulative power vastly improves the efficiency and scale of operations, but this concentration in turn exponentially increases the amount that can be stolen or subverted by a successful attack (Schneider, 2019, p. 855).

However, coming back to the initial logical assumption presented in this subchapter on strategic advantages and vulnerabilities, this theory of the security paradox must be adapted for hybrid operations. The security paradox, as presented by Schneider, does exemplify the concept with the digitalization of Syrian air defence systems (2019, p. 855). These systems were supposed to deliver increased efficiency but were eventually "brought to its knees" before an Israeli attack by Israeli offensive cyber capacities. However, the capability-vulnerability framework must be altered to resample the perception of hybrid threats. As discussed previously, hybrid threats are most often directed at civilian infrastructure, both digital platforms and physical objects, as well as the cognitive aspect related to information operations. By such logic, the development of offensive cyber capabilities would not necessarily introduce an increased vulnerability, as this capability is covert, and not usually the target of hostile cyber activities. However, the initial logic of asymmetric foundations for capability-building amongst states would imply that highly digitalized states would experience lower costs in developing such offensive cyber capacity because of their existing human capital within the field. However, by utilizing such capability, the state would

inherently be severely vulnerable if experiencing symmetric responses because of its high degree of digitalization in their civil society, which likely would be the target of retributions.

By applying the same logic from the opposite point, states with a low degree of digitalization would see increased costs of developing offensive cyber capabilities because they would likely be forced to import such knowledge from abroad, which could be seen as an initial vulnerability (Schneider, 2019, pp. 847-848). However, although development costs would be relatively higher, the scenario of symmetric retribution would result in a significantly lower vulnerability than that of the digitalized society. Examples of this are Iran and North Korea, which by the UK National Cyber Security Centre is named as two of the most prominent threat actors, in addition to Russia and China (NCSC, 2022).

The logic may also be brought into the information domain. Some states possess inherent advantages for their lack of development in the civilian sector. Countries such as Iran and Russia are seeing advantages within the information domain after banning the most popular social media platforms. Amongst the countries having blocked Facebook and Twitter, we find Iran, China and North Korea (Barry, 2022). Conversely, Russia is heavily influenced by Russian-developed platforms, such as VKontakte and Telegram (Statista, 2023). By keeping internal control of social media platforms (SMP), these states are less exposed to influence operations than those keeping more commercial and open platforms, as the accessibility to produce information campaigns would be severely limited. To lead this back to the initial logic or mechanism, we can say that these countries possess a strategic advantage, while the countries allowing commercial SMPs would possess an asymmetric vulnerability relative to the former.

3.5.5 Asymmetric hybrid warfare in the literature

Does this logic have support in theory? Bresinsky argues hybrid operations are naturally asymmetric (Bresinsky, 2016, p. 30). Asymmetric warfare is defined in various manners. Wolff Von Heinegg et al. (2011) argues that former definitions are outdated and must be seen in relation to contemporary conflicts. The initial definition of asymmetric warfare is "a conflict involving two states with unequal overall military and economic resources" (Von Heinegg et al., 2011, p. 464). Von Heinegg, however, argues that a more relevant definition would be such; "leveraging inferior tactical or operational strength against [the] vulnerabilities of a superior opponent to achieve disproportionate effect with the aim of undermining [the opponent's] will in order to achieve the asymmetric actor's strategic objectives" (ibid). The latter does to a larger degree grasp the effect we are looking for,

although the definition is concentrated around weak-agent tactics, and as such would be more relatable to irregular- rather than asymmetric warfare. However, there is no doubt that the element of uneven capabilities and vulnerabilities prove hybrid operations to be asymmetric, an argument also supported by Von Heinegg (ibid).

3.6 Established concepts applied to hybrid operations: Anti-Access Area Denial.

Anti-access area denial has become one of the most popular concepts of conventional military theory. The term most often conceptualizes actors' ability to close off geographical areas or domains and deny an adversary the ability to operate within that area. The most applied example is the use of anti-air assets to hinder freedom of navigation for air, maritime, and land assets, which all depend on air support to maintain freedom of movement. These are so-called A2/AD (Anti-access area denial) bubbles.

The emergence of new-generation warfare concepts and the increasing presence of hybrid means calls for an analysis of the possibility of converting the conventional concept into an adaptation of A2/AD operations carried out by hybrid assets.

Russel (2015, p. 155) understands the phenomena as follows:

> The modern understanding of anti-access and area denial operations (or A2/AD operations[..]) means explicitly to deny an adversary the ability to bring its operational capabilities into the contested region or to prevent the attacker from operating freely within the area and maximizing its capabilities.

Whereas A2/AD usually is related to the diminishing of access and freedom of movement geographically within an AO, the evolvement of technology and tactics demands a wider understanding of the concept to include the spheres and domains by which we consider hybrid or unconventional in addition to the classic conventional understanding of the phenomenon. One example of such is a generally acknowledged concept within cyber-theory; *Denial of services* (*DoS*), presented by "*an attack that inhibits a computer resource from communicating on a network, preventing it from being available to fulfil its purpose either temporarily or permanently*" (US Army Cyber Command, 2022). DoS, in its nature, comply with the understanding of the military Area Denial concept, as it prevents an agent from utilizing an area or a domain. In the information age, such operations are also widely used in

conventional warfare, as the cyber-domain has been an ever-increasing part of modern capability building. Military doctrine often refers to *C4ISR* (Command, Control, Computers, Intelligence, Surveillance and Reconnaissance) (US Army, 2010), a concept integrated into all modern combat operations. Whereas command and control (*C2*) is a concept that dates far back and is understood as the "direction by a properly designated commander over assigned and attached forces" (US Army, 2021a, p. 19), C4ISR is the developed concept in which information and communication systems, as well as digitally enabled platforms such as intelligence, reconnaissance and surveillance, is included. During the 2014 Russian hybrid campaign in Ukraine, Russian forces utilized cyberspace- and electromagnetic warfare to deny the Ukrainians access to C4ISR nodes critical to Ukrainian missions. Such operations at the tactical level were considered lethal (US Army, 2021b, p. 12).

Such operations are generally considered an integrated part of modern warfare. Yet, the same concepts could easily be derived as integrated parts of hybrid campaigns and may simplify our understanding of the existing use of hybrid means.

Hybrid forms of A2/AD may heavily rely on cyber-enabled operations but may not be considered cyber-operations by nature. To simplify, I will provide some examples of how I understand such operations may be carried out.

3.6.1 Scenario of hybrid A2/AD: Svalbard

The Svalbard peninsula is situated in the high north and is vulnerable to "satellite shadow" due to its high latitude and difficulty in receiving signals from commercial satellites in terrestrial orbit (Sysselmesteren på Svalbard, 2022, p. 21). The mitigation for this is two fibre cables from the Norwegian mainland, providing the peninsula with critical communication. These cables also provide the peninsula's citizens with internet and communications connectivity for private and commercial purposes (such as broadband, television and cellphone coverage).

The severely limited communication solutions call for significant vulnerabilities, which an aggressor in a potential conflict may exploit. Sabotaging both cables in a synchronized operation, including electromagnetic operations targeting the few remaining alternatives (commercial communication satellites, Iridium/Starlink, in polar orbit), would leave society wholly separated from the rest of the world. Such a situation would allow the aggressor to install solutions providing sovereignty in the information domain and denying the Norwegian authorities access to the geographically confined area. A scenario, as described, would also

allow for additional means of hybrid operations, such as information campaigns, either disinformation or influence operations, to manipulate and shape the situational awareness of the local population. This effort could be enabled to facilitate temporary or permanent territorial control for the aggressor. Synchronized employment of conventional efforts, such as small units of special forces or marine commandos and anti-air missiles, would further deny Norwegian authorities' physical access and, by such, fulfil all the preconditions laid forward by the military definition of anti-access area denial. The above-described scenario is not unlikely to be a highly significant problematization regarding the security of Svalbard from relevant adversaries, such as Russia or China, which both are considered to have shown increased interest in the Arctic (Etterretningstjenesten, 2021, p. 8)

3.6.2 Scenario of hybrid A2/AD: Financial institutions

Another hybrid A2/AD scenario is the potential attack against financial institutions. In Western societies, and more significantly in the highly digitalized ones, transactions have developed from being made by cash to instead being made by electronic solutions, such as with credit cards or mobile solutions (Vipps, Apple Pay etc.). In these societies, the populations are known to have a high tolerance for carrying cash and are thus highly dependent on digital solutions to fulfil their daily needs. In Norway, cash-based payments have dropped to a historic low over the last three years and have stabilized around 3-4% of all transactions. Even between citizens themselves, cash only counts for approximately 5% of all payments (Norges Bank, 2022, p. 26). The cash holdings in circulation in Norway are correspondingly historically low, at 37,3 billion NOK by the end of 2020, which accounts for merely 1,3% of the Norwegian GDP in 2020 (Norges Bank, 2021, p. 16).

A synchronized cyber-attack on the national transaction system "BankAxept", in combination with targeted cyber-attacks against payment terminals (which in Norway are usually limited to a handful of companies), would not only prevent payments made by national debit cards, but it would also deny payment by international cards, such as Visa, Mastercard and American Express, not only to include direct payments but also credit and contingency solutions. It would also deny customers the ability to withdraw money from services demanding digital authorization by card, phone, or NFC, such as ATMs and stores. This effectively denies customers from making payments in their everyday lives, in all spheres of life, in grocery stores, gas stations and drug stores. It would also prevent customers from applying digital transaction apps (such as Vipps) enabled by BankAxept solutions.

Such a scenario is briefly introduced and analyzed in the Norwegian Directorate for Civil Protection (DSB)'s report of crisis scenarios from 2019. In the scenario, the consequences are described as detrimental. In addition to causing logistical problems, the societal and psychological burden on the citizens would be severe. It would lead to a feeling of "a violation of individual rights and personal security" (DSB, 2019, p. 202). Furthermore, it assesses the societal consequences as very large, as it would lead to a high degree of unpredictability, fear, frustration, and lack of confidence in the general population. The report further considers the impact of the loss of democratic values and national control to be medium-large. Still, the scenario drawn in the DSB report is considerably more limited than this paper's.

Compared to the former, the scenario allows the aggressor a form of denial and anti-access to the financial domain. Further efforts that could be synchronized in addition to the scenario-enabling attacks could be information campaigns directed at further reducing the trust and confidence in the government and their institutions, possibly favouring competing actors and agents, such as the aggressor himself.

3.7 Established concepts applied to hybrid operations: Deterrence

Deterrence is, as defined by NATO, "the convincing of a potential aggressor that the consequences of coercion or armed conflict would outweigh the potential gains" (UK Ministry of Defence, 2019, p. 3). Generally, and less sophistically, deterrence is understood as a show of force to project power and capability in such a way that the adversary considers the risks and costs of aggression too high, preventing any conflict in the first place.

The literature on hybrid deterrence is currently overwhelmingly dominated by conceptualizations of defensive nature established to facilitate deterrence strategies towards the malicious use of hybrid means. This understanding aligns with the set deterrence theory and protects and defends territorial sovereignty by imposing additional costs and risks to the aggressor. However, there is an imminent need for a broader understanding of the combination of deterrence and hybrid means.

Strategic deterrence, or signaling, is often used to describe the phenomenon of nuclear weapons strategies and the act of preventing hostile use of such. Russian strategic deterrence in the European AO is often related to using long-range strategic bomber aircraft capable of carrying nuclear warheads. As with US strategic deterrence concepts, these are supplemented by submarine-based and land-based intercontinental nuclear ballistic missiles (Quinlivan & Oliker, 2011) which, when complemented, form what is popularly known as "the nuclear triad". Whereas ballistic submarines are often considered a more serious covert option, offering lower operational risk of detection thus higher potential strategic options, strategic bombers are a more visual asset, which is prominent for operations seeking to coerce the enemy. Russian strategic bombers are known as a regular sighting in the areas commonly known as "the bastion", a defensive concept of Russian strategy dating back to the Soviet Union and the cold war (Kvam, 2021, p. 1). The area in question is located in the Barents Sea, including the areas around the Svalbard peninsula. The Bastion defence, however, includes the outer areas, including the Norwegian basin and the immediate surroundings of Iceland,

Figure 3.3: The Bastion Defence (Kvam, 2021)

commonly known as the “GIUK” gap. The variance in activity and patterns for these strategic sorties are often subject to thorough analysis in the West and are often considered one of the indicators for Russian foreign policy behaviour. Coercive-wise, the deficiency in the effectiveness of this strategy is that the presence, absence and increase or decrease of such activities are related to a high level of readiness and escalation. Nevertheless, the concept is one of the fundamental frames for Norwegian defence doctrine (Kvam, 2021, p. 1). This effectively means that the use of strategic deterrence for coercive means in such cases can seem excessive for the situation and could increase the risk of an escalation out of control, potentially to be followed by unwanted secondary effects.

In such cases, strategic deterrence may be complemented by hybrid efforts to provide the necessary deterring effect as previously, yet avoid escalating situations out of control if conditions otherwise have left the situation on a high alert. Stig Tore Aannø presents a problematization around the use of the cyber domain for strategic deterrence (Aannø, 2018). Such an adaptation of “non-military” measures for strategic deterrence is also made by Ven Bruusgaard (2016). She emphasizes the lack of sufficient research on the topic. She states that “There is little detail in the theoretical writings on how non-military deterrence should work, beyond stating that the use of these tools will depend on the status of the aggressor state in the international system” (Ven Bruusgaard, 2016, p. 15). Bruusgaard further elaborates that “offensive cyber capabilities could be used to inflict what would be perceived as unacceptable damage on a developed, high-technology Western society, in the economic or political realm” (ibid). There is no doubt that the possibility of hybrid efforts as a substitute for traditional deterrence strategies might be fruitful for further analysis.

3.8 Hybrid capabilities as means to enhance the scope of political manoeuvrability and exogenous enhancing and limiting factors.

An initial reference back to the foreign policy analysis framework is due to be done in this inductive section. To sufficiently understand the political utility of hybrid measures, we must examine the previously discussed dimensions in the context of the variables that influence the scope of political manoeuvrability. This chapter is partly introduced from a prestudy for this thesis (Danielsen, 2022, pp. 12-13).

As seen in the previous subchapters, hybrid measures offer a capability with benefits of covertness, deniability, risk-reduction and cost efficiency. How may these attributes translate into pure utility for the scope of political manoeuvring? Fermann defines the political scope of manoeuvre (SPM) as the set of options politically possible and operationally available, given the limitations of external factors and domestic influences (Fermann, 2013, p. 53).

By this definition from Fermann, we see that SPM consist of four factors: Decision-makers' politics, operational capacities, and external and internal influences. These are the core factors influencing the decision-makers' leeway in politics and policymaking. The importance of SPM, or rather the perception of it made by decision-makers, is made clear, as Fermann defines foreign policy itself as "foreign policy as the state's projection of self-interest on the global arena, within the scope for political manoeuvring perceived to exist and constructed through creative political action"(Fermann, 2022, p. 94). Looking at the international system from a Realist, or rather a Hobbesian perspective, it is evident that it is somewhat anarchic. This anarchy of world politics also emphasises that the SPM is subject to different perceptions and interpretations and, in many cases, is subjective by nature (Fermann, 2013, p. 109). Misperceptions and inaccurate perceptions of capabilities with adversaries could further restrain or increase the sense of SPM. Plausible deniability further complicates this problem while hybrid efforts are observed, but no apparent originator can be established. Decision makers' misconceptions is a fundamental problem in politics (Levy, J. in Jervis et al., 2003, pp. 260-262).

Hybrid operations enhance and limit the scope of manoeuvring in different ways. The first factor influenced by the emergence of modern hybrid measures is the factor of operationally available options. The ability to project power through one or several hybrid measures enhances the operational capacity of the state and could offer decision-makers the option to

take action in cases where other foreign policy instruments are insufficient, too aggressive, or operationally unavailable in the given situation (Diesen, 2018, p. 9).

Moreover, as the restricting factors for the SPM are traits of the international system and the domestic society, the major advantage of hybrid operations is the covert nature which calls for plausible deniability. The choice of hybrid measures reduces the risk of retaliation and loss of political capital, simply because of the unclear origin of the attack. The perceived scope of political manoeuvre varies from decision-maker to decision-maker because many restricting factors are based on political capital and the varying willingness to accept risk. In cases where diplomatic options are considered insufficient and tougher instruments of power projection are deemed necessary, the level of conflict and tensions in most cases tend to be high. In many cases, public opinions and framing of the conflict would shape the frames in which the decision-makers seek their leeway to choose their preferred options of action (Fermann, 2022, p. 104). Strong public opinions might lead "weak" or risk-aversive decision-makers to select options that "sacrifice" strategic effectiveness to pacify a highly attentive domestic audience (Breuning, 2007, p. 124).

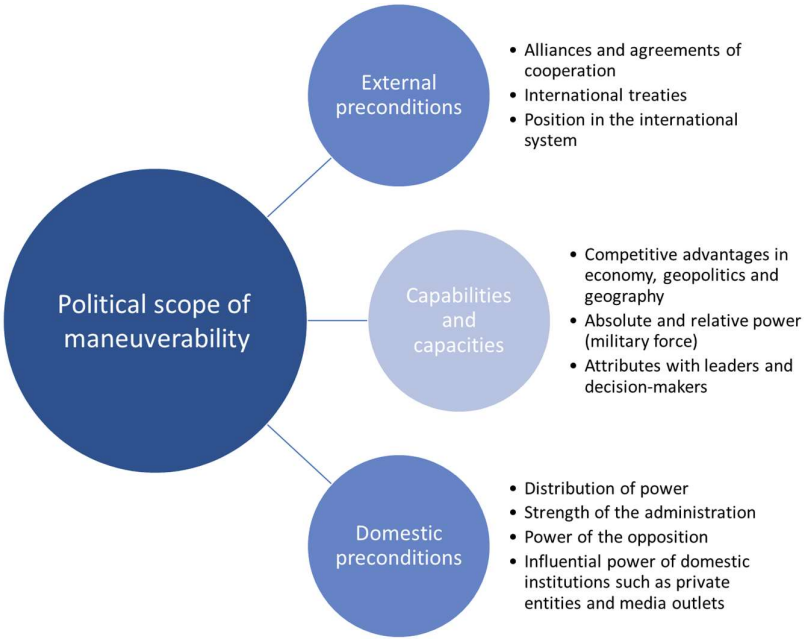


Figure 3.4: The influencing factors for the Scope of Political Maneuvering

The scope of political manoeuvring is influenced by several factors, as seen in Fermann's (2020) model of foreign politics. Essentially there are three factors determining the scope of manoeuvrability. The main factor is national capabilities and capacities. What must the state bring to the table to be credible in its actions while bargaining with other states? These are in

fundamental theories of foreign policy and international relations often considered to be means of power. In realist theory, relative power is the main factor for how states are allowed to interact in the system of states. Yet, in the contemporary system of highly integrated states and international institutions, also economic aspects affect the leeway decision-makers have in inter-state interactions. These could be related to competitive advantages such as cheap labour, production factors (such as availability of land and raw materials), it could be access to natural resources such as petroleum and gas, or it could simply be economic wealth, which effectively could be materialized into foreign loans or foreign direct investments. These capabilities and capacities allow the decision-makers to maintain a position of power towards the adversary in a bargaining situation.

After the capabilities and capacities are determined, there are two enhancing or restricting factors; external and internal influences. External influences are related to the system in which the state is situated, internationally and regionally. These could be limiting factors such as international conventions on limitations in use of force, or partnerships and alliances, which may restrict each member's sovereignty and power in exchange for universally distributed rules and regulations. Although unions and alliances may restrict each state's scope of manoeuvrability, these institutions may, however, increase each member's leeway while interacting with third parties, as the institutions themselves may offer enhanced capabilities beyond what is covered by the state in question. An example would be the power balance between a state organized in a military coalition and states without such cooperation agreements. The potential relative power would be incremental for the alliance member compared to their relative power assembly as an individual state.

Lastly, internal factors may deem restricting or enhancing to the scope of manoeuvrability. These are mainly centralized around one central issue; the administration's ability to utilize assets of national power. This issue is further divided into two main spheres; the sphere of power distribution between the administration or cabinet and the parliament on one hand, and the sphere of democratic restraints on the authorities, namely the nation's ability to hold decision-makers accountable for their actions. Capabilities and capacities are irrelevant if the decision-makers cannot utilize them to balance the power in bargaining situations with other states (Christensen (1997) as cited in Rose, 1998, p. 163). If the administration is dependent on parliamentary approval and suffers from weak control of the parliament, this could be an immensely limiting determinant for the SPM. This problem is mainly relevant to multi-party systems but could also be related to bureaucratically inefficient states, such as states requiring

majority votations in several parts of parliament. Likewise, if the strategies of foreign politics are in opposition to the general opinion of the people, the risk of loss of political capital could itself be a restraining factor for which actions are deemed available to the decision-maker. The latter is, of course, related to the degree of democratization in the respective state.

Hybrid measures could be considered yet a coercive asset in the toolbox of coercive means. The capability provides the state with enhanced capacities while bargaining with other states. However, adding hybrid measures to the toolbox offers more than an addition of conventional means would have done relatively. As established in the current chapter, hybrid operations are highly related to covert operations and plausible deniability, allowing the decision-maker to project power towards adversaries yet reducing risk from both internal and external audiences. In short, hybrid efforts provide increased utility for foreign policy strategies. As will be reviewed in the deductive part of this thesis, such efforts, with low costs, both politically and economically, as well as low risk, could be the decisive element to shift an offensive or defensively aggressive strategy from previously considered non-profitable to profitable. This could be a pivotal change in how states assess their SPM and thus behave towards their surroundings, as will be further discussed in the coming part.

4: Towards a reasoned conception of hybrid operations: Types and relations to adjacent phenomena.

In this subchapter, I will seek to summarize the former inductively analysed information and provide a clearer framework of how hybrid operations may be understood. The visualization and figural aids below are intended to provide a deeper and more meaningful interpretation of what hybrid operations are, how we may define them by their modes, and for what operational contexts they may be used.

4.1 Typology of hybrid operations.

First, I will present a taxonomy of hybrid operations. The figure below illustrates how we may translate the previously consumed information into a meaningful taxonomy of definitions and terms, set in its correct hierarchical place in the modes of hybrid operations.

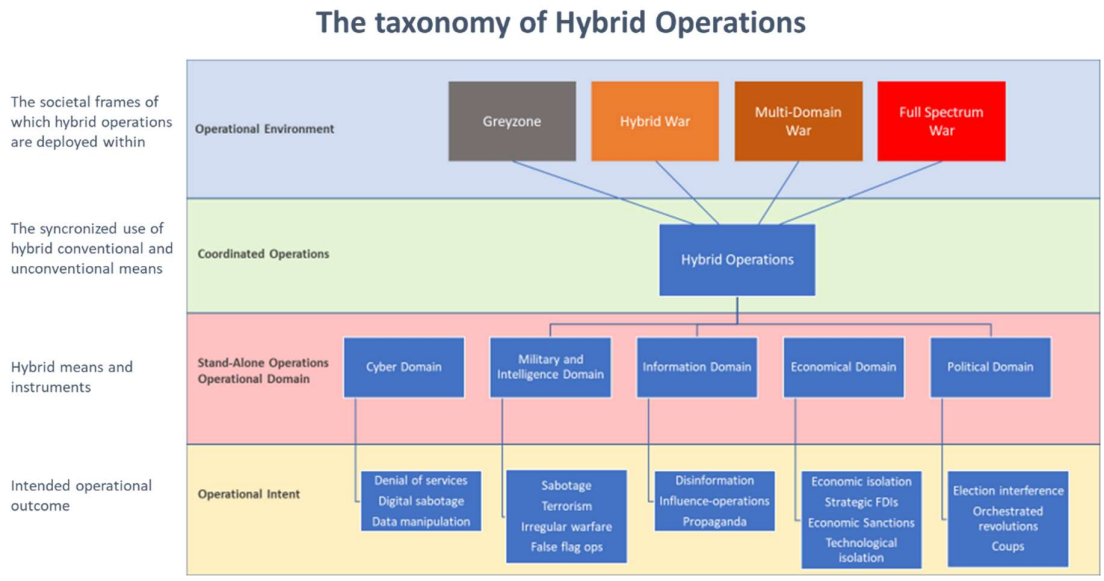


Figure 4.1: The Taxonomy of Hybrid Operations

The figure shows the four levels of understanding in hybrid operations; the outcomes, the domains, the coordinative effort, and the operational environments into which such operation may be deployed. The first level is *operational intent,* previously described as the direction of outcome or intent for the specific action. The second level is the domains in which these preferred outcomes of action are intended to be deployed. Sabotage, for instance, may be found in both the Cyber and Military domain but could also be argued to be an outcome of actions taken in the Economic or Political domain as well. The third level is coordinative efforts. By revisiting the fundamental definitions of hybrid operations, we find that hybrid

operations in its core are based upon the synchronous use of several of these actions or domains, either consecutive or simultaneous in time. If actions are carried out as singular events, it is not to be defined as hybrid, but rather by the domain in which it is deployed. We may still perceive these means as hybrid instruments, but the hybrid element is not represented unless synchroneity is observed.

The fourth and last level of this analysis is the operational environment. The operational environment is, as formerly envisioned, the set of conditions under which operations are conducted and could be easier illustrated as the situational awareness the actors involved inherit.

4.1.1 The fluid boundaries between diplomatic conflict, grayscale conflicts and hybrid warfare

When discussing the operational environments and reading previously conducted research and analysis on the topic, there is no clear distinction as to when operations are in the greyzone or when it is designated as "war" or "warfare". Therefore, to simplify the definitions and interpretations, I will provide the following trichotomy:

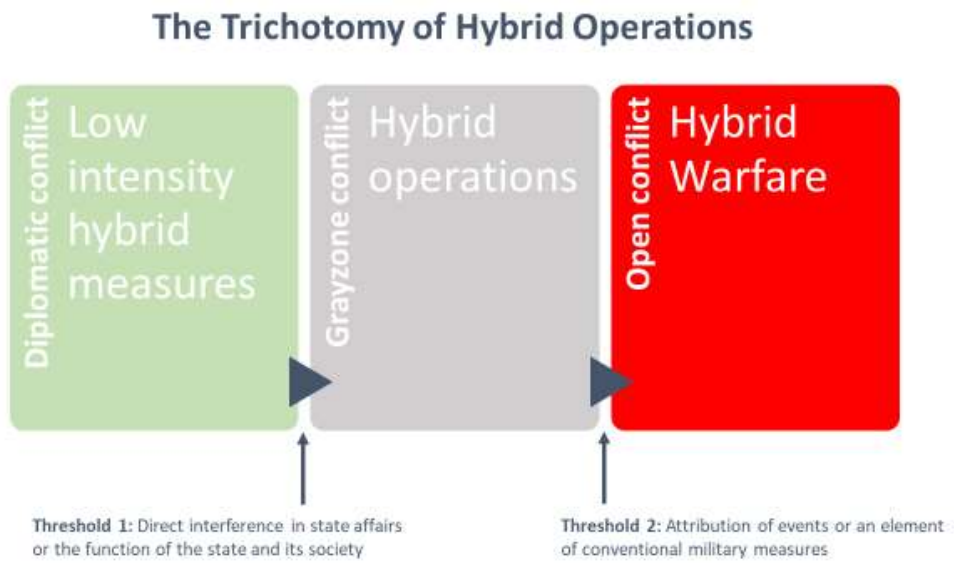


Figure 4.2: The Trichotomy of Operational Environments for Hybrid Operations

The trichotomy reduces the operational environments into three categories: Diplomatic, greyzone, and open conflicts. The preconditions for categorizing events will be based on the surpassing of two "thresholds". The first threshold is interference in state affairs. This is the

fundamental surpassing of diplomacy and is the introduction of more direct and harder measures to support foreign policy strategies. There may be applied lighter methods of hybrid measures on a pre-threshold basis as well, such as economic measures, but these are likely to be unsynchronous with other measures and rather part of either unilateral or multilateral "packages" of diplomatic actions. Once surpassed the first threshold, hybrid measures may be utilized in two modes, either as greyzone hybrid operations, or by surpassing the second threshold, as hybrid operations of open conflict, more popularly called hybrid warfare. The second threshold has two conditions, of which I have chosen for this illustration: Attribution of events, or an overweight of conventional measures or traditional combat operations. These two conditions partition the threshold into two approaches, further complicating the manoeuvring within these environments. Whereas the introduction of an overweight of conventional measures would be self-inflicted, the attribution of hybrid operations lies with the receiver of such actions and is, by such, out of control for the aggressor. The surpassing of the second threshold would thus lead the aggressor into an open conflict, where the agents are known, or at least presumed by the defendant, and would thus either, with regards to the initial taxonomy above, remain in the hybrid warfare environment, or if the option of conventional measures overweighs the unconventional means, lead the parties into traditional combat actions, where a hybrid element would pursue either enabling or supportive operations for the military campaign, which could be multi-domain, or in an all-out scenario, including elements of nuclear weapons.

4.1.2 Utilization of hybrid means in the context of an escalation process.

As revealed in the subchapter on both layers and intensity, hybrid means may be applied over a broad spectrum and with varying intensity to best feature its strategic objectives, fit the conditions for the operational environment it is set to operate in, and maintain its utility and cost-efficiency. Depending on how we measure intensity, it may vary from day to day or hour to hour. Some activities, such as cyber-attacks, have a limited time span of endurance because it depends on how quickly it is identified and the defendant resolves the vulnerability. The aggressor therefore may seek to attack several objects simultaneously, in combination with other hybrid efforts, to maximize the operational utility and intensity over shorter timeframes. The following figure illustrates how the escalation ladder for operations involving hybrid elements may be understood:

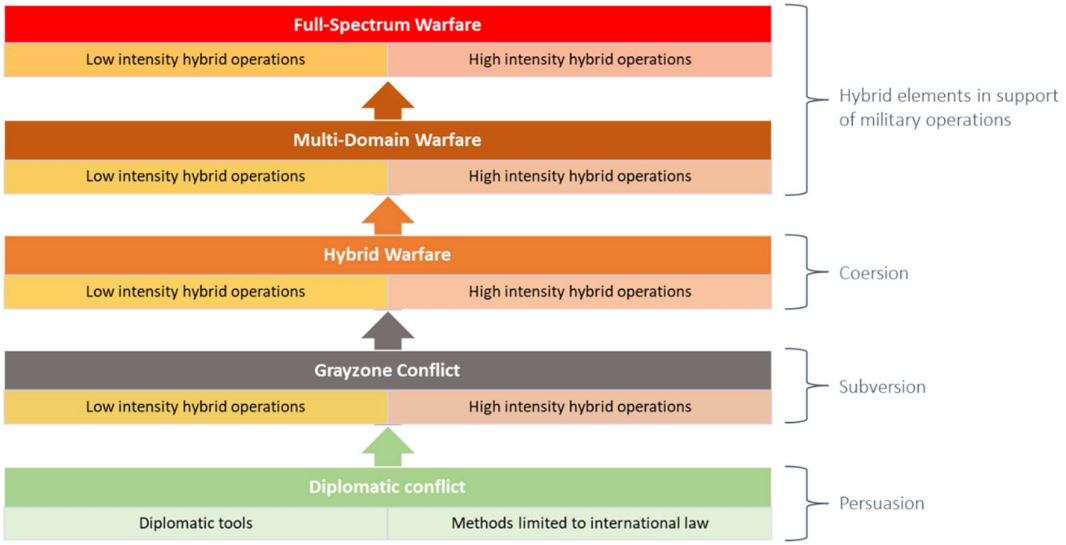


Figure 4.3: The escalation ladder for Hybrid Operations

The escalation ladder reveals how the intensity varies inside the operational environment and the strategies it may aim to achieve. Depending on the activities undertaken, an increase in intensity may lead to an escalation into the superseding operational environment. This is especially prominent in the first three environments, in which thresholds lead to an escalation of the concept. The first threshold is overstepped once the activities directly affect internal affairs or the state's population. This threshold is thus more related to the nature of the activity rather than the intensity itself. The second threshold, however, is related to the intensity of operations. An increase in intensity would likely increase the chances of being detected, either because the intensity is too severe for the efforts to be played undetected (activities lose their covertness) or that the number of ongoing activities is making the aggressor vulnerable to proceed with the necessary command and control to efficiently maintain its focus and becomes indiscreet in ways that may ease the defendant's possibilities of direct attribution.

The increase in escalatory level shifts the strategy of operation from persuasion and subversion to be of a more coercive nature once the conflict opens up. In the final two escalation levels represented here, where traditional military warfare dominates the conflict, the intensity of the hybrid elements could still vary, depending on the operational demands set forward. However, the escalation is rather dependent on the traditional efforts that dominate, such as an increase in domains utilized to provide operational utility or the introduction of nuclear weapons in either tactical or strategic manners.

Having clarified the concept of hybrid operations and reasoned how they help foreign policymakers defend their state or offensively apply hybrid operations in statecraft, I now turn to the deductive and explanatory part of the study. Supported by a richer understanding of hybrid operations, how may we go about explaining the actual use of hybrid operations in foreign and security politics?

Part 3

Deductive reasonings of hybrid operations

5.0 A deductive approach to the foreign policy of hybrid operations

Hybrid operations are part of the strategic toolbox for foreign policy and part of international politics. However, as it could be used subversively and coercively, it demands a framework of security politics. Realism is often the go-to theory for security politics, as it embraces state aggressiveness in the international system, as opposed to theories embracing international cooperation and integration. For the pilot study, I will employ systemic theories of international politics, more precisely, offensive and defensive realism. These theories do not apply domestic variables for their explanatory power and will thus be a preliminary study of how hybrid operations in its core could be used for interstate conflict. The subsequent empirical analysis will explore whether a systemic approach to the concept is sufficient or if domestic variables are needed to provide adequate explanatory power to its use and utility.

5.1 A fundamental approach to foreign policy analysis

Foreign policy itself could seem obscure and exhaustive. A general understanding is to perceive foreign policy as the state's interaction with other states. Fermann defines foreign policy as "the state's projection of self-interest on the global arena, within the scope for political manoeuvring perceived to exist and constructed through creative political action" (Fermann, 2022, p. 94). Foreign policy analysis (FPA) intends to, as opposed to the theories of international politics, understand states' foreign-directed strategies and behaviour, whereas international politics is more directed at understanding interstate interactions on a more overarching level (Fermann, 2022, p. 83). As a comprehensive perception of FPA, it could be understood as a multi-level and decision-making study (Fermann, 2022, p. 23). Fermann has

developed the following model to understand this interaction between levels further :

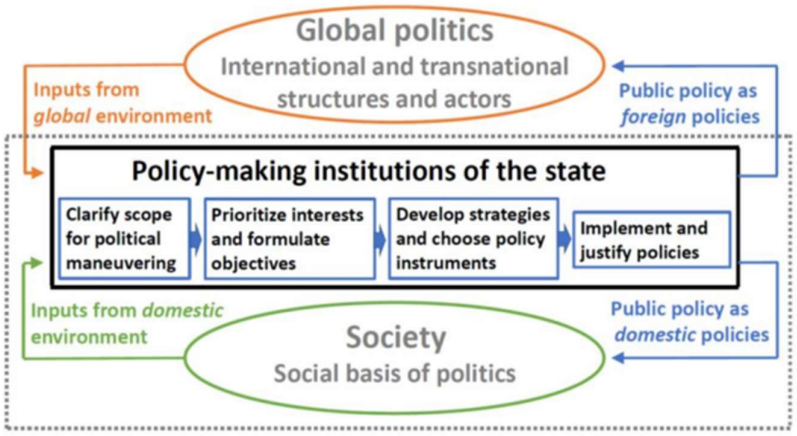


Figure 5.1: A multilevel model for Foreign Policy Analysis (Fermann, 2022, p. 23)

The FPA approach is divided into theories on a structural level (external influences), societal level, and the policy-making process. Some theorists seek to perform multi-variable analyses, whereas others are either mid-range theories with smaller scopes or are seeking to explain foreign policy from either the inside-out or outside-in perspectives only. As the instrument to be analysed in this thesis is related to security politics, structural theories of realism will be applied. However, as an axiom of such is related to the scope of political manoeuvring and the costs and risks involved, the analysis will be directed towards both the external and the decision-making process levels of FPA.

5.2 Outside-in approaches to FPA: Systemic realism

Systemic realism, or more precisely, offensive and defensive realism, is critical to the study of security politics. Both approaches are developed from the Realist theory tradition but offer different ways of explaining systemic state behaviour, as will be examined below.

5.2.1 Offensive realism

Eric Labs (1997, p. 11) argues that:

> Offensive realism holds that because security and survival are never assured in the international system, states seek to maximize their security by maximizing their relative power and influence where the benefits of doing so exceeds the costs.

By such means, offensive realist-oriented states seek to maximize their relative power yet remain cost-oriented. By many considered the founding father of the offensive realist approach, John Mearsheimer argues that great powers seek to maximize their power, and thus act aggressively to maintain their sovereignty. However, Mearsheimer also specifies that great

powers seek to maximize their share of world power (Mearsheimer 2001, p. 29). This does inevitably mean that great powers act as expansionist agents to pursue their aim of gaining increased relative power. This point establishes the primary conflict between offensive and defensive realism, whereas the latter focus on maintaining the state's status quo in the system, both by relative power and influence, whereas the former would seek to increase such expansionably.

Labs (1997, p. 12-13) states that weak states "are unlikely to pursue a strategy of expansion because the risk of doing so are likely to be high". This is because weak states would need to increase their relative power substantially more than great powers, and the risk would thus be exponentially higher, and by that, so would the costs.

When considering these axioms of offensive realism, it is reasonable to argue that hybrid operations would mitigate restraints in both risk and cost. With less risks and operational costs, the scope of manoeuvring for weak states could be exponentially enlarged, allowing weak states to explore expansionist strategies that previously would have been considered beyond their ambition-level. Labs further elaborates that "successful expanders learn from past mistakes and they try to go about expanding in a manner that draws the least attention from the other great powers" (Labs, 1997, p. 13). Hybrid capabilities are difficult to detect unless utilized in a manner that allows for the aggressor to be identified. The cyber- and information-domain's capabilities remain highly undetectable and are not as readily observable as the consolidation of conventional troops or material.

Offensive realists assess a state's relative position in the system, which is generally considered anarchic and Hobbesian. Based on capabilities and ability to project power, this relative position is traditionally determined based on military capabilities. Dependent on the relative damage potential of hybrid operations as opposed to conventional operations, hybrid capabilities are less detectable and thus impose additional risk for adversaries, demanding even more resolute actions to ensure their state's security. Such an environment amongst power-seeking states could lead to a potential security dilemma (as per subchapter 3.5.3), where the uncertainty of capabilities and motives with the adversary leads to an arms race where none of the parties practically gain any profit in relative power.

According to Mearsheimer, the urge for maximisation of power is not urged by human struggle to dominate others, as previously assumed by classical realist Morgenthau. Rather, it is driven by a search for security, forced by the anarchic structure of the international system

(Snyder, 2002, p. 151). Snyder maintains that "when all states have capabilities for doing each other harm, each is driven to amass as much power as it can to be as secure as possible against attack" (ibid).

Patrick (in Freyberg-Inan et al., 2009, p. 50) argues that offensive realism concentrates on five principal assumptions: the importance of anarchy, great power possessions of offensive military capabilities, a lack of certainty about each other's intentions, survival, and states as rational actors. Further, Patrick maintains that "great powers are primed for offense" (ibid).

According to Mearsheimer, even a distinct military advantage over rivals will not stop the driving force for maximation by great powers. "The pursuit of power stops only when hegemony is achieved" (Mearsheimer, 2001, p. 34). Further, Mearsheimer argues that states will pay particular notice to how the power is distributed amongst them and look for any opportunity to alter the balance of power "by acquiring additional increments of power at the expense of potential rivals" (ibid). The theories of offensive realism are specifically linked to the security dilemma at this point, although the dilemma itself reflects the paradox of security maximation. The security dilemma concentrates on the uncertainty between the states. This uncertainty concerns whether capability development is meant for offensive or defensive purposes, and what capabilities exist with the adversary, as pointed out by Patrick (2009). The constant development of capabilities and capacities is necessary not to fall behind. As Mearsheimer assess the security dilemma; the best defence is a good offence (Mearsheimer, 2001, p. 36).

To make this theory relevant for hybrid operations, even the knowledge about the existence of such capability would lead power-maximizing states to develop that capacity of their own because the absence of such capacity would make them relatively weaker to adversaries in possession of such capability. Mearsheimer states that "great powers cannot always act on their offensive intentions, because behavior is influenced not only by what states want, but also by their capacity to realize these desires" (Mearsheimer, 2001, p. 37). Hybrid measures, however, are an achievable capacity even for states with less resources because of their low costs, and in its current modus, heavily reliant on technology and digital infrastructure, infrastructure and knowledge in possess by most developed states in our contemporary system. Mearsheimer further asserts that "By contrast, great powers facing powerful opponents will be less inclined to consider offensive action and more concerned with defending the existing balance of power from threats by their more powerful opponents. Let there be an opportunity for those weaker states to revise the balance in their own favor,

however, and they will take advantage of it" (ibid). The development of hybrid capabilities could introduce a pivotal opportunity for states less inclined to project power by conventional means to achieve increased power by projecting power through hybrid capabilities instead. An example is Russia, which will be analyzed in the following empirical study in the next section. In a belligerent and malevolent system, Russia managed to expand into the Ukrainian region of Crimea by utilizing hybrid capacities only. The expansion increased security for Russian forces in the Black Sea region and allowed for greater Russian abilities to project power into a region of Europe subject to a "Westernization" after the disintegration of the Soviet Union. This specific example may also be analyzed through the lenses of defensive realism, an approach which will be made later in this section.

The possibility for relatively "weaker" states to develop hybrid capacities could prove itself as a game changer regarding the system's power distribution. As (Labs, 1997, p. 11) maintain, the states will only pursue expansionist strategies if the expected utility outweighs the expected cost. In other words, there must be a utility surplus as to the risk the state experience while pursuing such offensive ambitions. If the assumptions made in Part 2 on retribution and responses to hybrid operations hold, a successful hybrid strategy with sufficient levels of plausible deniability could potentially incentivise smaller and less resourceful states, with regard to traditional power capabilities, to pursue expansionist strategies, changing the distribution of power to their advantage, and yet face relatively "soft" material damage if deniability fails to hold. This could be the trigger allowing for the utility to supersede costs and risk. Labs argue that "when states are presented with opportunities that will easily and cheaply increase their relative power, states will take advantage of them" (Labs, 1997, p. 12). Given the uncertainty of outcome of hybrid operations, as opposed to the possibility of "war gaming" conventional operations in advance, it is likely to assume that hybrid strategies would be more prominent for states with a relatively weaker conventional capacity, as great powers would see more certainty, thus lower risk, by utilizing their conventional capabilities. Labs supports this point and asserts that "states calculate rationally the best way to expand their relative power" (ibid) and thus emphasizes one of the main axioms of offensive realism, namely rational actors.

How may hybrid operations be utilized for expansive strategies?

The main feature of hybrid operations, from an offensive realist approach, is that it offers a cost-efficient, low-risk option for aggressive strategies of foreign policy. The utilisation level for hybrid operations is yet to be revealed in its entirety. Offensive realism is centred around power maximisation through expansion. As hybrid operations themselves offer no "occupying" force, it is difficult to predict whether it has the ability of substantial expansion alone or not. The Russian annexation of Crimea in 2014 is one example of expansionist endeavours initiated and fulfilled by hybrid measures alone. It could be argued that Russia already possessed a fleet presence in the city of Sevastopol at the time, but operations were largely carried out with unconventional measures, and Russia was quickly able to control the whole peninsula. Whether such an operation would be profitable for larger areas of operation, including regime change strategies, is unknown.

However, it is prominent that activities in the information domain, combined with special activities, such as false flag operations carried out in the form of violence or terrorism attacks, could undoubtedly lay the foundations for riots, demonstrations and potential regime change in states. Such regime change could enhance the aggressor's influence and control of the area by pushing forward for the election of benevolent leaders prone to cooperation with the antagonist.

Hybrid operations could also come in handy for growing powers seeking to expand their influence and power for strategies of systemic change. One example that is clear for this certain point is Iran's use of Hezbollah as a proxy, as previously mentioned, to diminish Israeli influence and power in the Middle East, and thus diminish the Israeli capacity and ability to grow stronger while at the same time accumulating strength themselves by being able to occupy the adversary while developing and increasing capabilities and capacities of their own.

One of the maybe least discussed modes of hybrid operations is its enabling ability for conventional military campaigns. The ability of the information domain to set benign preconditions for military intervention could, if successful, be a game changer regarding how quickly and easily an invasion or intervention could proceed. In combination with pre-established vulnerabilities or diminishing of capabilities and capacities caused by sabotage to digital or physical infrastructure, a well-established hybrid-enabled conventional operation

could possibly see a much higher utility and reduced costs as compared to a conventional operation carried out without enabling premeasures.

From the theoretical arguments of offensive realism, we may deduce the following argument:

H1: *Hybrid measures offer a pivotable capability for offensive operations and could be the decisive capacity for expansionist strategies.*

Especially prominent for H1 is the concept of A2/AD for hybrid efforts, a strategy that denies the adversary access to a specific domain or geographical area on the battlefield.

5.2.2 Defensive realism

Defensive realism is, in contrast to offensive realism, more oriented around maintaining the current status quo than aggregating additional relative power, as seen in offensive realism. Rose (1998, p. 150) states that:

> Defensive realists view the international system as the cause of what might be called "natural" conduct, which includes a resort to aggression only if military technology or certain other factors provide clear incentives to strike first. They consider the remainder of aggressive behavior to be "unnatural" and account for it by auxiliary hypotheses involving domestic variables (Rose, 1998, p. 150)

Mearsheimer argues that defensive realism came with the appearance of Walt's *Theory of International Politics* in the late 1970s, when Waltz drew the assumptions that great powers, as opposed to Morgenthau's classical view, are not inherently aggressive "because they are infused with a will to power". Rather, they merely aim to survive" (Mearsheimer, 2001, p. 19). Above all else, states, seen from a defensive realist point of view, seek security, not power (ibid). Kenneth Waltz states that:

> In anarchy, security is the highest end. Only if survival is assured can states safely seek such other goals as tranquillity, profit, and power. [..] The first concern of states is not to maximize power but to maintain their position in the system (in Schweller, 1996, p. 102; Waltz, 1979, p. 126).

Where offensive realists think of the international system as anarchic and hostile, defensive realists assume it is more benign (Rose, 1998, p. 149). Waltz, however, does inherit the anarchic-systemic view but emphasizes that it does not incentivise great powers to act offensively to gain power. Rather, Waltz holds that it encourages defensive behaviour to maintain rather than change the balance of power (Mearsheimer, 2001, pp. 19-20). Moreover, offensive realists presume that security is scarce, whereas defensive realists see it as more

plentiful than might previously assumed (Rose, 1998, p. 149-150). Where the actors in the system usually act rationally to the systemic incentives, only reaching to conflict-related behaviour when the security dilemma demands such of the involved parties, the abnormal occurrences of unwarranted hostilities is by defensive realists explained by rogue states, that either misperceive or simply ignore the security-related incentives offered by their environment (Ibid).

Randall Schweller names these defensive realist-oriented states "status-quo states". Schweller asserts that "because status-quo states value what they possess more than what they covet, they maximize security, not power. Most important, status-quo states do not employ military means to extend their values" (Schweller, 1996, p. 99).

In contrast to offensive realism, defensive realism opens up for cooperation and alliances to maintain security, stability and balance of power distributions. Schweller asserts that "only the strongest of states under the best circumstances can hope to achieve security through unilateral means." Furthermore, that "most often, states seeking security share a common interest in cooperation" (Schweller, 1996, p. 103). Schweller, however, makes the caveat, supported by Robert Jervis, that this holds "when technology and geography favour defensive military strategies and force structures" (ibid).

Taliaferro (2001) argues that different defensive realist assumptions on anarchy are to be found, mainly divided between theorists belonging to either the neorealist or neoclassical realist tradition (Taliaferro, 2001, p. 135). Taliaferro argues that offensive realists, such as Fareed Zakaria and Randall Schweller, maintain that defensive realism cannot explain state expansion "because it argues that there are *never* international incentives for such behaviour" (2001, pp. 129-130). Yet, Taliaferro maintains that under neorealist approaches to defensive realist assumptions on anarchy, the international system provides incentives for expansion, yet only under certain conditions (2001, p. 135).

Taliaferro argues that defensive realists assume that *structural modifiers* influence the likelihood of conflict or cooperation more than the distribution of power (Taliaferro, 2001, p. 137). Structural modifiers, conceptually developed by Glenn Snyder, assume that other factors other than the gross distribution of power play a role in the systemic balance. Such variables include the offense-defence balance in military technology, geographic proximity, access to raw materials, international economic pressure, regional or dyadic military balances, and each state's ability to extract resources from conquered territory (Taliaferro, 2001, p.

137). Mearsheimer emphasizes the points of Taliaferro and previously Schweller, on the offense-defence balance and the importance of what the technology favours at any given point. Supported by arguments of Jervis, Snyder and Stephen Van Evera, Mearsheimer asserts that “military power at any point in time can be categorized as favouring either offense or defence” and that “conquest is therefore difficult, great powers will have little incentive to use force to gain power and will concentrate instead on protecting what they have” (Mearsheimer, 2001, p. 20). The latter forms the objective of defensive realism concentrating on security maximation rather than power maximation, and how the status quo in such times would be favourable to the system's actors. However, as maintained by Taliaferro, by turning his axiom of defensive realist approaches to the anarchy, the international system *does* provide incentives for expansion under certain conditions. Mearsheimer asserts this further: "if offense is easier, states will be sorely tempted to try conquering each other, and there will be a lot of war in the system” (Mearsheimer, 2001, p. 20). However, Mearsheimer emphasizes that defensive realists argue that the offense-defence balance is usually heavily tilted toward defence, “making conquest extremely difficult” (ibid).

The distribution of power in the balance of power is heavily discussed in both offensive and defensive realism, but it appears to be a given as to how states understand this situation. It is understood that systemic theories such as offensive and defensive realism are to be analysed at a systemic level rather than to provide a unit-level analysis, of which instead would be subject to the foreign policy analysis (FPA) field (Levy, in Jervis et al., 2003, p. 254). However, is it a given that there is a universal understanding, or situational awareness, as to how the status quo is balanced or how the power is distributed amongst the states? Realism, in general, presumes states as rational actors. Levy (in Jervis et al., 2003, pp. 269-270) argues that “there is growing evidence that people systemically depart from the predictions of [this] core theory of rational decision making”, being the maximation of expected utility. Levy introduces the assumptions of prospect theory as an alternative, as it posits that “people are more sensitive to changes in assets than to net asset levels” and that “people frame choice problems around a *reference point*” (ibid). If this theory on rationality also holds at a systemic level, the reference point concept could be the understanding of behaviour that defensive realist depicts as “rogue” states. The status quo could be of different understanding, and the responsiveness of states to interact offensively or defensively could possibly be related to their reference point as related to what status quo or distribution of power the state feels impelled to safeguard themselves to belong. If such an argument holds, aggressiveness in

cases of reference point-regaining measures could possibly be understood as defensive or balancing as opposed to expansive power-maximizing behaviour. A supportive argument for the latter is found in the concept of *preventive wars*, where aggressive behaviour is related to the growing imbalance in relative power, where the declining power initiates a war as "a necessary mean of maintaining equilibrium in the system", because of the fear for restriction, "if not the extinction, of their own" (Howard and Morgenthau, as cited in Levy, 1987, p. 83). Such measures support the fundamental idea of defensive realism being about the security and survivability of the state.

How may the theories of defensive realism explain hybrid operations?

Hybrid measures as an instrument of the state are fairly coinciding with the strategies and assumptions of the defensive realist approach to the system. The plausibility and "softness" of hybrid operations, yet coercive by kind, align well with balancing and non-aggressive behaviour. However, there is still uncertainty regarding the utility level of hybrid operations. The utility is not necessarily linked to the success of such operations but rather to how large and comprehensive objectives it could achieve. The examples previously mentioned in this thesis, the joint US-Israeli Olympus operation against Iran, as well as the Chinese use of economic pressure and irregular warfare through paramilitary fishing vessels in the South China Sea, could be seen as hybrid operations carried out to preserve interest and power projection abilities in their respective areas. Further, they might diminish foreign influence, causing a regional change in the power distribution, which with the named actors, could have implications for the power distribution in the global system of states.

Although hybrid operations, as established through the inductive introduction of the various measures it could involve, are primarily directed towards the civilian society and common infrastructure, they are "softer" than using kinetic force through conventional combat. This aspect makes the measures less aggressive, in common sense, even though the strategies and objectives they are employed to achieve are aggressive from a strategic perspective. It is also worth noting that plausible deniability and unattributionality could be utilized to deter responses and retributional aggression and thus secure objectives of survivability and upkeeping of the status quo.

Another factor that might be the most important utility function of hybrid operations is its operational modus as a mechanism of deterrence. As conceptualized previously, hybrid operations could be applied as an instrument of deterrence, not only for expansionist

endeavours. The leading example is the (at this point not officially attributed) Russian use of drones in close vicinity to critical infrastructure installations, such as offshore platforms and nuclear energy plants. These special intelligence activities are not destructive to the infrastructure but work as a form of power projection in a way to warn adversaries about the capabilities and capacities of the aggressor to cause detrimental damage, not only to the state's ability to function, but to the safety and survival of its population, the founding objectives of the state's tasks towards its population. The actual sabotage of infrastructure, such as seen with the Nord-Stream pipeline explosions, and potentially, if found proven as intended actions, the outage of subsea communications cables in Scotland and the Svalbard peninsula, would further amplify the signals of deterrence and power projection.

Also, to support the previous assumption on deterrence, it is essential to revisit the argument of hybrid operations being "softer" and more asymmetric than conventional power projection. Going back to the example of Russian deterrence, one of the strategies of the great power has since the cold war been nuclear deterrence through visible overflights by long-range strategic aviation elements. These are effective because of the potential destruction these operations could carry out in a live-firing scenario. Such a strategy of deterrence is effective because it visualises a will and ability to carry out nuclear strikes. However, it also risks escalating the situation to possibly cause more uncertainty and alert by the systemic states than what would be favourable from a defensive and balancing strategy, and thus be "too efficient" and leave a diminishing return on utility.

From the theoretical arguments of defensive realism, we may deduce the following argument:

H2: *Hybrid operations offer suitable measures for the defence of territorial integrity and the maintenance of the state's ability to project power and maintain the status quo of the system.*

The second hypothesis is especially aligned with the concept of hybrid deterrence, as inductively argued from conventional doctrine and adapted for a hybrid context.

5.3 Inside-out approaches to systemic FPA theories: How may the perception of risk and cost affect the SPM of foreign policy making?

How do states employing hybrid measures justify such utilization for the cost/benefit utility equation that is so clearly prominent in realist theory? To provide a clearer understanding of the importance of such, especially how the attributes of hybrid measures are especially prominent at this point, I will review a few theories on political behaviour and risk management. Such variables are in a greyzone as to the core element of systemic theories not including unit-level variables. However, the specific axiom that calls for a strategy to be profitable to be employed makes it evident that some kind of utility function must be assessed, and the definitions of risk and cost with regard to this context should be reviewed.

Jack Levy (2003) focuses on the impact of psychological factors on judgment and decision-making by political leaders. Levy argues that:

> "Psychological variables must be integrated into a broader theory of foreign policy that incorporates state-level causal variables and that explains how the preferences, beliefs, and judgements of key individual actors get aggregated into a foreign policy decision for the state" (Levy, as cited in Jervis et al., 2003, p. 254)

Preferences for state leaders will often be related to risk-taking and perceptions of their adversaries. The international system provides insufficient and sometimes asymmetric distribution of information, which could lead to misperceptions and actions enacted on incorrect premises.

Linde & Vis (as referred to in Vis & Kuijpers, 2018, p. 577) identifies two types of risk. Type 1 is considered what we usually perceive as risks, namely the expected consequences of an action. Type 2 is used in prospect theory and theories of expected utility and defines risk as the degree of uncertainty of outcome. Both types of risk become evident while analysing the decision-making processes behind the utilization of strategies for hybrid operations. The risk related to the consequences of the actions, Type 1, introduces the cost element to the equation. This element could be divided into two subtypes; the cost related to the operation itself, and the cost related to potential backlashes from the operation. The second subtype is the most relatable here, as the backlashes and retributions coming from the operation could induce a higher cost on the aggressor than that generated by the resources put into the operation respectively. This leads to basic assumptions on the gain over potential costs. It is, however, important to emphasize that also potential losses of own capabilities, as in conventional

operations, could be encountered, as physical operations often involve some element of personnel involved.

Also Type 2 risk perception is related to an element of cost. The first subtype, the cost related to the operation, becomes an element while assessing the confidence of the operation and the risk related to the uncertainty behind this element. If there is a high degree of uncertainty about the operation, and the operation itself generates a requirement of substantive resources, the traditional calculations of utility level would, in many cases, deem the risk too high.

As previously established, hybrid operations are characterised by low cost and reduced risk. The risk element referred to in this case is related to type 1 risk, as plausible deniability reduces the risk of attributability, thus reducing the risk of retributions. However, little is known about the uncertainties related to the projected successability of such operations. Furthermore, hybrid operations often involve a psychological aspect with the recipients, especially those related to the information domain. Therefore, it would be natural to assume that the uncertainties related to the successability of such operations are high. However, since the operational costs and relative requirement of resources are low, this balances the risk regarding Type 2 risk perceptions. An initial conclusion would thus be that decision-makers assessing hybrid strategies would be presented with reduced type 1 risks, while the uncertainties related to outcome, Type 2, would be substantial. However, the risk could be deemed acceptable since the related costs are low.

Both offensive and defensive theories of realism keep, as their primary assumption, that the international system is composed of "unitary, rational states motivated by a desire for security" (Rose, 1998, p. 149). While ascribing the latter to theories including domestic-political variables, such as the theory of Fearon (1998), we would primarily assess decision-makers as rational agents. Fearon elaborates that the opposite would require additional domestic variables to discover the underlying causes for such irrational behaviour. Both rational and irrational behaviour must be investigated with a focus on perceived risk. Irrational behaviour could potentially be rational given the information available and the situational awareness and perceptions made by the decision-makers in any given case. A case of irrational behaviour while fully informed could just as much be rational behaviour given the situation the decision-makers face while carrying out their actions. The latter may explain the anomalies in defensive realism, popularly named "rogue states" (Rose, 1998, p. 150).

Considering the theories of risk management with decision makers we may formulate the following proposition:

H3: States would pursue hybrid rather than conventional strategies in offensive operations when Type 1 risks introduce serious inquiries about the profitable utility of the operation.

H3 seeks to test whether the assumption of hybrid operations used for risk mitigating purposes holds. In other words, do states shift to hybrid strategies if the Risk 1 factors are deemed too high, as hybrid strategies mitigate some of this risk by operating under ambiguity and facilitate plausible deniability? With the following review on risk, cost and utility in mind, we can set forward a more comprehensive theoretical framework for study in the following empirical analysis.

5.4 Pointing the theoretical arguments: Formulating empirical propositions

The theories applied here for the understanding of international politics, offensive and defensive realism, will be applied as the fundamental theoretical framework to be tested in the empirical analysis. We see that the inductive findings of hybrid measures are feasible for explanation in both structural theories. The main benefit that is prominent for both theories is that hybrid operations enhance the states' respective political scope of manoeuvring, a variable usually applied as a domestic variable, but when simplified to a utility function of presumed successfulness (risk) and cost, becomes effective for the primary axiom of realism, the rationality of states, that aggressiveness only is preferred when the utility is assumed as higher than the costs related. As discussed concerning risk theories, the cost element of risk is both related to operational costs (the possibility of loss of personnel and materiel, as well as the economic costs of running the operation) as well as the possible loss of political capital related to the risks of attribution or retaliation. This means that the presumed outcome and the calculated likelihood of success must outweigh the calculated costs.

As inductively reasoned, hybrid operations are both cost-efficient and low-risk policy instruments, primarily due to their covertness and possibility of plausible deniability. This enhances the strategic abilities capability and capacity wise with the states possessing such capabilities. What we would want to test in the initial test environment presented in the empirical study is whether or not these features offer sufficient profitability for offensive or defensive purposes and whether or not the concepts found in the inductive section are likely to occur in a benign testing environment. The following analysis of the empirical study will then answer whether the induced framework and theoretical arguments are sufficient for large-scale testing by generalizable cases or if the framework needs improvement or changes in explanatory theories.

Part 4

Researching plausible cases of hybrid operations

6.0 Case-selection and the empirical mapping of hybrid operations in a pilot study

In Part 3, an attempt was made to establish an FPA framework and invite additional theories from which empirical propositions on the conditions for using hybrid operations in statecraft for defensive or offensive purposes could be made. In this chapter, we follow up on the deductive challenge by confronting the hypotheses with empirical evidence from two related cases. This third main contribution to the study of the foreign politics of hybrid operations should not be considered conclusive, but rather be assessed on its merit as a pilot study.

6.1 Case selection

As set by the plausibility probe research design, this empirical study is intended to be a pilot study conducted in a benevolent testing environment to conduct preliminary testing of the framework. The following analysis of the pilot study will reveal possible improvements to the framework and indicate whether the framework is sufficient to explain the phenomenon or if alterations or a change of theories should be made. The selected case for the pilot study is the Russo-Ukrainian war, which has been ongoing since 2014, with various degrees of intensity. This conflict will, for simplicity, be divided into two semi-cases, the 2014 annexation of Crimea and the ongoing full-scale invasion of Ukraine that started in February 2022. First, I will start this part by briefly explaining the cases and their background.

6.1.1 Case-specific background:

The Russian annexation of the Ukrainian peninsula Crimea, and consequently also to include the eastern Ukrainian oblasts of Luhansk, Donetsk, Zaporizhzhia and Kherson, is the only breach in security on the European continent since the conflict of the former Yugoslavia at the very end of the 1990s. The Russian application of force in Crimea, and the Donbas region in 2014 and the years to follow, quickly popularized the term Hybrid Warfare and would by some be considered the rebirth of the concept into contemporary strategic doctrine. The Russian operation in Ukraine started at the very end of February 2014 but has been a long-lasting conflict, leading to the formal annexation of Crimea - evolving into a civil war by proxy in the easternmost region of Donbas, including the oblasts of Luhansk and Donetsk – and for the time being, ending in the full-scale invasion, initiated in February 2022, eight years after the initial hostilities started. It is essential to acknowledge that although this case study treats this conflict as two separate cases, the hostilities and conflict have lasted for nine years to date.

However, the level of intensity does allow for certain distinctions to be made, and for the case of this paper, the conflict will be analyzed as two campaigns – the 2014 campaign directed against Crimea, and the 2022 full-scale invasion, initially directed to force forward a regime change in Kyiv.

As the conflict isolated may be divided into two separate, yet interconnected campaigns, the conflict itself must also be treated as a conflict of two levels. The microspectre, focusing on the mere area of operation in which the level of intensity of the hostility is at its most severe, and the macrospectre, the extended area of operation in which strategies are employed to deter the adversary from intervening in the main theatre of operations. For these very cases, it must be made a distinction between Russian strategies and actions in the Ukrainian theatre of war, and Russian actions against other agents related to the main subject, in these cases, NATO and its partners. The comparative case study will thus analyze changes and similarities in the choice of measures both at the micro and the macrolevel.

6.1.2 Criticism of empirical evidence

This case study sets out to analyze the comparative differences in the two described cases regarding the utilization of hybrid measures on both the micro and macro level. The study is looking at Russian foreign policy strategies in the cases, and will thus not look at hybrid efforts by other actors.

This case study makes use of empirical evidence and government reports to test the hypotheses set forward by this paper's deductive analysis. However, a caveat must be emphasised regarding the empirical evidence presented in the following analysis. The conflict is relatively new, both the Crimean annexation, for which this analysis will treat as Case 1 and the ongoing campaign accounting for Case 2. The recentness lays forward a potential scientific trap, for which the conflict is highly relevant for contemporary research, albeit data proves too uncertain to return a sufficiently asserted result with regard to unpoliticized evidence.

The nature of hybrid warfare does, as previously asserted, treat the information domain as one of its main venues. This axiom of hybridity, combined with the uncertainties created by plausible deniability, makes it impossible to assert the objectivity in both free and state-owned media sources, think tanks, research establishments and not least, government documents. As far as objectivity in the free media and research communities in Western countries go, some

sort of politicization will remain, especially in cases like these, where narrative control and opinion priming are so extensive.

The above remarks are especially prominent while analyzing the Russian perspective of the Western conflict approach. Russian media outlets are often state-owned or have extensive ties to government bodies or high-ranking government officials (Kovalev, 2021, p. 2908).

6.2 Background:

Russia has, since the early 1600s, exercised firm control over various regions of what since 1991 has been recognized as the sovereign nation of Ukraine. As a region, Ukraine has been controlled by various regimes, and fairly divided over time, between the Muscovites, the Polish-Lithuanian duchy, and the Habsburg Empire. This area division has mainly been exercised around the Dnieper River, dividing the country land into the west- and east bank Ukraine (Plokhy, 2015). This division has have led to a cleavage in both languages, culture and national affiliation. In a study by Bureiko & Moga they find that when asked "I feel Ukrainian" in 2013, only 69,8% of the Crimean respondents agrees, as opposed to the national average of 85,9%. The result is correspondingly low in Luhansk, and only slightly higher in Donetsk (Bureiko & Moga, 2019, p. 151), the latter two being subject to subsequent annexation by Russia.

In contrast, the western parts, especially parts of Lviv and the former principality of Galicia have been influenced by European and especially Polish culture and thinking, and the eastern regions (in Ukrainian "oblast") have been more exposed to Russian influences. This have led to a demographic cleavage (Shulman, 1999, p. 1012). This division has also revealed itself in the presidential elections, where Russian and European-friendly administrations have relieved each other over the soon-to-be three decades of independence. In 2013, Ukraine was on its way to sign an association agreement with the EU. However, after pressure from Russia, the agreement was suspended. The Euromaidan revolution in 2013, followed by the Maidan revolution in 2014 against the Russian-oriented President Viktor Yanuchenko, allowed the people to "voice their protest against the government's decision to choose a Russian model of development for Ukraine (Törnquist-Plewa & Yurchuk, 2019, p. 699). Russia found themselves gradually losing increasingly more of their influence over the former Soviet republic.

Crimea, as subject to its geography, is strategically important to Russia, as the peninsula encloses the Azov Sea from the Black Sea, limiting all passage into the important Russian cities of Taranrog and Rostov-on-Don to the strait of Kerch. Following the disintegration of the Soviet Union, Russia has considered Ukraine a buffer zone integral to their security (Tuncer & Erkut, 2022, pp. 96-97).

6.3 Case 1: The Russian operations in Ukraine in 2014

6.3.1 The microlevel – Russian operations in the Theatre of War

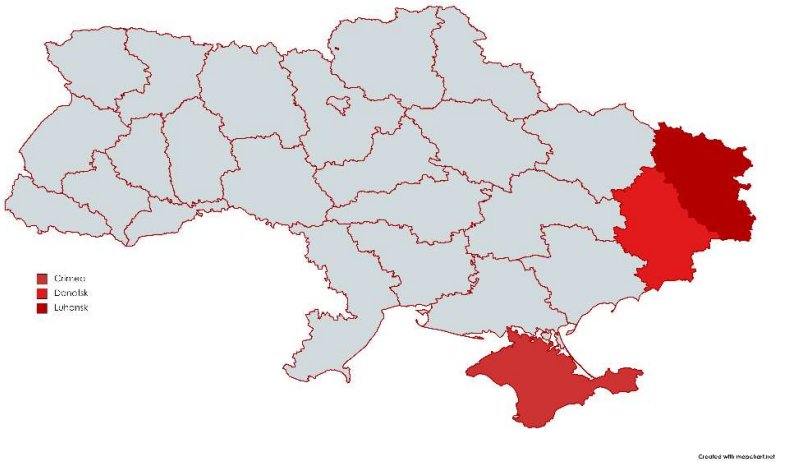


Figure 6.1: Area of Operation during the 2014 Crisis. This case focuses on the Crimean Theathre in the south.

Chronology of events and the military domain:

Both Russian and Ukrainian military units went on a high-readiness alert on February 20th 2014, following the escalations in the Maidan protests in Kyiv, as they went into violent clashes between protesters and the Ukrainian security forces. On February 24th, the city council of Sevastopol replaced its mayor with a Russian citizen. In the wake of the former event, Russian units from the naval infantry deployed to the permanent Russian base were mobilized into the city centre. On February 27th, Russian SOF elements, disguised as local militia (Kofman et al., 2017, p. 7) or even allegedly as Ukrainian security forces (DeBenedictis, 2021), seized the Crimean parliament and raised the Russian flag over the building. Further, in the evening of the 27th, Russian forces without insignia surrounded the Belbek Air Base, situated north of Sevastopol. The operation allowed for the arrival of Russian transport- and attack helicopters to the theatre. The following day, a similar operation was conducted in the Simferopol International airport, leading to the cancellation of civilian air traffic and the arrival of additional Russian elements, this time from airborne VDV units (Kofman et al., 2017, p. 8) These force movements led to the events and sightings of what quickly was popularized as "the little green men" in Crimea. With no insignia and under cover of being local resistance forces, these Russian military elements effectively took control of the peninsula and established Russian control over the region. In the wake of the events, Crimea declared independence from Ukraine, details of which will be included in the subsequent subchapter.

Russian influence and information operations during the campaign

RAND maintains that Russian information campaigns were in place both before, during and after the actual campaign in Crimea occurred (Kofman et al., 2017, p. 12). They further maintain that these operations were directed towards both Russian and Ukrainian audiences. The close association between Russian news outlets and Russian authorities allowed disinformation to be distributed through various channels. Skewed framings of the Euromaidan crisis were publicized already prior to the campaign, in close conjunction with stories on brutalities from the Ukrainian authorities towards their Russian-speaking population, allegedly leading to hundreds of refugees fleeing to Russia (Jaitner & Mattsson, 2015, p. 42).

Russian disinformation campaigns during the 2014 campaign were largely intended to cause confusion and chaos within the Ukrainian theatre. Already before the annexation, Russian military intelligence, the GRU, used extensive resources to create fake social media profiles to reshape the narrative of the Maidan demonstrations in Kyiv (Moore, 2019, p. 5), which was directed at moving Ukraine towards a more European-directed approach, opposing the political views of the then incumbent Russian-friendly administration of President Viktor Yanukovych. Russian disinformation campaigns also initiated at framing the Ukrainian opposition movement as "fascist", a characteristic used by Russia to describe the Ukrainian authorities ever since (ibid).

The above exemplification represents the application of hybrid measures, both disinformation and influence operations, employed to create both a pretext for the campaign, but also to domestically legitimize Russian involvement, if the denial of Russian involvement lost its credibility.

Russian information operations also sought to create an information dominance for its campaigns. To achieve such, the Russian operation put forward what arguably could be called an effort of A2/AD in the information domain. Keir Giles maintains that "Russia also successfully achieved control over telecommunications including the notionally independent internet, and thus successfully isolated Crimea from independent news from the outside world." Furthermore, that this led the "public perception in Crimea of events in the rest of Ukraine being determined exclusively by Russia, which greatly facilitated the Russian seizure of the peninsula and subsequent attempts at its legitimation" (Giles, 2016, p. 12). Russian control of the information domain was effectively achieved by taking physical control of the internet and telecom infrastructure on the peninsula (ibid), which introduces synergies of

synchronous use of measures, as this involves the military element of such instruments, as well as the cyber element in the infrastructure.

The information operations in Crimea were conducted in a clearly benevolent environment. Rusnáková maintains that:

> "The fact that Russian speaking minority in Crimea represents in overall 58.5% of the total population of Crimea made the likelihood of operation's success and effectiveness even higher when we consider the potential of the misuse of this statistics: The Russian-speaking diaspora, who have maintained cultural and emotional bonds with Russia, was Russia's main ally during the Crimean operation" (Rusnáková, 2017, p. 359).

Shortly after the occupation, the local semi-autonomous authorities launched a referendum on independence from Ukraine. Whereas disinformation quoted 97% of the votes to be in favour of independence, with an 80% voter turnout, the realities of the referendum, according to Murphy, was, in fact, a 30% turnout, in which half of whom voted against independence (Murphy, as cited in Rusnáková, 2017, p. 360).

Russian cyber operations during the campaign

In March 2014, Russia launched an eight-minute-long DDoS attack on Ukraine aimed at destabilizing Ukrainian networks and communication solutions. The attack was launched merely three days before the referendum on the status of Crimea and served as a measure to divert public attention away from the presence of Russian troops in the area (Przetacznik, 2022, p. 3).

In May 2014, pro-Russian hacktivist groups, often tightly related to formal bodies, carried out a series of cyberattacks aimed at the Ukrainian presidential election, leading to a delay in the final election count. Over the course of the years 2015 and 2016, several DDoS attacks led to power outages for civilian Ukrainians, resulting in more than 230.000 Ukrainians experiencing power outages (ibid).

For the 2014 campaign, it is important to emphasize that cyber operations, concerning efforts through network operations and malware were not especially prominent and had no decisive importance for the successfulness of the Russian occupation of Crimea (Rusnáková, 2017, p. 361). However, as discussed in the previous subchapter, Russian forces did successfully cause a disturbance to unfettered internet access, which could be seen as an attack on cyberinfrastructure. However, as established previously, this operation was conducted through physical efforts rather than through cyber-attacks.

6.3.2 The macrolevel – Russia's behaviour towards its neighbours

During the hybrid operation in Crimea, Russia initiated a snap major joint exercise in its western military district. The exercise included 150,000 troops, including three armies, and hundreds of tanks and aircraft (Norberg, 2014). The exercise functioned to project Russian military power from the Kola Peninsula to the Ukrainian border, and functioned to prevent adversary intervention in the ongoing operation in Crimea (ibid).

Russian strategic deterrence and signaling were otherwise at a high level and air operations showed an increase in 2014, compared to 2013 (VG, 2015). This is illustrated further in subchapter 6.4.2, where comparative levels during the Russo-Georgian war and during the 2022 campaign is elaborated.

6.4 Case 2: The Russian operations in Ukraine in 2022

6.4.1 The microlevel – Russian operations in the theatre of war

Chronology of events

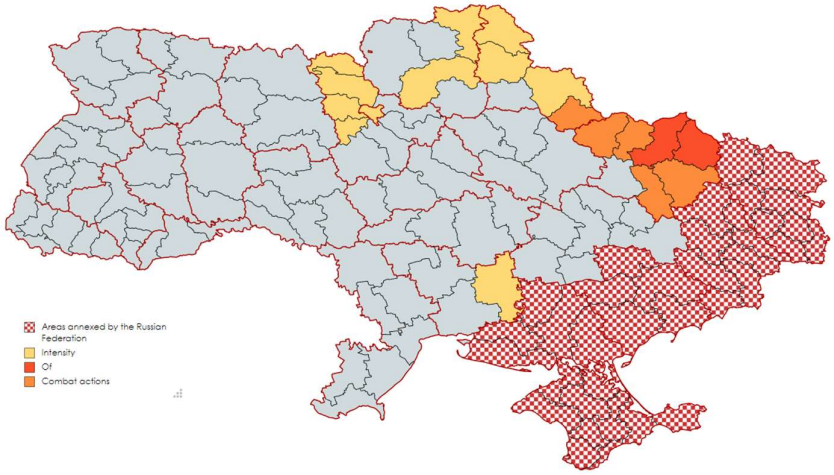


Figure 6.2: Area of Operation during the 2022 campaign. Marked annexed areas must be seen as the current status by March 2023. (Data for graphics: Financial Times, 2023)

At the end of 2021, Russia started a limited mobilization of forces within its territory, publicly announced to be carried out as preparations for a Russo-Belarusian joint exercise in the winter of 2021/2022. This mobilization caught international headlines, and especially US intelligence warned against the exercise being a smokescreen to cover for an imminent attack on Ukraine (Breuninger & Wilkie, 2022; Ivanova et al., 2021). The warnings were not recognized publicly by Ukrainian president Volodymyr Zelensky (BBC, 2022b), but there is no doubt that the US warnings did diminish the Russian element of surprise, as opposed to the preconditions seen before the 2014 operation.

On February 24th 2022, Russia initiated its campaign against Ukrainian territories. The invasion started with a massive fire-strike campaign across Ukraine. Before the physical attack, Russian electronic warfare units carried out electronic attacks against Ukrainian radar and air-defense installations to facilitate the coming attacks (Danylyuk et al., 2022, p. 24). Initial Russian air strikes were unexplainably unsuccessful and bizarre. Although Russian intelligence had mapped a substantive number of military sites, the prioritizing and timing of the strikes were inadequate at best and calls for serious inquiries to be made about the Russian targeting process. Few air strikes were timely coordinated against tactical groups (manoeuvrable forces), allowing the Ukrainians to re-group and displace elements to new locations. Some air strikes were even targeting military sites that had seized to commence

military activities several years earlier (Ibid). However, within the first 48 hours of the operations, Russian air strikes had successfully engaged approximately 75% of the stationary Ukrainian Air Defense sites, while the corresponding hit rate against mobile air defence systems was merely 10% (Ibid). This ultimately led to a situation where Russia found themselves commencing a land operation into Ukrainian territory but was unsuccessful to adequately securing air sovereignty in the air domain and thus failed to sufficiently be able to provide close air support to their own forces. This was further complicated by poor communication between strategical and tactical elements, as Russian land-based elements were told to presume that aircraft were friendly (Danylyuk et al., 2022, p. 26).

Within the first 72 hours, Russian land elements had seized territories within the borderlands of Ukraine's northern, eastern, and south-eastern areas. The initial Russian strategies anticipated a ten-day fighting period to facilitate a presumed annexation of Ukraine by August 2022 (Danylyuk et al., 2022, p. 1). U.S. intelligence holds that Russia anticipated a total seizure of Kyiv within 48 hours (Macias, 2022). However, due to operational security precautions, information distribution within the Russian command chain was poor and limited, and Russian battalion commanders were not informed about the actual orders of mobilization from the forward staging areas into the theatre until merely 24 hours before actions were set to commerce (Danylyuk et al., 2022, p. 26). This led the forces set to engage Kyiv from the north to face poor logistics and challenges to basic command and control. Convoys clogged up on the small roads, and logistical units could not efficiently transport ammunition, fuel and other fundamental materiel to the most forward-deployed units (Jones, 2022, p. 1).

Following the initial phase, Russian forces backed out of the areas of operation around Kyiv, regrouped, and started new offensives from the eastern and southernmost parts of Ukraine, and have by March 2023, successfully been able to control large areas east for the Dnepr-river. By October 2022, Russia announced the complete annexation and integration of the Ukrainian oblasts Zaporizhzhia, Kherson, Luhansk, and Donetsk (Sveen, 2022), as presented in the former figure. As this paper is produced, the Russian operations have changed from an aggressive, expansive land operation to a defensive operation, where the majority of efforts at the tactical level are directed to secure, hold, and defend already seized territory. However, western intelligence assesses that despite the drawbacks in the theatre, Russia still maintains their initial overarching ambition to produce a regime change in Kyiv and secure complete political control over Ukraine (Norwegian Intelligence Service, 2023, p. 6).

Russian information operations

In 2022, as in 2014, Kremlin sought to create a form of pretext, leverage to justify and legitimize coercive action against Ukraine. According to a report by DFRLab (Aleksejeva & Carvin, 2023), released by the Atlantic Council, the most prominent finding of such pretext occurred on February 17th, merely seven days prior to the invasion, as an artillery strike struck a kindergarten in Luhansk. The OSCE's special monitoring mission, on-site in the region to observe the conflict, was not allowed on the premises, and thus unable to assess the direction of fire or the originating weapons system (Aleksejeva & Carvin, 2023, p. 17). The US State Department told the Washington Post it was "unclear if this was an intentional false-flag attack by Donbas separatists" (ibid). RIA Novosti, one of the leading Kremlin-friendly news outlets in Russia, first claimed that Ukraine had admitted to shelling the school, yet stated in a separate report that Luhansk officials had confirmed Ukraine as the originator, and that "any contradictory evidence shared by Ukraine was fake" (ibid).

Aleksejeva & Carvin define this as *narrative warfare*. The process originates in basic terms of political communication – priming and framing. However, the seemingly coordinated process between the Kremlin narrative and the news stories presented by Russian news outlets presents a clear form of influence and propaganda operation, in this case, directed towards a Russian-speaking audience. The attack on the kindergarten became the first story in a series of events that a couple of days later led to the Russian Federation recognizing Luhansk and Donetsk as independent republics, maintaining that Russia, as a regional power, has a responsibility to protect the republics, and did on the 24th of February (Aleksejeva & Carvin, 2023, pp. 23-25), initiate the full-scale invasion, as described in detail in the previous subchapter.

The Google Threat Assessment Group (TAG) maintains that "Moscov has leveraged the full spectrum of Information Operations – from overt state-backed media to covert platforms and accounts – to shape public perception of the war". These operations were directed towards a Ukrainian and Russian audience, to degrade the public trust in the Ukrainian government, fracture international support for Ukraine, and to increase the domestic support in Russia for the war, which facilitates the legitimization process of the operation (Huntley, 2023). Google disrupted more than 1950 instances of Russian Information operation activities on their platforms in 2022, of which more than 90% were in the Russian language (Ibid).

Cyber operations against Ukraine

Several Ukrainian services, both in the private and the governmental sector, have been subject to cyber operations during the 2022 campaign. Many of these attacks are not necessarily attributed to specific agents, but it is plausible to assume that most of this traffic is generated by either Russian state-sponsored actors, Russian intelligence agencies, or private groups with a pro-Russian position. The common issue is that these operations are carried out to degrade the Ukrainians' access to civil services and trust in official institutions, for which all attacks, regardless of origin, serve to support Russian interests in the conflict.

Since the start of the conflict, Russia has launched 12 malicious operations against Ukraine, including government, telecom, finance, media and the energy industry (Huntley, 2023). Over the same period, Russian targeting of Ukrainian users increased by 250% compared to 2020 (Ibid).

Russian cyber operations have also been conducted against critical infrastructure within the Ukrainian AO. These attacks have most dominantly been targeting installations critical to the Ukrainian power grid infrastructure. However, these efforts have seen little effect, which have resulted in such efforts being substituted by kinetical efforts, such as air strikes. This has ultimately diminished the cost-reducing argument of hybrid efforts.

Bateman (2022) elaborates that:

> "Rather than serving in a niche role, many Russian cyber fires have targeted the same categories of Ukrainian systems also prosecuted by kinetic weapons, such as communications, electricity, and transportation infrastructure. For almost all these target categories, kinetic fires seem to have caused multiple orders of magnitude more damage. While cyber fires potentially offer unique benefits in certain circumstances, these benefits have not been realized in Russia's war against Ukraine. Moscow's military strategists quickly discarded any aim of reducing physical or collateral damage or creating reversible effects in Ukraine, and Russia has gained little deniability or geographic reach from cyber operations. Likewise, Russian cyber fires have not achieved any systemic effects, and they have arguably been less cost-effective—or at least more capacity-constrained—than kinetic fires." (Bateman, 2022, p. 2)

6.4.2 The macrolevel – the escalated conflict between Russia and the West

Strategic deterrence

Since an all-time high of NATO scrambles for Russian aircraft in the high north in 2020, the number of Russian aircraft identified has decreased to a number of 43 in 2022, the second lowest number since 2010 (Luftforsvarets Kommunikasjonsenhet (personal communication), 21.11.2022).

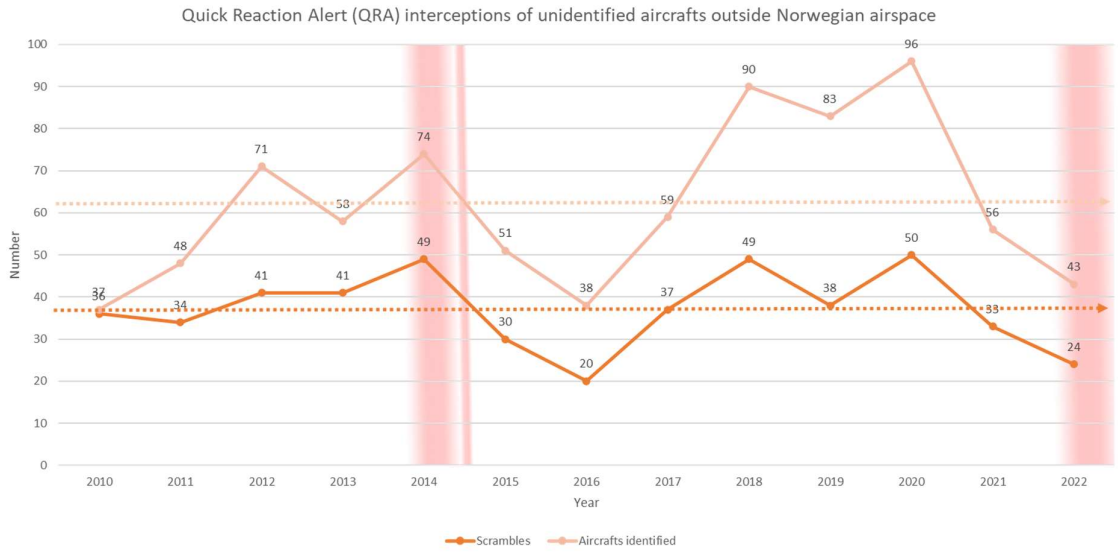


Figure 6.3: QRA scrambles and identifications of Russian aircraft outside Norwegian airspace carried out by the Royal Norwegian Air Force (Data genereated from: Luftforsvarets Kommunikasjonsenhet (personal communication), 21.11.2022; VG, 2015)

The number of identifications of Russian aircraft in 2022 (43) was 40% lower than in 2014, despite the increased area of operations in 2022. To make more accurate comparisons regarding the methods of use during the conflict, the 2022 number of observations is 51% lower than that of 2008, the year of the conventionally fought Russo-Georgian war (VG, 2015). Although exact numbers regarding aircraft types are sensitive and thus undistributable for public dissemination, NATO confirms that the number of strategic bombers is correspondingly reduced compared to the years before the 2022 campaign (NATO AIRCOM (personal communication), 25.01.2023).

The Russian struggles to maintain satisfiable success on the battlegrounds of Ukraine has led to a general fear of an escalation of measures used in the theatre, frightened that Russia will employ tactical nuclear weapons to ensure successful operations in areas where the land forces are yet to maintain control and freedom of movement. The combination of concerns for such application of nuclear weapons (A. T. Andersen, 2022), combined with the Russian

commitment to strategic deterrence, makes it plausible for Moscow to substitute conventional strategic deterrence with an increase in hybrid measures against NATO members, to maintain a reliable threat to NATO involvement in Ukraine, yet avoid uncontrollable escalations which could sparkle effects leading to increased risk for an all-out war between Russia and NATO.

Cyber operations

From February 2022 until February 2023, twenty-three significant cyber incidents attributed to Russian-linked hacking groups were noted. These attacks include operations aimed at sabotage, exploitation, denial of access, intelligence gathering and disruption. The events are spread across NATO and directed at official networks, such as government websites and services, critical infrastructure, such as hospitals and energy-related institutions, and other services, such as financial and postal entities (CSIS, 2023, pp. 2-15).

Although these attacks have been attributed to "Russian-linked" hacker groups, it is difficult to distinguish between state-sponsored cyber operations carried out by government bodies or private groups and cyber-attacks carried out by pro-Russian hacking groups on their own initiative. Google's Threat Analysis Group assess that Russian state-sponsored hacking groups started increasing network operations as early as 2021. Throughout the campaign, Russian targeting of users in NATO countries increased by more than 300% in 2022 compared to 2020 (Huntley, 2023).

In addition to targeting NATO members, Russia is also believed to have pursued malicious network operations against Finland and Sweden, who applied for NATO membership due to the Russian invasion of Ukraine (Canadian Centre for Cyber Security, 2022, p. 4).

Operations within the information, influence, and psychological spectre

Former Russian president, Dmitry Medvedev, currently serving as the deputy chairman of the Russian security council, has launched a series of statements about Western aggression against Russia. One of the points of the former president is that the West has been employing non-governmental organizations (NGOs), such as human rights groups, aid organizations etc., in a malign form to conduct activities of disruption and destabilization of civil society (RT, 2023). However, there are otherwise no specific observations of covert Russian information operations directed towards its surroundings for efforts concerning neither the operations inside the Ukrainian theatre, nor for the territorial defence of Russia.

6.4.5 Unattributed events of hybrid operations outside the Ukrainian theatre

This subchapter is dedicated to provide empirical clarity on observations that could be elements of Russian hybrid efforts from a macro-perspective. It must be emphasized that these observations are not publicly attributed to Russia, making it impossible to draw certain conclusions regarding causality and mechanisms. It must, however, also be mentioned that the nature of such operations facilitates for plausible deniability and that it, in some cases, might not serve strategic purposes to pursue public attribution, as doing so could simply serve the objectives of Russian deterrence operations, if such is the case, by creating chaos and fear with the population, acknowledging such capabilities to reside with the adversary.

Sabotage against critical infrastructure: The sabotage against the Nord Stream pipelines.

The sabotage operations against the Nord Stream pipelines in the Baltic Sea are undeniably the most publicized event of intentional damage towards critical infrastructure during the campaign. Launched in 2015 as an addition to Nord Stream 1, Nord Stream 2 became a politically discussed element in several countries, and the Swedish Armed Forces Research Establishment (FOI) did, already in 2007 with Nord Stream 1, maintain that it could *"change the strategic pattern and be a source of friction as it may rock the regional stability and reduce the potential of the new EU members to become security providers in Europe's northern dimension"*. And that *"the pipeline will also give increased leverage and influence to Russia, a state that has moved in an authoritarian direction under President Putin. In addition, it divides the EU-members into two parts and makes it more difficult to form a common European energy policy"* (Larsson, 2007, p. 1).

Figure 6.4: Map of the Nord Stream infrastructure and incident sites. Source: (Plucinska, 2022)

On September 27th 2022, an unusual depressurization occurred in both Nord Stream 1 and 2, later revealed to be resulting from explosions on the seabed close to the Danish island of Bornholm the day prior (Plucinska, 2022). Swedish official investigations concluded already in November that the explosions were an act of intent (NTB, 2022). News outlets and analysts quickly suggested that Russia was the originator of the hostile actions. Shortly after, CNN cited three sources that Russian navy support ships and submarines had been observed not far away from the sites of the Nord Stream leaks (Plucinska, 2022). However, in February 2023, US journalist Seymour Hersh published an article claiming that the sabotage, in fact, was carried out as a joint US-Norwegian special operation during the NATO exercise BALTOPS 22 (Hersh, 2023).The accusations were quickly dismissed by both US and Norwegian authorities.

Nevertheless, following the incident, Russia has followed a line of denial, as Russian spokesmen have maintained no Russian involvement in the sabotage and pressured for Russian involvement in the official investigations, and after such inquiry was declined, sought to diminish the investigation. Russian authorities have also tried to direct responsibility elsewhere. Amongst others, the United Kingdom has been introduced as an involved party (NRK, 2022)

Minor events of incidents to critical infrastructure during the 2022 campaign

In October 2022, one of the subsea cables providing communication connectivity to the Shetland Islands was disrupted (BBC, 2022a). This happened only a week after a similar cable connecting the Faroe Islands with Shetland went inoperable for similar reasons. The outage left the islands without connectivity, causing disruptions to landlines, mobile phones and broadband services. Although the incident was considered a result of an accident, the outage of two cables in such a short timeframe was described as “rare” (ibid).

During the same month, the Bornholm Island, situated near the Nord Stream sites, were left with a total power outage for almost four hours due to a connectivity error in the subsea cable between the island and the Swedish mainland. According to the connectivity-provider, the error was caused by a voltage error in the gridlines, leading the termination point in Sweden to disconnect the cable for safety reasons (TT-Ritzau, 2022).

Sightings of drones

In the months leading up to the invasion and throughout 2022, a number of drones were observed in the immediate vicinity of critical infrastructure in Scandinavia. The first notifiable observations were done in Sweden in mid-January, when “military-style” large-winged drones were observed over Sweden's Forsmark, Ringhals and Oskarshamn nuclear power plants. Observations of such drones did also include the royal palace and airports (I. Andersen, 2022).

Similar observations were later done near Norwegian offshore installations in the North Sea. The observations were reported on several fields, such as Johan Sverdrup, Gullfaks and Snorre A (I. Andersen, 2022).

7.0 Analysis: How may variants of realism and theories of risk explain the utilization of hybrid means during the Russian campaigns?

7.1 Russian aggressiveness, offensive or defensive by nature?

In the first case, hybrid means are utilized as the primary domain for hostile action. To explain the underlying causes of this, from a realist approach, we must examine the systemic circumstances surrounding the involved states at the given time. Despite the USSR's disintegration, Russia is still considered one of the few great powers in world politics. Russia possesses the greatest arsenal of nuclear weapons by numbers and inherited most of the equipment and material from the Soviet armed forces. However, it is necessary to emphasize the condition of the Russian equipment at the time. The brands of the Russian armed forces did, during the 2000s, suffer from an under-investment in defence expenditure, which inevitably led to a massive maintenance backlog on the already obsolete and ageing Soviet equipment. This was especially prominent during the Russo-Georgian war in 2008 (Crane et al., 2019, pp. 56-57). It is likely to believe that considering the strategic geopolitical localization of Ukraine, not least to say Crimea in particular, in addition to the incumbency of resolute and decisive decision-makers in the West, would have led the Russian strategic elite to consider it a great risk to initiate combat action in the AO. The combination of insufficient Russian combat readiness and a strong collective West could have led to a fear of direct military confrontations on the easternmost borderline of NATO, a confrontation the Russian armed forces at that point could have been considered unable to withstand.

As discussed in the deductive section of this paper, realist theory holds that expansionist action should merely occur if such likely would lead to higher utility than the costs (Labs, 1997, p. 11). If the considerations above are valid, there is no doubt that the risk for failure, with the potential political and economic costs, would have been severe and thus lead to a change of strategies from the Russian decision-makers. This leads to the introduction of hybrid means for foreign political gains. Hybrid means introduce less risk and cost, and it is considered to produce symmetrical countermeasures when encountered and attributed. This means that in a given situation of Russian hybrid warfare, Russia would, considering the assumptions on hybrid warfare, merely face hybrid repercussions, a scenario causing significantly less cost to the Russian armed forces.

At first glance, one might argue that both cases suffer from offensive expansionist tendencies, as both cases are examples of occupation of foreign territory. By such understanding, there is no doubt that the empirical findings of this analysis, with regards to the 2014 campaign, support the first hypothesis on hybrid operations being successful in supporting expansionist strategies of offensive realism. The concept of A2/AD by hybrid means could be argued to be present in Crimea, as the Russian forces gained an information sovereignty, denying Ukrainian free media and Ukrainian authorities access to the domain through traditional communication. This might, as discussed inductively, be considered an overstretch of the original concept of anti-access area denial, however, the changing nature of warfare does incentivise for adaptations of concepts to be made, and is especially important for us while assessing the strategic value and intent behind such efforts.

The Russian aggression may also be seen from a defensive approach. Russia has previously held great influence over the region, which in later decades has abandoned its previous partnerships and shifted towards more westly oriented politics. The former Warszawa-pact countries of the Baltics, Poland, Hungary and Romania have already entered membership into the NATO alliance, and with the Ukrainian Maidan demonstrations, also Ukraine is in a position to assimilate into the Western sphere of influence. Both EU and NATO memberships have been discussed and are desired by the current political administration. There are few doubts about the Russian loss of influence and ability to project power in their former spheres of influence. By revisiting the deduced theory of defensive realism and applying Levy's reference point to the analysis, we can argue that Russia's action in Ukraine, despite expansionist and aggressive, is driven by a Russian need to defend their strategic interests and readjust the power distribution to an equilibrium equal to what was seen during the cold war. This is most prominently seen in Putin's demands towards NATO, urging them to withdraw all multinational battalion groups from NATO's eastern flank (Balmforth & Tétrault-Farber, 2021). It is beyond doubt that Russia is seeking to regain their position in the system and reintroduce an equilibrium they use as its reference point - a *status quo ante*. By such understanding, we may argue that the probability of Russia seeking expansion beyond their traditional spheres of influence is unlikely, and it may therefore be seen as an effort of *security maximation* rather than *power maximation*. The latter is critical for understanding whether the conflict is of defensive or offensive nature. By such interpretation, we may consider Russia's strategy a strategy of defensive realism by such theoretical framework.

By interpreting the aggression as defensive by nature, we may analyse the empirical results towards the second hypothesis. There is no doubt, again, that the 2014 operation was a strategic win for Russia, both by a defensive and offensive approach. From the defensive perspective, the hybrid operation allowed Russia to regain lost territories after the disintegration of the Soviet Union and fortified the Russian presence in the Black Sea region. Further, we can see tendencies to what could be understood as hybrid deterrence during the 2022 campaign, as there is a correlation between hybrid observations and highly reduced numbers of identifications of Russian aircraft in the Bastion region. It must, however, be emphasized that the observations of drones or physical sabotage to critical infrastructure, and a set of other less verifiable incidents, are yet to be readily attributed to Russia. However, the narrative in the general media suggests Russia as the originator, a narrative that supports the Russian strategy. This means that no absolute conclusions could be drawn from this correlation, although this would be a relevant problematization while analysing covert action and efforts supported by plausible deniability. To conclude, if the assumption holds, Russia would have successfully maintained a level of deterrence toward the West yet avoided increasing the risk of nuclear confrontations.

7.2 How well do hybrid operations manifest themselves in foreign political strategic wins?

The two cases, or periods of intensity, in the ongoing Russian campaign in the Ukrainian theatre have given mixed results with regard to success rate and durability. Undoubtedly, the 2014 campaign resulted in a massive Russian success, ultimately leading to the lasting annexation of the Crimean Peninsula. The swift and costless operation produced no direct military confrontation between Russia and the West. The diplomatic reactions in the wake of the operation were primarily a combination of diplomatic condemnation and economic sanctions, arguably the mildest response Russia realistically could have anticipated for such a strategic move.

The 2022 campaign, however, is in its operational nature carried out as a hybrid-enabled multidomain joint operations, where the conventional strategies dominate. However, as presented here, hybrid instruments have also been present *during* the campaign and are to be understood, as inductively introduced, hybrid efforts in support of conventional operations.

It is important to emphasize that the application of hybrid means during the 2022 campaign causes serious inquiry into the successfulness of hybrid operations in large-scale operations. As presented in the previous sections of this case study, Russia has seen limited success in hybrid attacks against critical infrastructure. Cyber operations towards Ukrainian power plants have been highly unprofitable, leading the Russian forces to complement such digital attacks with physical kinetic missile strikes. This means that rather than serving a cost-efficient strategy, it actually induces a *higher cost* than what would result from a sole air campaign.

Undoubtedly, the Russian hybrid efforts in the Ukrainian theatre returned more extensive strategical utility in the 2014 campaign than seen this far in the current campaign. The initial question that appears, however, is whether or not the differences in success are related to strategic deficiencies or temporal problems related to the fact that the conflict has been ongoing for eight years and that Ukraine, as discovered previously, have implemented measures to reduce vulnerability and increase societal resilience.

The strategic problem is related to the size and tactics of the operation. As far as the measures of the 2014 operation largely were aimed directly towards the operational area in question, the hybrid instruments of the 2022 campaign have rather been directed elsewhere, either to legitimize the operation for the domestic audience in Russia or covert power projection towards Western adversaries in a period where conventional or nuclear power projection

might have come across as too excessive. Nevertheless, it is interesting to ask the question as to whether hybrid operations efficiently could serve regime-shifting purposes in more extensive campaigns. However, the limited number of known cases of hybrid operations of this scale limits the possibilities of generalizable conclusions to this question thus far and remains to be answered by future studies applying the refined framework for more in-depth analyses.

The temporal issue corresponds to the methodological problem of this study. There is a highly linked correlation between the 2014 and 2022 cases, which with high confidence, could be presented as a continuum of the same operation. However, the autocorrelation is also present in the strategic outcome of Russian operations and thus is a finding of its own. Russian cyber and information operations in the 2022 campaign are seeing reduced efficiency due to measures taken by the Ukrainian society after the annexation of Crimea. Firstly, Ukrainian companies have invested in higher levels of cyber security, thus increasing the operational cost of malicious cyber operations towards those sectors. Secondly, the Ukrainian society and numerous other Western societies have been made aware of the increased risk of disinformation campaigns, fake news, and bots on social media platforms. This has ultimately led to more resilient recipients for Russian hybrid strategists.

The temporal problem introduces a new aspect to hybrid warfare both as a strategic option and as a strategy of foreign policy; is hybrid warfare limited by a sequential constraint in its operational nature? Conventional operations possess the ability to re-engage previously contested territories, normally after a remobilization or shift of strategies. However, the instruments of hybrid operations appear more limited and simplistic by nature. After a successful cyber operation, the exploited vulnerabilities in the software would be mitigated. Following the general awareness of a disinformation campaign, the audience would continue with greater caution and awareness to the truthfulness of information dissemination. Operations previously conducted as clandestine, covert activities would lose their deniability after the attribution of previous activities in the same area. Although a shift in strategies could lead to continued operational success, it would appear more difficult and may involve higher risk and reduced likelihood of success.

The temporal issue, if at some point proven generalizable and applicable to similar cases, does endorse previous studies of hybrid warfare, that rather than assess hybrid warfare as an isolated and individual strategy of coercive foreign policy, assess hybrid warfare as an integrated part of multidomain warfare. In contrast, the hybrid instruments would dominate

the preface and the initial part of the operation, while the intensity of operations is still at a reduced level, for then to be relieved by traditional modes of military warfare. Diesen (2018) is one of the authors introducing the latter to his morphological study previously discussed in this paper.

7.3 How may we interpret the risk of the operations?

The location of Ukraine, as a flat landscape bridge between Russia and the West, makes it a strategically important area in a geopolitical context. This makes the Type 1 risk highly relevant, as the structural consequences of aggressiveness would not go unnoticed by the adversaries in the system. This could ultimately escalate to involve third-parties, resulting in additional areas of operations, battlespaces and domains. However, this risk of unwanted structural effects is less dominant in the Crimean operation, as the efforts utilized were either covert measures or measures providing ambiguity, such as the application of SOF elements camouflaged as local militia. Above all, the ambiguity and rapidness of the Crimean operation resulted in Russian strategic wins so quickly that the Ukrainians and the structural adversaries of Russia were left with no time to respond. Correspondingly, during the full-scale invasion, hybrid efforts as supportive efforts lost their ambiguity because of the overwhelming overt element of conventional efforts.

There is an entirely different cost aspect related to the two operations. These variations are based on two aspects: Firstly, the Crimean annexation is limited to a smaller geographical area, compared to the full-scale invasion of Ukraine. Although, as Figure 6.2 illustrates, ground combat has primarily occurred in the country's easternmost oblasts. Secondly, there is a large difference in the operational costs between hybrid and multi-domain operations. The combination of these makes the Crimean operation less costly concerning both operational cost and its ambiguity and facilitation of plausible deniability. On the other hand, the full-scale invasion introduces higher operational costs and the risk of unwanted structural secondary effects.

With regards to Type 2 risk, concerning the uncertainty of outcome, hybrid operations suffer from a relatively high uncertainty of outcome concerning the actual effects of the efforts applied. This is related to two aspects of hybrid operations: The role of psychological efforts, and attribution. The psychological aspect presented in efforts related to the political or information domain depends on the receptiveness of the targeted population or group. This receptiveness is hard to presume sufficiently and will lead to some degree of uncertainty of

outcome. The second aspect is related to attribution. As established, hybrid operations tend to apply efforts prone to facilitate some plausibility for the originator. Ambiguity reduces Type 1 risk, but the robustness or timeframe for how long this ambiguity holds is uncertain for the aggressor. This is also related to the intensity of operations, as higher intensity is likely to result in implausibility.

On the other hand, traditional military operations are subject to a long-standing history, both of contemporary and former conflicts. Russia has previously carried out small- and large-scale operations, most recently in Georgia in 2008. The experiences and lessons from these are considered while the risks and uncertainty are assessed for future operations. Also, war gaming is a widespread tool to simulate outcomes and uncertainty of success. The combination of simulations and previous lessons learned makes it easier to presume uncertainty of outcome or success with conventional, as opposed to hybrid operations.

Overall, we may assess that the Type 1 risk was less in the Crimean operation than in the full-scale invasion, as the operational costs were less, and ambiguity was sufficiently held until operational success was accomplished. However, the Type 2 risk was likely greater, due to greater uncertainty of outcome related to the hybrid operation than the most likely pre-simulated full-scale invasion in 2022. The question remains whether the simulated risk related to the latter was coherent with the observed outcome and if this calls for an assessment of risk-willingness on an individual level, which would be outside the scope of this format.

The third hypothesis, H3, holds that "*States would pursue hybrid rather than conventional strategies in offensive operations when Type 1 risks introduce serious inquiries about the profitable utility of the operation".* If the risk assessment in the previous paragraph holds, it would likely present lower Type 1 risks to engage with hybrid operations rather than a majority of conventional efforts. However, the fact that Russia still moved forward with conventional efforts does reject the third hypothesis in the 2022 case. The reason for this could either lay in greater presumed utility through conventional efforts concerning the projected uncertainty in Type 2 risks or be related to concerns on the individual level, which would call for irrational behaviour not explained by the theories applied in this thesis.

7.4 What does the empirical observations say about the intensity of the operations?

The following analysis of the intensity of the operations is limited due to its format as a pilot study. However, we may analyse the readily observable events to assess the intensity of both operations. In a larger format with a different scope, such intensity analysis would benefit from a semi-quantitative analysis.

During the Crimean annexation, we can see that the operation commenced over a short timeframe, from initial disruptions until the votation of the Crimean parliament. This effectively means that all events described in the empirical study were executed in a highly simultaneous or synchronous effort, which, following Figure 3.2 demonstrates a high level of intensity. Also, the severity of some of the efforts could be defined as high. Examples of this are the use of special force elements, which effectively took control of the parliament and secured high-value installations.

To compare, the hybrid efforts during the full-scale invasion in 2022 have been of lower intensity. The enabling and supportive efforts in Ukraine have seen little success, which effectively have led hybrid efforts, such as cyber-attacks, instead of being substituted by conventional efforts, such as air strikes. Russian disinformation campaigns during the operation, primarily directed towards a Russian-speaking audience, have been of relatively high intensity but have not been substantially synchronous with other hybrid efforts directed at similar targets. The observations of plausible hybrid efforts directed towards the West are, at this moment, unattributional and thus out of the scope for a proper analysis until officially attributed. If analysed, however, each event demonstrates the ability to sabotage critical infrastructure with serious potential damage – thus, high intensity. The Nord Stream event, acknowledged to be intended, yet not officially attributed, is an excellent example of a single high-intensity hybrid effort.

Part 5

Recommendations and Final Conclusion

8.0 Towards a refined framework for the understanding of hybrid operations for foreign policy analysis.

The benefit of the plausible probe research design is that it allows the writer to revisit his design after testing it and assess prominent changes to how the empirical study shows areas of possible improvement.

The empirical analysis finds that hybrid elements were used in different manners concerning the 2014 and 2022 campaigns. Whereas the 2014 campaign was strictly hybrid, the hybrid element served as an enabling and supportive effort through the 2022 campaign. The fact that these cases, depending on situational understanding, could be interpreted as defensive by nature. In Russia's case, these operations have been conducted into a semi-friendly operational environment. It goes without saying that there have been beneficial conditions for hybrid efforts to succeed, and there is no guarantee that such efforts would have proven successful in similar manners while deployed into a more hostile environment. As the empirical pilot study to this thesis is only a testing environment for the framework, and thus not generalizable for certain conclusions to be made. However*, it would likely be appropriate to lower the expectations as to what we can expect hybrid operations to deliver on*.

From the empirical testing, we observe that both newly introduced concepts in Part 2 operationalized for a hybrid context, A2/AD and deterrence, have been observed in the cases, proving prominent for additional testing in a more ambitious testing environment with a more significant number of cases. However, it should be noted that these adaptations are subject to the author's own assessment of how much, or in what directions, the original military concepts may be derived. They would benefit heavily from being recognized by either more academics or official institutions.

The empirical study shows that, although the concept is testable with primarily systemic theories, the output is limited, and it appears that the concept would benefit from being tested for multi-level analysis featuring more variables subject to foreign policy analysis rather than more standard international politics systemic variables. There are two reasons for this. Firstly, hybrid operations offer a new toolbox, and the fact that observations of such utilization are scarce is thus open to various explanations. The main benefits, which go beyond measurable

variables for systemic theories, are the legitimation and cost perspectives. However, as done in this study, these are interpreted as part of the utility equation, which features as the primary variable, especially in offensive realism, deciding whether aggressiveness is profitable. These variables deserve a more comprehensive analysis and understanding, and this is beyond the framework put forward by systemic theories. A refined framework should therefore include the process for foreign political decision-making.

Another important aspect found in this particular pilot study is that the efforts are leaning heavily on a feasible environment, as mentioned earlier. This leads particularly back to the societal level and leads the study into a behavioural and psychological direction. This is prominent for the information and political domains, which maybe, alongside the cyber domain, are the *presumed* driving elements for the overall operation. It is also found that Russian cyber measures were relatively abundant in the first campaign and suffered heavily in the second campaign. A more detailed study should examine whether or not this was a capability, capacity, or resilience problem. This is important for the greater understanding of hybrid conflicts because it, in its nature, is ever developing, and capabilities seen fit 10-15 years ago when Hoffman and others laid the foundation for the concept may not see fit for contemporary conflicts, as infrastructure and societies have sought to either resolve vulnerabilities or to grow more resilient structures. If this is the case, then the utility and risk equation is due for review as to whether hybrid efforts are beneficial for strategies of aggression and subversive and coercive foreign policy.

In short, I believe the framework should include more unit-level variables, and in-depth analysis of the various levels, to analyze conditions favouring or abandoning hybrid strategies, both with the adversary and the aggressor. However, such an analysis would have been out of format for this thesis and would demand a more extensive scope and format, with a multilevel – multiple case analysis. For instance, theories fitting for such an analysis could be presented by Fearon (1998), who combines systemic and domestic variables in his model.

8.0 Main contributions and findings of the thesis:

The thesis has contributed to the research field in both conceptual, theoretical and analytical manners. The contributions vary in importance, but as the concept lacks comprehensive and in-depth research, the conceptual contributions might be of highest significance to the field. The most significant contributions may briefly be summarized as such:

Conceptual contributions:

- Explained and differentiated between the terms Hybrid Operations, Hybrid War, Hybrid Warfare and the Greyzone, terms understood to be misused interchangeably in contemporary literature.
- This thesis has differentiated between various modes of hybrid operations, distinguished by certain thresholds to identify a variety of operational environments such efforts may be deployed into.
- Established that it is not only the actions themselves that influence the fluid presence within each operational environment – it is also highly dependent on the responses and perceptions of the receiving entity.
- Identified various instruments from existing literature and compiled each instrument into a typology of hybrid efforts distinguished by its domain.
- Determined ways of measuring the intensity of hybrid operations.
- Successfully adapted concepts of traditional military doctrine, deterrence and A2/AD, into a hybrid context.
- Created an overall taxonomy of the dynamics between hybrid instruments and their function in each operational environment of the theatre, as well as illustrated the intensity of operation may vary within an operational environment, and the escalatory hierarchy of such.

Theoretical contributions and findings:

- Established how hybrid operations may be explained theoretically by the systemic theories of offensive and defensive realism, especially supported by new concepts of hybrid operations.
- Integrated risk theory to amplify the benefits of hybrid measures for the SPM in foreign policy making and to emphasize how hybrid operations may allow for aims to be made where conventional strategies previously would have been deemed too risky to pursue.
- Found that a framework of hybrid operations for FPA needs inclusion of variables at all levels, especially in-depth analyses of decision-making processes and the society of both the aggressor and the target population.

Empirical findings:

- Observations, either directly inside the theatre or in the strategic areas of the aggressor, could be identified as hybrid deterrence and hybrid A2/AD.
- Structural theories of both offensive and defensive realism could explain both cases, yet defensive realism is likely to achieve greater explanatory power if more domestic variables were introduced.
- The availability of hybrid measures reduced both costs and risks during the annexation of Crimea in 2014.
- Hybrid efforts of enablement and subsequently supportive operations were present during the multi-domain invasion of Ukraine in 2022.
- Temporal issues diminished the effects of hybrid efforts in 2022, emphasizing the argument of limitations in hybrid strategies.
- Found that the ambition-level of hybrid operations need more research, as to whether or not such efforts alone could achieve expansionist strategies in larger AOs.

9.0 Conclusion

Hybrid operations in our time have proven that the lines between civil society and the battlespace of interstate conflict is ever-blurring. As seen in this thesis, even modern military combat is fought in the civil spheres of our lives, not necessarily with aircraft and infantry units, but with disinformation and sabotage. These actions are not directed at diminishing an adversary's military capabilities. Instead, it is aimed at our private spheres and the institutions and framework that hold our society together, from our basic needs to societal culture and coherence. This shift in contemporary conflicts is not to be taken lightly and is due for a more comprehensive analysis and understanding than previous studies have undertaken. Its implication, if realized in full-scale, could be impeccable to our way of living and how the digital tools that surround us could be shifted from an everyday aid to a fearful tool that could be used against us. What information are we to trust? How do we maintain our trust in governmental institutions while adversaries seek to polarize, disinform and disintegrate our societal unity? Last but not least, while this concept is already utilized for aggressiveness, how may we integrate it to augment and strengthen the foreign policy strategies of our own?

This thesis has sought to grasp the concept of hybrid operations, inductively introduce new concepts that seem fit for further analysis as elements of such operations and integrate this concept into the frames of foreign policy analysis. The design and methodology applied to manage such a task have been the plausible probe design, a design feasible for early framework development, as it features both inductive and deductive analysis to be tested in a benign environment. In such, the empirical observations are believed to provide us with a deeper understanding as to whether the early structures of the concept is sufficiently feasible for wide-spread testing for generalizable results and conclusions, or if the framework does not hold adequately, make use of the lessons learned from the pilot-testing to suggest proper improvements for future adjustments to the framework. As seen in the previous section, there are arguments to support a revisit of the theories applied to the framework. As hybrid operations are directed towards the civilian society to a much larger extent than traditional warfare and serve beneficially to steps in the decision-making process as well, it proves necessary to include domestic variables, increasing the explanatory power of the framework and providing a deeper understanding of the connection between the phenomenon and the state through a multilevel analysis.

Literature

Alba, D. (2022). Russia has been laying groundwork online for a 'false flag' operation, misinformation researchers say. *The New York Times*, https://www.nytimes.com/2022/02/19/business/russia-has-been-laying-groundwork-online-for-a-false-flag-operation-misinformation-researchers-say.html

Aleksejeva, N., & Carvin, A. (2023). *Narrative Warfare - How the Kremlin and Russian News Outlets Justified a War of Aggression against Ukraine*. A. Council. https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Narrative-Warfare-Final.pdf

Andersen, A. T. (2022, 16.11.2022). Vil Russland bruke atomvåpen i Ukraina? Bekymringen kan både overdrives og underdrives. *Aftenposten*, https://www.aftenposten.no/meninger/kronikk/i/RGjmlO/vil-russland-bruke-atomvaapen-i-ukraina-bekymringen-kan-baade-overdrives-og-underdrives

Andersen, I. (2022, 30.09.2022). Nye droneobservasjoner i Nordsjøen. *Teknisk Ukeblad*. https://www.tu.no/artikler/nye-droneobservasjoner-i-nordsjoen/522629

Baisotti, V., Hetland, K., Olsen, A. N., Olsson, S. V., Ulvin, P. B., & Øvrebø, E. F. (2022, 30.09.2022). Sjøforsvaret: – Vi går fra en fredelig tilværelse til en mer skjerpet situasjon. https://www.nrk.no/norge/nye-droneobservasjoner-i-nordsjoen-1.16122628

Baker, J. (2019). The Empathic Foundations of Security Dilemma De‐escalation. *Political psychology*, *40*(6), 1251-1266. https://doi.org/10.1111/pops.12623

Balmforth, T., & Tétrault-Farber, G. (2021, 17.12.2021). Russia demands NATO roll back from East Europe and stay out of Ukraine. *Reuters*, https://www.reuters.com/world/russia-unveils-security-guarantees-says-western-response-not-encouraging-2021-12-17/

Barry, E. (2022, 18.01.2022). These Are the Countries Where Twitter, Facebook and TikTok Are Banned. *TIME*. https://time.com/6139988/countries-where-twitter-facebook-tiktok-banned/

Bateman, J. (2022). Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. *CYBER CONFLICT IN THE RUSSIA-UKRAINE WAR*. https://carnegieendowment.org/files/Bateman_Cyber-FINAL21.pdf

BBC. (2022a, 20.10.2022). Damaged cable leaves Shetland cut off from mainland. *BBC*, https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-63326102

BBC. (2022b, 28.01.2022). Ukraine crisis: Don't create panic, Zelensky tells West. *BBC*, https://www.bbc.com/news/world-europe-60174684

Benjaminsen, H. (2022, 23.05.2022). Slipper håndgranater fra minidroner. *NRK*, https://www.nrk.no/urix/slipper-handgranater-fra-minidroner-1.15975176

Bergh, A. (2020). *Påvirkningsoperasjoner i sosiale medier - oversikt og utfordringer*. Forsvarets Forskningsinstitutt.

https://www.ffi.no/publikasjoner/arkiv/pavirkningsoperasjoner-i-sosiale-medier-oversikt-og-utfordringer

Bresinsky, M. (2016). UNDERSTANDING HYBRID WARFARE AS ASYMMETRIC CONFLICT: SYSTEMIC ANALYSIS BY SAFETY, SECURITY AND CERTAINTY. *On - line Journal Modelling the New Europe*(21), 29-51. https://www.proquest.com/scholarly-journals/understanding-hybrid-warfare-as-asymmetric/docview/1872206522/se-2

Breuning, M. (2007). *Foreign Policy Analysis : A Comparative Introduction* (1st 2007. ed.). Palgrave Macmillan US : Imprint: Palgrave Macmillan.

Breuninger, K., & Wilkie, C. (2022). White House warns that Russia could invade Ukraine within days, urges Americans to leave. *CNBC*, https://www.cnbc.com/2022/02/11/white-house-warns-russia-could-invade-ukraine-during-olympics-urges-americans-to-leave.html

Bureiko, N., & Moga, T. L. (2019). The Ukrainian-Russian Linguistic Dyad and its Impact on National Identity in Ukraine. *Europe-Asia Studies*, *71*(1), 137-155. https://doi.org/10.1080/09668136.2018.1549653

Canadian Centre for Cyber Security. (2022). *CYBER THREAT BULLETIN: Cyber Threat Activity Related to the Russian Invasion of Ukraine*. Canadian Centre for Cyber Security Retrieved from https://cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf?fbclid=IwAR2XViWnHTFEZf3FGLIBIme85QGwj-4F2DbN0mP1bO2T8x20MkK5CzhbXOg

Chen, T. M. (2010). Stuxnet, the real start of cyber warfare? Editor's Note. *IEEE network*, *24*(6), 2-3. https://doi.org/10.1109/MNET.2010.5634434

Chiacu, D., & Mohammed, A. (2014, 07.02.2014). Leaked audio reveals embarrassing U.S. exchange on Ukraine, EU. *Reuters*, https://www.reuters.com/article/us-usa-ukraine-tape-idUSBREA1601G20140207

Clausewitz, C. v., Howard, M., Paret, P., & Heuser, B. (2007). *On war*. Oxford University Press.

Cormac, R., & Aldrich, R. J. (2018). Grey is the new black: covert action and implausible deniability. *International affairs (London)*, *94*(3), 477-494. https://doi.org/10.1093/ia/iiy067

Crane, K., Oliker, O., & Nichiporuk, B. (2019). *Trends in Russia's Armed Forces: An Overview of Budgets and Capabilities*. RAND Corporation. https://doi.org/10.7249/RR2573

CSIS. (2023). *Significant Cyber Incidents Since 2006*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230404_Significant_Cyber_Events.pdf?VersionId=3UxjuqXLPluSCUtSXhGM1ZecgewJ4wPI

Cullen, P. J., & Reichborn-Kjennerud, E. (2017). *Understanding Hybrid Warfare - A Multinational Capability Development Campaign project*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Danielsen, J. (2022). *Foreign politics of hybrid operations: Reviewing and conceptualizing a nascent field of research*. Norwegian University of Science and Technology. https://1drv.ms/b/s!AmtqVvb6lOqLgdQ0IEdUn1BPEAI9yA?e=lpPoFw

Danylyuk, O. V., Reynolds, N., Watling , J., & Zabrodskyi, M. (2022). Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022. Retrieved 03.03.2023, from https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf

DeBenedictis, K. (2021). *Russian 'hybrid Warfare' and the Annexation of Crimea: The Modern Application of Soviet Political Warfare*. I.B. Tauris. https://books.google.no/books?id=3rxJzgEACAAJ

Diesen, S. (2018). *Lavintensivt hybridangrep på Norge i en fremtidig konflikt*. Forsvarets Forskningsinstitutt. https://publications.ffi.no/nb/item/asset/dspace:4175/18-00080.pdf

DSB. (2019). *Analyser av krisescenarioer 2019*. Direktoratet for Samfunnssikkerhet og Beredskap, Justisdepartementet. https://www.dsb.no/globalassets/dokumenter/rapporter/risikoanalyse-av-cyberangrep-mot-ekom-infrastruktur.pdf

Eckstein, H. (1975). *"Case Study and Theory in Political Science." in Handbook of Political Science, Volume 7: Strategies of Inquiry*.

Etterretningstjenesten. (2021). *Fokus 2022 - Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Forsvarsdepartementet. https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus-2022-til-web.pdf/_/attachment/inline/ec6bec00-d2d3-41c0-af08-02b3b494e8b7:e4014ab4d0e3bd8b2509e7974430fe121e0473ba/Fokus-2022-til-web.pdf

European Commission, Directorate-General for Communications Networks, C., & Technology. (2018). *A multi-dimensional approach to disinformation : report of the independent High level Group on fake news and online disinformation*. Publications Office. https://doi.org/doi/10.2759/739290

Farwell, J. P. (2020). *Information Warfare*. Quantico, VA: Marine Corps University Press (MCUP).

Farwell, J. P., & Rohozinski, R. (2012). The New Reality of Cyber War. *Survival (London)*, *54*(4), 107-120. https://doi.org/10.1080/00396338.2012.709391

Fearon, J. D. (1998). DOMESTIC POLITICS, FOREIGN POLICY, AND THEORIES OF INTERNATIONAL RELATIONS. *Annual Review of Political Science*, *1*(1), 289-313. https://doi.org/10.1146/annurev.polisci.1.1.289

Fermann, G. (2013). *Utenrikspolitikk og norsk krisehåndtering*. Cappelen Damm akademisk.

Fermann, G. (2022). Foreign Politics of Caveats in Coalition Operations: Empirical Research Program. In.

Financial Times. (2023). Russia's invasion of Ukraine in maps — latest updates. *Financial Times*, https://www.ft.com/content/4351d5b0-0888-4b47-9368-6bc4dfbccbf5

Fraioli, P. (2022). The US Army's multi-domain-operations doctrine. *Strategic Comments*, *28*(8), i-ii. https://doi.org/10.1080/13567888.2022.2153499

Freyberg-Inan, A., Harrison, E., & James, P. (2009). *Rethinking realism in international relations : between tradition and innovation*. Johns Hopkins University Press.

Fridman, O., Kabernik, V., & Pearce, J. C. (2019). *Hybrid conflicts and information warfare : new labels, old politics*. Lynne Rienner Publishers.

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). The landscape of hybrid threats: a conceptual model : public version. *30585*. (EUR)

Giles, K. (2016). *The Next Phase of Russian Information Warfare*. https://stratcomcoe.org/publications/download/keir_giles_public_20-05-2016.pdf

Gomm, R., Hammersley, M., & Foster, P. (2009). *Case Study Method* https://doi.org/10.4135/9780857024367

Hersh, S. (2023, 08.02.2023). How America Took Out The Nord Stream Pipeline. https://seymourhersh.substack.com/p/how-america-took-out-the-nord-stream

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies Arlington.

Holden, S. (2016). *Makroøkonomi*. Cappelen Damm akademisk.

Huntley, S. (2023). *Fog of war: how the Ukraine conflict transformed the cyber threat landscape*. Google Threat Analysis Group. Retrieved 26.02.2023 from https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/?fbclid=IwAR0pKj6ov8CxVIwALJvPOVrK2ojCKvFzxt7vLslii2P_HAiiE99FOsXfwNA

Hutchinson, W. (2006). Information warfare and deception. *Informing science*, *9*, 213-223. https://doi.org/10.28945/480

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, innovation and technology*, *9*(2), 159-189. https://doi.org/10.1080/17579961.2017.1377914

Ivanova, P., Manson, K., Politi, J., & Sevastupolo, D. (2021, 04.12.2021). US says Russia could invade Ukraine in early 2022. *Financial Times*, https://www.ft.com/content/90873607-8a8a-48fb-8cb0-3414e277bf25

Jaitner, M., & Mattsson, P. A. (2015). Russian Information Warfare of 2014. *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*.

https://www.ccdcoe.org/uploads/2018/10/Art-03-Russian-Information-Warfare-of-2014.pdf

Jakobsen, T. G., & Mehmetoglu, M. (2022). *Applied statistics using stata : a guide for the social sciences* (Second edition. ed.). SAGE Publications.

Jervis, R., Sears, D. O., & Huddy, L. (2003). *Oxford handbook of political psychology*. Oxford University Press.

Jones, S. G. (2022). Russia's Ill-Fated Invasion of Ukraine - Lessons in Modern Warfare. Retrieved 04.03.2023, from https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220601_Jones_Russia%27s_Ill-Fated_Invasion_0.pdf?VersionId=Ggqjb.JsRbJzr_wlu5jrVT_Xe3AW3jur

Kaunert, C., & Wertman, O. (2020). The securitisation of hybrid warfare through practices within the Iran-Israel conflict - Israel's practices to securitize Hezbollah's Proxy War. *Security and defence quarterly*, *31*(4), 99-114. https://doi.org/10.35467/sdq/130866

King, G., Keohane, R. O., Verba, S., & Keohane, R. O. O. (1994). *Designing Social Inquiry : Scientific Inference in Qualitative Research*. Princeton University Press.

Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., & Oberholtzer, J. (2017). *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. RAND Corporation. https://doi.org/10.7249/RR1498

Kolb, R. (2017). *The International Law of State Responsibility: An Introduction*. Edward Elgar Publishing. https://doi.org/10.4337/9781786434715

Kovalev, A. (2021). The political economics of news making in Russian media: Ownership, clickbait and censorship. *Journalism (London, England)*, *22*(12), 2906-2918. https://doi.org/10.1177/1464884920941964

Kvam, I. H.-p. (2021). Bastionforsvaret og Russlands militærmakt - Et utdatert trusselbilde? *NUPI Policy Brief*, *2/2021*. https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2738224/NUPI_Policy_Brief_2_2021_Kvam.pdf?sequence=2&isAllowed=y

Labs, E. J. (1997). Beyond victory: Offensive realism and the expansion of war aims. *Security studies*, *6*(4), 1-49. https://doi.org/10.1080/09636419708429321

Larson, E. V., Darilek, R. E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L. H., & Thurston, C. Q. (2009). *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*. Santa Monica: RAND Corporation, The.

Larsson, R. L. (2007). *Nord Stream, Sweden and Baltic Sea Security*. T. forskningsinstitut. https://foi.se/rest-api/report/FOI-R--2251--SE

Levy, J. S. (1987). Declining Power and the Preventive Motivation for War. *World Politics*, *40*(1), 82-107. https://doi.org/10.2307/2010195

Levy, J. S. (2008). Case Studies: Types, Designs, and Logics of Inference. *Conflict management and peace science*, *25*(1), 1-18. https://doi.org/10.1080/07388940701860318

Luftforsvarets Kommunikasjonsenhet (personal communication). (21.11.2022). In J. Danielsen (Ed.).

Macias, A. (2022, 08.03.2022). U.S. intel chiefs warn Congress that Putin will 'double down' in Ukraine as Kremlin's war drags on. https://www.cnbc.com/2022/03/08/us-intel-chiefs-warn-putin-will-double-down-in-ukraine.html

Martin, R. (2023). false flag. In *Encyclopedia Britannica*.

Maxwell, J. A. (2005). *Qualitative research design : an interactive approach* (2nd ed., Vol. vol. 41). Sage Publications.

Mearsheimer, J. J. (2001). *The tragedy of Great Power politics*. Norton.

Moore, C. (2019). *Russia and Disinformation: Maskirovka*. C. C. f. R. a. E. o. S. Threats. https://crestresearch.ac.uk/download/2409/19-024-01.pdf

Moses, J. W., & Knutsen, T. L. (2012). *Ways of knowing : competing methodologies in social and political research* (2nd ed.). Palgrave Macmillan.

Mueller, R. S. (2019). *Report On The Investigation Into Russian Interference In The 016 Presidential Election*. Washington, D.C. Retrieved from https://www.justice.gov/archives/sco/file/1373816/download

NATO. (2023). *NATO's response to hybrid threats*. North Atlantic Treaty Organization. Retrieved 05.03.2023 from https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO AIRCOM (personal communication). (25.01.2023). In J. Danielsen (Ed.).

NCSC, U. (2022, 01.10.2022). *NCSC Annual Review 2022*. UK National Cyber Security Centre. Retrieved 18.03.2023 from https://www.ncsc.gov.uk/collection/annual-review-2022/threats-risks-and-vulnerabilities/state-threats

Norberg, J. (2014). The Use of Russia's Military in the Crimean Crisis. Retrieved 27.05.2023, from https://carnegieendowment.org/2014/03/13/use-of-russia-s-military-in-crimean-crisis-pub-54949

Norges Bank. (2021). *Kunderetta betalingsformidling 2020*. Norges Bank. https://www.norges-bank.no/contentassets/b29d4d26c2f34625917b06392f44021d/memo_2_21_betalingsformidling.pdf?v=05/19/2021161656&ft=.pdf

Norges Bank. (2022). *Finansiell Infrastruktur*. Norges Bank. https://www.norges-bank.no/contentassets/7437af41dbd94dbfaee9e7f0d231a3ba/finansiellinfrastruktur_2022.pdf?v=08/08/2022123229&ft=.pdf

Norwegian Intelligence Service. (2023). *FOKUS 2023 - Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Retrieved from

https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf/_/attachment/inline/c1a9a458-aa1d-4bf6-a558-9cec57acde8f:9b2050d897a2b2db1bddc8e505db7b666e608b98/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf

NRK. (2022, 21.12.2022). Russland klager på Nord Stream-etterforskningen. *NRK*, https://www.nrk.no/nyheter/russland-klager-pa-nord-stream-etterforskningen-1.16229256

NTB. (2022, 15.01.2022). Stor drone observert over svensk atomkraftverk. *Teknisk Ukeblad*, https://www.tu.no/artikler/stor-drone-observert-over-svensk-atomkraftverk/516540

OECD. (2022). Disinformation and Russia's war of aggression against Ukraine: Threats and governance response. *Policy Responses: Ukraine Tackling the Policy Challenges*. Retrieved 19.03.2023, from https://www.oecd-ilibrary.org/docserver/37186bde-en.pdf?expires=1679237832&id=id&accname=guest&checksum=A0ECF5644701849B35AE6EF7040E84CB

Perkins, D. G. (2017). Multi-domain battle: driving change to win in the future. *Military review*, *97*(4), 6.

Plokhy, S. (2015). *The gates of Europe : a history of Ukraine*. Allen Lane.

Plucinska, J. (2022, 06.10.2022). Nord Stream gas 'sabotage': who's being blamed and why? *Reuters*, https://www.reuters.com/world/europe/qa-nord-stream-gas-sabotage-whos-being-blamed-why-2022-09-30/

Przetacznik, J. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Quinlivan, J. T., & Oliker, O. (2011). *Nuclear Deterrence in Europe: Russian Approaches to a New Environment and Implications for the United States*. Santa Monica: RAND Corporation. https://doi.org/10.7249/mg1075af

RadioFreeEurope. (2015, 02.02.2015). Lavrov Claims Obama's Remarks Prove U.S. Backed Ukraine 'Coup. *RadioFreeEurope*, https://www.rferl.org/a/obama-russia-lavrov-coup-ukraine/26826632.html

Ringstrom, A. (2022, 15.01.2022). Swedish police hunt for drone seen flying over Forsmark nuclear plant. *Reuters*, https://www.reuters.com/world/europe/swedish-police-hunt-drone-seen-flying-over-forsmark-nuclear-plant-2022-01-15/

Rose, G. (1998). Neoclassical Realism and Theories of Foreign Policy. *World Pol*, *51*(1), 144-172. https://doi.org/10.1017/S0043887100007814

RT. (2023, 17.02.2023). NGOs are weapons in 'hybrid war' – ex-Russian president. *Russia Today*, https://www.rt.com/russia/573136-ngo-weapons-hybrid-war/

Rusnáková, S. (2017). Russian New Art of Hybrid Warfare in Ukraine. *Slovak Journal of Political Science*, *17*(3-4), 343-380. https://doi.org/10.1515/sjps-2017-0014

Russel, A. L. (2015). Strategic Anti-Access/Area Denial in Cyberspace. *2015 7th International Conference on Cyber Conflict*. Retrieved 01.02.2023, from https://ccdcoe.org/uploads/2018/10/Art-11-Strategic-Anti-Access-Area-Denial-in-Cyberspace.pdf

Schneider, J. (2019). The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war. *Journal of strategic studies*, *42*(6), 841-863. https://doi.org/10.1080/01402390.2019.1627209

Schweller, R. (1996). Neorealism's status-quo bias: What security dilemma? *Security studies*, *5*, 90-121. https://doi.org/10.1080/09636419608429277

Shulman, S. (1999). The cultural foundations of Ukrainian national identity. *Ethnic and racial studies*, *22*(6), 1011-1036. https://doi.org/10.1080/014198799329224

Slotten, A. (2022, 11.12.2022). Kan Kina bruke TikTok til å manipulere oss? *NRK*, https://www.nrk.no/norge/kan-kina-bruke-tiktok-til-a-manipulere-oss_-1.16209209

Snyder, G. H. (2002). Mearsheimer's World-Offensive Realism and the Struggle for Security: A Review Essay. *International security*, *27*(1), 149-173. https://doi.org/10.1162/016228802320231253

Statista. (2023, 24.03.2023). *Leading social media platforms in Russia in 3rd quarter 2022, by monthly penetration rate*. Retrieved 25.04.2023 from https://www.statista.com/statistics/867549/top-active-social-media-platforms-in-russia/

Steen, J. (2022, 27.10.2022). Stanset flytrafikken etter dronemeldinger. *TV2*, https://www.tv2.no/direkte/jpybz/siste-nytt/635ab7841be5231186fc7719

Sveen, S. L. (2022, 04.10.2022). Russlands parlament har formelt godkjent annekteringen. *VG*, https://direkte.vg.no/krig-i-ukraina/news/russland-har-ratifisert-annekteringen-av-fire-ukrainske-regioner.3O86h2EK1

Svenonius, O. (2022). *Countering Mis- and Disinformation – A Narrative Review of Reactive Measures*. T. forskningsinstitut. https://foi.se/rest-api/report/FOI-R--5263--SE

Sysselmesteren på Svalbard. (2022). SvalbardROS 2022-2026 - En analyse av risiko og sårbarhet på Svalbard. Retrieved 01.02.2023, from https://www.sysselmesteren.no/siteassets/samfunnssikkerhet-og-beredskap/svalbardros-2022-2026.pdf

Taliaferro, J. W. (2001). Security seeking under anarchy : defensive realism revisited. *International security (trykt utg.). 25 : 2000 : 3*, S.128-161.

Thyne, C. L. (2010). Supporter of stability or agent of agitation? The effect of US foreign policy on coups in Latin America, 1960-99. *Journal of peace research*, *47*(4), 449-461. https://doi.org/10.1177/0022343310368350

TT-Ritzau. (2022, 10.10.2022). Strömmen tillbaka på Bornholm. *Aftonbladet*, https://www.aftonbladet.se/nyheter/a/8JQaXW/hela-bornholm-utan-strom

Tuncer, O. S. T., & Erkut, F. N. (2022). Ukraine's Balance Policy between European Union and Russia. *Acta politica polonica*, *54*, 95-113. https://doi.org/10.18276/ap.2022.54-07

Törnquist-Plewa, B., & Yurchuk, Y. (2019). Memory politics in contemporary Ukraine: Reflections from the postcolonial perspective. *Memory studies*, *12*(6), 699-720. https://doi.org/10.1177/1750698017727806

UK Ministry of Defence. (2019). *Deterrence: the Defence Contribution*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860499/20190204-doctrine_uk_deterrence_jdn_1_19.pdf

CHARTER OF THE UNITED NATIONS, (1945). https://treaties.un.org/doc/publication/ctc/uncharter.pdf

US Army. (2008). *Army Special Operations Forces Unconventional Warfare*. US Army Publishing Directorate Retrieved from https://irp.fas.org/doddir/army/fm3-05-130.pdf

US Army. (2010). *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance On-the-Mo*. Retrieved 01.02.2023 from https://www.army.mil/article/40089/command_control_communications_computers_intelligence_surveillance_and_reconnaissance_on_the_mo

US Army. (2021a). *Field Manual Operational Terms*. US Army Publishing Directorate Retrieved from https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34799-FM_1-02.1-000-WEB-1.pdf

US Army. (2021b). *FM 3-12 CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE*. US Army Publishing Directorate Retrieved from https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN33127-FM_3-12-000-WEB-1.pdf

US Army. (2022). *FM 3-0 Operations*. US Army Publishing Directorate Retrieved from https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf

US Army Cyber Command. (2022). *Factsheet: Cybersecurity Terminology*. Retrieved 01.02.2023 from https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/2686075/cybersecurity-terminology/

Vaczi, N. (2016). *Hybrid Warfare: How to Shape Special Operations Forces*.

Vasquez, J. A. (2009). *The war puzzle* (Vol. 27). Cambridge University Press.

Veibäck, E., Stenérus Dover, A.-S., & McWilliams, A. (2021). *Gråzonsproblematik och hybrida hot i transportsystemet*. T. forskningsinstitut. https://www.foi.se/rest-api/report/FOI-R--5118--SE

Ven Bruusgaard, K. (2016). Russian Strategic Deterrence. *Survival*, *58*(4), 7-26. https://doi.org/10.1080/00396338.2016.1207945

VG. (2015, u.d.). Russiske fly identifisert av norske F-16. *VG*, https://www.vg.no/spesial/2015/forsvaret-f16/identifiseringer.html

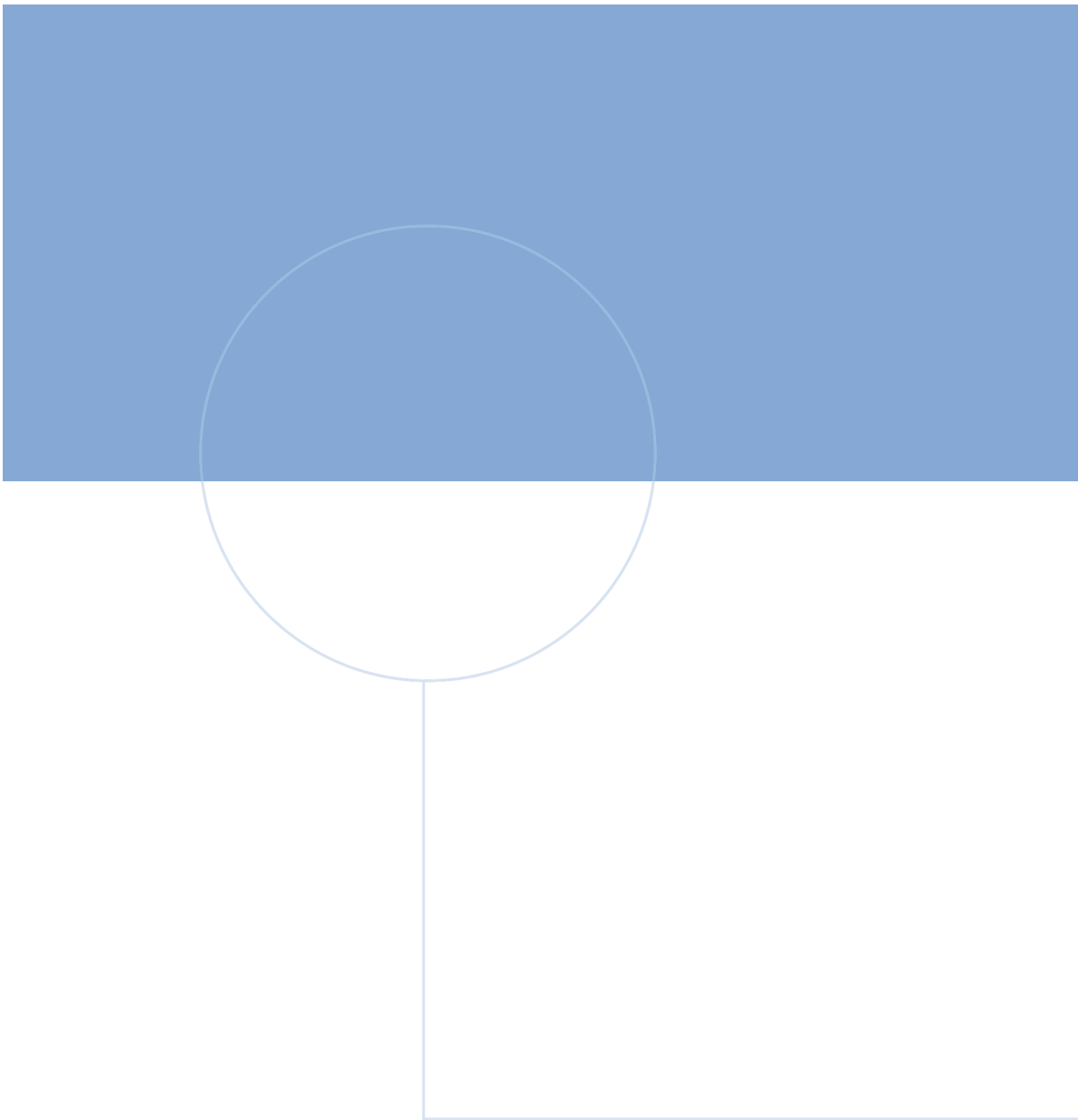
Vis, B., & Kuijpers, D. (2018). Prospect theory and foreign policy decision-making: Underexposed issues, advancements, and ways forward. *Contemporary security policy*, *39*(4), 575-589. https://doi.org/10.1080/13523260.2018.1499695

Von Heinegg, W. H., Dinstein, Y., & Domb, F. (2011). Israel Yearbook on Human Rights, Volume 41 (2011). In *Asymmetric Warfare - How to Respond?* (pp. 31-48). Brill | Nijhoff. https://doi.org/https://doi.org/10.1163/9789004226449003

Waltz, E. (1998). *Information warfare: principles and operations*. Artech House Incorporated.

Waltz, K. N. (1979). *Theory of international politics*. McGraw-Hill.

Aannø, S. T. (2018). *Strategisk avskrekking i det digitale rom - Finnes det rasjonelle strategier for små stater?* Forsvarets Høgskole]. https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2505601/MA_2018_Aanno.pdf?sequence=1&isAllowed=y



NTNU

Norwegian University of
Science and Technology