Unmasking Russian Hybrid Warfare in Europe:

A Comparative Study of Estonia and the Netherlands

July 2023

University of Glasgow: 2685728r
Dublin City University: 21109729
Charles University: 82733938

Presented in partial fulfilment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies

Word count: 23,739
Supervisor: prof. David J. Smith
Date of Submission: 20-07-2023

Table of Contents

Acknowledgements

My sincerest gratitude goes out to Professor David J. Smith at the University of Glasgow for his plethora of valuable insights and excellent and sharp feedback during the writing process.

I would also like to thank my fellow students, peers, friends and especially my family who have supported and helped me whilst conducting this research, with structural and mental support as well as constructive feedback.

Finally, I want to express my deep appreciation for the city of Prague and in particular its many excellent cafes, which have been pivotal in the writing of this dissertation as they proved to be exceptional places for studying and writing.

Abstract

This dissertation examines the development of hybrid warfare as an analytical concept, and in particular the development of Russian hybrid warfare post the 2014 Russian annexation of Crimea. Russian hybrid warfare has since then developed into large-scale policy and Russia is unlikely to cease its hybrid activities, making them an important field of study. Making use of a comparative case study approach, the dissertation looks closely at two small states, Estonia and the Netherlands, and their respective experiences with Russian hybrid warfare and to what extent there exist differences and similarities between the two cases studied.

The study demonstrates that Russia views itself as at war with the West and that it involves all elements of its state to gain the upper hand, with a particular focus on hybrid methods ranging from information warfare to cyber warfare and proxy warfare. Similarities as well as differences between the two cases exist, although the similarities have the upper hand with information warfare being the strongest asset of the Kremlin in both states. Further, this dissertation argues that studying and understanding Russian hybrid warfare is of significant importance for protecting democratic societies in the West and that future research may engage in exploring possible countermeasures in depth.

Keywords: hybrid warfare, Russia, Estonia, the Netherlands, small states, information warfare, cyber warfare, economic warfare, proxy warfare, political influencing operations

1. Introduction

Ever since the Russian Federation took the world by shock with its swift annexation of Crimea in March of 2014, analysts, academics and policymakers have increasingly used the term "hybrid warfare" as an analytical construct in an attempt to explain Russia's actions. The extensive literature on the term and the substantial analysis of Russia's foreign policy in Europe reveal that Russia does indeed attempt unconventional incursions within Europe. A great variety of hybrid methods are deployed by Russia, varying from economic and cyber warfare to meddling in foreign democratic elections and misinformation campaigns, amongst others. Despite its popularity amongst scholars and policymakers, the concept of hybrid warfare, and utilizing it as an analytical tool has received ample criticism and remains contested. Scholars have argued that the term is too broad, overused and does not constitute something "new" but has rather been around for centuries.

Even though the presence of Russian hybrid operations in Europe has been acknowledged, little academic effort has been made to categorize these operations and study the differences in the Russian approach, depending on the state targeted. This dissertation aims to analyse the variation in Russian hybrid operations towards Europe. It seeks to reveal the differences and similarities that may exist in these operations, depending on their targeted state, and divulge what lessons can be learned in regard to effectively countering hybrid incursions by Russia. These questions hold significant relevance: since the annexation of Crimea Russian illicit involvement in Europe has increased and evolved into large-scale policy. Unwanted Russian interference is likely to remain an integral part of European politics for the foreseeable future. Studying these threats is thus vital if Europe strives to ready itself to effectively counter hybrid incursions, or at the very least, learn how to deal with them in order to minimize their impact on European societies.

To do this, this dissertation makes use of a comparative case study of Russian hybrid operations in both Estonia and the Netherlands. Both states studied have

experience with Russian interference and are similar in geographical size. Despite their relatively small size, both states have been able to exert significant influence within international relations and often act proactively within the international organisations they are both part of, such as the European Union and NATO. Furthermore, they are frontrunners on several key issues, with the Netherlands being a leading actor in human rights and international law and Estonia profiling itself as an important advocate of digitalization. Not only their similarities make Estonia and the Netherlands suitable case studies. Their differences, in particular their different historical trajectories of relations with Russia, are instrumental in their suitability. Estonia is characterized by its close geographical proximity to Russia, having been a part of the Soviet Union until its independence in 1991, and its present-day large Russian minority that makes up a quarter of its population (Statistikameet, 2021). The Netherlands, on the other hand, is located far from Russia in Western Europe and has had diplomatic relations with the modern Russian state since the end of the Second World War, perceiving it as a threat to its safety during the Cold War. Since the end of the Cold War, Dutch relations with Moscow were mostly in line with the European Union's relations with Russia. Relations with the Kremlin deteriorated after the annexation of Crimea and especially the downing of Malaysia Airlines Flight 17 in 2014 during the War in Donbas, an event in which 193 Dutch nationals were killed. One of the aims of this study is to unravel potential differences in Russian hybrid warfare towards both states. If Russian hybrid warfare strategies towards either state vary substantially, these differences could help uncover the reasons behind different Russian approaches.

Europe is a continent that plays host to a relatively large number of small states in geographical size. Thus, studying Estonia and the Netherlands may also produce lessons that could be of value to similar states that are forced to deal with hybrid warfare from Russia. A more detailed explanation of the methodology, case selection and limitations of this dissertation have been outlined within the chapter on methodology.

Before being able to assess and analyse Russian hybrid warfare operations within the states studied, this dissertation will engage in a review of the academic literature, in order to clearly conceptualize and define the term "hybrid warfare", as well as discuss the criticism the term has received. Then, this dissertation will thoroughly discuss both case studies and categorize the various hybrid approaches that have been orchestrated against these states. Finally, this dissertation will engage in an elaborate analysis of the cases studied and discuss the similarities and differences between hybrid operations in the abovementioned states, before coming to a conclusion.

It is important to mention that this research primarily covers the period starting from the annexation of Crimea in 2014 up until the Russian invasion of Ukraine in 2022. The reasons for choosing this time frame are further discussed within the methodology section, but it is imperative to stress that this dissertation condemns the illegal Russian invasion and does not seek to ignore it. However, as is good academic practice, it is difficult to study and provide structural analysis on events that are ongoing, even if these events may contradict policies of the past. For example, this dissertation discusses hybrid warfare being used by Russia as a strategy to minimize its use of conventional forces and suggests that in the era of hybrid warfare, the chance of all-out conventional wars occurring is diminishing. However, we now know this to be a false premise, in light of Russia's aggression towards Ukraine. This does not mean that the topic studied becomes obsolete; hybrid warfare still holds a significant presence amongst the palette of strategies that form warfare and states are highly likely to have to keep facing hybrid threats in the next decades.

2. Methodology

The following section will outline the methodological decisions and considerations that have been made in order to answer the main research question as well as the sub-questions of this dissertation.

2.1 Research questions & sub-questions

The main research question that this dissertation aims to answer is: to what extent do Russian hybrid warfare operations in Estonia differ from such operations in the Netherlands and what can we learn from this?

In order to answer the main research question, the dissertation makes use of the following sub-questions:

1. What is hybrid warfare, and how can we conceptualize this term?
2. What Russian operations in Estonia and the Netherlands can be defined as a form of hybrid warfare?
3. What are the fundamental differences and similarities (if any) of Russian hybrid warfare operations in Estonia and the Netherlands?
4. What lessons can Estonia learn from the Netherlands regarding the response to Russian hybrid warfare and vice versa?

2.2 Comparative case study

The main research question has been clearly pinned towards a comparative case study approach. This methodology is deemed to be the most effective means of analysing and comparing Russian hybrid warfare operations in Estonia and the Netherlands. Through this approach, this dissertation aims to conduct in-depth research on both cases and answer complex questions on a real-world issue. The comparative case study approach is defined by Yin as an empirical inquiry that is used to study present-day phenomena in their real-life contexts (2003). It is seen as a flexible approach since the cases selected can be moulded to the research question. Using the comparative case study method enables the

researcher to use many research tools on a small number of subjects, leading to very detailed knowledge on the cases, thus enabling a more thorough assessment. Furthermore, bias is reduced due to the fact that a wide range of variables and perspectives are involved (Mills et al., 2009).

Another reason for opting for the comparative case study approach is to produce more generalizable knowledge on Russia's use of hybrid warfare in Europe. Causal questions, such as why Russia may adopt policy x in country y and not in country z or vice versa are answerable by means of this approach. This dissertation does not underestimate the challenge that lies in making meaningful comparisons across complex political systems. Comparative case studies are known to reduce the representativeness of their findings in relation to cases that have not been studied intensively, as findings tend to be case-specific (De Vaus, 2001; Yin, 2003). These are valid concerns; however, case studies often focus on unusual, peculiar cases that stand out and question presently existing assumptions. Doing so, the comparative case study can act as an effective method of filling in the gaps in our understanding of various topics. In this dissertation, both cases studied differ substantially, as do all countries, but also share similarities that make them worthy of study. These will be further expanded upon within the following section on case selection.

2.3 Case selection

This dissertation has selected the cases of Estonia and the Netherlands respectively. These two states share many similarities as well as differences and have been chosen as subjects of study for a variety of reasons. First, is the geographic dimension. Both states are similar in geographical size, with Estonia being slightly larger at 45,340 km2 in comparison to the Netherlands at 41,543 km2. However, in terms of population Estonia is much smaller, having 1.35 million inhabitants in comparison to 17.5 million inhabitants in the Netherlands. Estonia is one of the Baltic states and borders Russia, whereas the Netherlands is a Western European state, far from Russia. Second, is the international

dimension. Both Estonia and the Netherlands are relatively small in geographical size but yet manage to be vocal on the international stage. Both states are members of a great number of international organisations such as the EU and NATO and are well integrated within these organisations. Third, is the domestic dimension. Both Estonia and the Netherlands have a history of dealing with attempted Russian interference. For Estonia, Russian interference tends to focus on disinformation campaigns with the aim of influencing public opinion, especially since Estonia plays host to a significant number of ethnic Russians. In the Netherlands, Russia mainly focuses on hacking and attacking government institutions as well as research institutes to extract information. However, both nations have had to face multiple types of threats and the types of threats have been similar for both nations. Naturally, the history of Russian involvement in both states and its operations in the present day will be examined in much greater detail within the case studies themselves.

Despite their geographic size, both states that are studied within the case study are able to exert significant influence on international relations. Estonia has since its independence been a frontrunner in digitalization, the EU Eastern Partnership and has first-hand experience in dealing with hybrid threats. It has acted proactively within NATO, the EU and on relations with Russia. Similarly, the Netherlands has a long history of punching above its weight within the international arena. The Dutch are respected globally for their efforts towards international development and international law and are regarded as important policymakers, especially within the European Union.

These factors contribute to the conviction that studying these cases in depth can provide us with valuable knowledge on Russian hybrid policies towards Europe. The two cases differ but share significant similarities too. This puts forward the interesting question of whether Russia's hybrid policies towards Europe are substantially different depending on the state targeted, and if so why, and if not, what those similarities are and how European states can aid one another to proactively counter this threat. Some important similarities, such as

geographical size and their membership in international organisations such as the EU and NATO will benefit the generalisability of this study's findings because the EU and NATO are composed of a great number of small states, which could potentially draw lessons from the conclusions of this dissertation, albeit not being amongst those states intensively studied. Larger states could also learn from the findings of this research because hybrid warfare is not at all exclusively used on smaller states, great powers such as the U.S. have faced hybrid threats as well. On top of that, until recently the security interests and perspectives of Western and Eastern European states have been researched mostly separately, however the crisis in Ukraine proves to us beyond doubt that this approach has become redundant. Eastern European states are now part of organizations such as NATO and face similar threats as Western European states because of NATO's inherent collective responsibility for defence.

2.4 Methods of analysis

Secondary sources will make up the majority of sources used within this dissertation. This dissertation aims to provide analysis through the studying of the available academic literature, government publications, think-tank reports and news articles. By doing so, this dissertation will provide an accurate representation of events and circumstances, supported by an overview of the theory that constitutes the term hybrid warfare.

2.5 Limitations

This dissertation studies the period starting with the annexation of the Ukrainian peninsula Crimea in February 2014. The annexation of Crimea is often seen as a turning point in Russian foreign politics, as it marked Russia's intent to entrench itself in a "wider" continental Europe (Sakwa, 2012). It also marks Russia's turn to becoming an expansionist power and is thus a relevant timeframe to study for it increasingly threatens the European security order. For the sake of accurate research, ongoing geopolitical events are not researched

and the timeframe of this dissertation, therefore, limits itself to the start of the ongoing war in Ukraine.

3. Literature Review

3.1 Introduction: Hybrid Warfare: One Term, Many Definitions

Hybrid warfare is a term that has recently gained significant prominence in academia as well as defence and policy circles, especially since the annexation of Crimea in 2014. The term is broad and has often been described to be an umbrella term for all unconventional means of warfare. Its ambiguity is one of the term's primary sources of criticism, amongst others. Defining hybrid warfare is important, not merely for the sake of academic practice, but also to better understand the actions of states. Different perceptions and definitions of hybrid warfare may lead to different actions and responses to hybrid threats. The following section will discuss the definition of hybrid warfare, its origins, the criticism that has followed its rise in popularity, as well as the Russian relationship with the term.

The term "hybrid warfare" describes a theory of military strategy that gained significant popularity in recent decades. One of its earliest and main proposers is the scholar and former U.S. marine corps lieutenant Frank Hoffman, who argues that the 9/11 attacks on the United States marked the dawn of a new age of warfare (Hoffman, 2007). He argues that modern wars have become more "blurred" and have adopted an "ambiguous" and "uncomfortable" nature, especially for the traditional power actors, as they had been used to a traditional opponent who adheres to certain standards and common practices of warfare, such as fighting in clearly structured formations (Hoffman, 2007, p. 12). According to Hoffman this trend is not new and did not come out of nowhere on the 11th of September 2001 but had rather been overlooked by scholars, military specialists and policymakers as far back as the 1983 Beirut barracks bombing.

So how may we define this new form of military strategy? One option would be to argue that it implies a combination of approaches to warfare, a synthesis of different methods (Mattis & Hoffman, 2005). Early hybrid warfare theorists

related this new phenomenon to the role of non-state actors on the battlefields in Lebanon, Chechnya, Afghanistan and Iraq (Reichborn-Kjennerud & Cullen, 2016). Modern adversaries are deemed to be unlikely to limit themselves to a single method of warfare. Conflict will be blurred, with uncertainty existing as to who is fighting, and what technologies are used. Hezbollah, for example, was used as an illustration of a non-state actor that started combining conventional and non-conventional methods of warfare with non-military modes of operation that were unfamiliar and new to Western military practice and thinking, leading to blurring (Reichborn-Kjennerud & Cullen, 2016). As a result, the new age of warfare will be characterized by a wide range of varying and complex tactics that may be defined as hybrid warfare (Hoffman, 2007). This early approach is thus characterized by perceiving hybrid warfare as a product of the international context of the late 1980s and 1990s, a period defined by American military dominance. These scholars hold that adversaries to the United States realized that a conventional war could not be won and that unconventional methods are therefore required to achieve success.

3.2 Hybrid Threats: Something New?

Another approach to hybrid warfare challenges the notion that the concept is relatively new and rather proposes a historical perspective. Put simply, this school of thought defines hybrid warfare as a military situation in which conventional and unconventional forces are used concurrently (Wither, 2016). Furthermore, this is not a new phenomenon; as von Clausewitz already wrote in On War, many factors contribute to what we call war, with hatred, violence, politics, chance and probability being some of them. Ever since we have known war, these factors compose it and we recognize them in the interactions between peoples, governments and militaries (Von Clausewitz, 1976). War may appear to change and morph into forms that are unfamiliar to us but will in essence remain the same. Murray & Mansoor define hybrid warfare as a "conflict involving a combination of conventional military forces and irregulars

(guerrillas, insurgents, and terrorists), which could include both state and non-state actors, aimed at achieving a common political purpose." (2012, p. 2) If we adhere to this definition, it becomes clear that hybrid warfare is definitely not an anomaly but rather of all ages. Examples date back as far as ancient times, with chronicles of the Peloponnesian War as well as the writings of Sun Tzu clearly outlying military strategies involving both regular and irregular forces. During the Peloponnesian War in the 5 th century BC, the Spartans recognized the necessity of withholding a significant force in the Spartan-controlled regions of Messenia and Laconia, in order to prevent an uprising that would threaten their military and agricultural supply lines. The Athenians on the other hand aimed to stir an uprising, in order to add an irregular element to the conflict by fortifying a settlement in the occupied region and garrisoning a force of strong anti-Spartan sentiment. The insurgency that followed forced the Spartans to come to terms with the Athenians, in fear of a hybrid war that would threaten their own homeland (Murray & Mansoor, 2012). Some of the great modern armies, notably Hitler's Wehrmacht and Napoleon's Grand Armée, have struggled against irregular forces. During World War II, the German Army suffered severe disruptions on the Eastern Front, due to Soviet partisans, together with other irregulars, cutting lines of communication (Grenkevich, 2013). The Vietnam War saw the People's Army of Vietnam cooperate intensively with the irregular Viet Cong, a move that proved decisive in prolonging the conflict with their superior adversary in the U.S. and France (McCulloh & Johnson, 2013). Modern conventional militaries have continuously struggled to effectively combat guerrilla groups and western operations in Iraq and Afghanistan showcase the difficulty of fighting an irregular enemy (Wither, 2016). During the 2000s, the term hybrid warfare became even more commonly used, mainly because non-state actors became increasingly sophisticated in their use of lethal action as well as the increase in the potential of cyber warfare. In part, this was due to technological advancements that enabled various kinds of groups to operate more effectively.

Scholars that support the historical perspective on hybrid warfare argue however that this does not constitute a new form of warfare, but rather puts more emphasis on the fact that contemporary warfare has increasingly become a blend of methods and approaches, along the full spectrum of a conflict (U.S. Government Accountability Office (GAO), 2010).

3.3 Characteristics of Hybrid Warfare

The plenitude of historical examples of hybrid warfare and hybrid threats might confirm its presence over time; however, they do not solve the problem of defining what exactly a hybrid threat is. One reason for the difficulty that lies in defining hybrid warfare could be the fact that the uniqueness of each situation in which a hybrid threat may exist renders any definition of such a threat inadequate. Because each context differs fundamentally in space, logic and time, a single definition is hard to attain (McCulloh & Johnson, 2013). Therefore, some argue that the term is "too inclusive to be analytically useful" (Gray, 2012, p. 41). This and other forms of critique will be discussed at length in the "criticism" section.

One could argue that the struggle to define hybrid warfare calls for some sort of theorisation, an approach that enables us to better understand hybrid warfare by outlining the key characteristics of what is generally understood to be a contemporary hybrid threat.

Scholars distinguish warfare as "hybrid" in many situations that include some, or parts of the following aspects:

- A hybrid actor is **non-standard**, **unconventional**, **complex** and **fluid**. Actors that are labelled as hybrid may take many forms and shapes and can be state actors as well as non-state actors. To add to the complexity, there are ample examples of non-state actors that act within the state system, for example as proxy forces, such as the notorious "Wagner Group" Russian private military company. This force of mercenaries is known to have been active in various conflicts in Syria, Sudan, Libya,

the Central African Republic and Ukraine (Rauta, 2020). Despite not officially being a part of the Russian military, it acts in Russia's interests and receives military equipment and training facilities from the Russian state, hence it is considered to be a de facto unit of the GRU, Russia's military intelligence agency (Higgins & Nechepurenko, 2018). The Lebanese militant group and political party Hezbollah is another frequently used example that fits the contemporary definitions of a hybrid actor. During the 2006 Israel-Hezbollah War, Hezbollah, having been equipped and trained by Iran, was able to surprise Israel by making use of a combination of guerrilla and conventional tactics (Wither, 2016). It also made use of advanced weaponry and communication methods that were usually found within conventional armed forces only (Hoffman, 2007). The internet and mass communication were used to quickly spread propaganda amongst its supporters, and the group was able to successfully influence global opinion on the conflict from its inception (Wither, 2016).

- A hybrid actor makes use of a synergy of **conventional** and **unconventional** methods. There are a great number of methods that are associated with hybrid warfare within the literature. These vary from the use of conventional methods to irregular ones, diplomacy, terrorism, politics, cyber, indiscriminate violence and criminal activity (Reichborn-Kjennerud & Cullen, 2016). Vital here is the combination of irregular methods with conventional ones. A hybrid actor employs an approach of combining methods because it believes it is the best road to achieving strategic success (Hoffman, 2007). The Islamic State did not only make use of conventional tactics to conquer territories, but simultaneously used unconventional methods to subdue the population. It orchestrated terrorist attacks, spread hate propaganda and carried out mass killings of any resisting population (Moreland & Jasper, 2014).

The combined use of methods in order to attain a strategic goal is an important characteristic of a hybrid actor.

- A hybrid actor is **flexible** and able to respond **quickly**. Unlike conventional militaries, hybrid actors are often able to respond to new situations rapidly, as they often operate outside the bureaucracy-filled state system (Anton, 2016). For example, private military companies, such as the American Blackwater and the Russian Wagner Group are often said to operate in "legal grey zones", under relatively little scrutiny, enabling quicker and more flexible action (Scahill, 2008). Maintaining support for the Wagner Group is deemed to be advantageous for the Kremlin because it can operate under the law, and thereby do the "dirty work". Its existence provides Moscow with plausible deniability of Russia's official involvement in the conflicts in which Wagner is active, because it does not act as an official entity of the state (Reynolds, 2019). Furthermore, hybrid actors are often highly versatile: they are able to disperse themselves amongst the population, shift rapidly from combatant status to that of an innocent civilian and use informational warfare to an extent that it can diminish the technological superiority of the enemy (Balan, 2016). During the War in Afghanistan that followed the 9/11 terrorist attacks, the Taliban was able to effectively make use of flexible fighters that would be heavily integrated in local tribal structures, essentially making them "innocent" civilians by day and militant operatives by night (Schroefl & Kaufman, 2014).

- A hybrid actor is able to make use of **advanced**, **disruptive technologies** and **weapon systems**. Hybrid actors that operate outside of the state system are able to attain and make use of advanced technologies and weapons systems because the prices of such systems

are nowadays affordable (Grant, 2012). Technologies such as cellular networks and phones can be used as a means of effective command and hybrid actors often do not require expensive reconnaissance equipment because they fight on familiar terrain. The Israel-Hezbollah War of 2006 is an example of a conflict wherein decentralized cells of guerrillas and conventional troops successfully made use of advanced weapon systems such as precision-guided missiles, downing Israeli helicopters, damaging tanks, communicating through encrypted phones and monitoring enemy troop movement with night vision equipment (Deep, 2015).

- A hybrid actor is capable of using **propaganda** and **mass communication** effectively. The information revolution of the early 21st century has enabled the growth of mass communication networks, offering powerful tools for spreading information, propaganda and recruiting. The power of the internet has been used by virtually every hybrid actor in various conflicts over the past decades. Hezbollah successfully discredited Israel through a (dis)information campaign in 2006, the Islamic State gained a large following through its online presence and Russia has been widely accused of influencing western politics through social media (dis)information campaigns (McCulloh & Johnson, 2013; Moreland & Jasper, 2014; Standish, 2019). These tools add to the palette of options available to a hybrid actor to attain their strategic objectives. Especially the Islamic State was able to exploit information warfare and propaganda in an unprecedented fashion, rallying thousands to their cause as a result through the glorification of its operations on social media (Wither, 2016).

- A hybrid actor makes use of **three distinct battlefields**. What makes modern conflict even more complex for conventional, state actors, is that

hybrid actors tend to operate on three distinct battlefields simultaneously. These are 1) the conventional, military battlefield, 2) the media battlefield and 3) the battlefield of the international community, international courts and public opinion (Ganor, 2012). The importance of this multidimensional approach to conflict cannot be overstated. With terrorism being widely regarded as illegal, many hybrid actors that make use of terrorism also extend their reach to the media and the international community battlefields, in order to gain public support and a sense of legitimacy for their cause. When effective, these (political) movements may act as fronts for illegal terrorist activities. Public support may also be sought by hybrid actors in order to delegitimize an opponent, sometimes by making use of falsified or biased information. Examples of this are plentiful, and may for example be found in the Israel-Palestine conflict and the current War in Ukraine.

3.4 Hybrid Warfare post-2014 & "Russian" Hybrid Warfare

Within the literature, there exists a clear delineation of the term hybrid warfare before and post-2014, when Russia's involvement in Ukraine intensified with its annexation of the Crimean Peninsula. It is this occasion of escalation that significantly increased the interest in the term. As Russia was making use of a varying blend of methods and tools in Ukraine, many in the West felt that "hybrid" was the most appropriate description of the Kremlin's actions (Wither, 2016). The following section will discuss hybrid warfare post-2014, with a particular focus on its use by Russia.

In 2014, the then NATO Secretary General Anders Fogh Rasmussen argued that Russia was waging a "hybrid war" in Ukraine, defining it as "a combination of military action, covert operations and an aggressive programme of disinformation" with the intent of weakening the Ukrainian state and its government, as well as the resolve of the West, and thereby retaining Russian

influence over the eastern part of the country (Landler & Gordon, 2014). Russia's swift annexation of Crimea was a showcase of a wide set of methods, integrated into a single campaign. These varied from military and non-military tools to diplomatic means, information campaigns, cyber and electronic operations, economic pressure and covert as well as overt military and intelligence action ("Complex Crises Call for Adaptable and Durable Capabilities," 2015). All of these tools served a single objective: to seize the initiative and gain a physical as well as a psychological advantage (Wither, 2016).

But before we delve into greater detail on Russian methods and practice when it comes to hybrid warfare, it is important to discuss what distinguishes this, post-2014, definition of hybrid warfare from those discussed in previous sections. The key distinction lies in its focus on non-military methods of warfare, especially information warfare and electronic/cyber warfare (Renz, 2016). Whereas the use of mass media, propaganda and the multidimensional battlefield was not new, as shown in the previous section, it was arguably rarely so vital to the success of a campaign as it was to Russia's campaign to capture Crimea in 2014. Acts of electronic warfare and cyber-attacks successfully removed any chance of an effective Ukrainian response, and a carefully orchestrated media strategy made it a challenge to differentiate the truth from falsehoods, thereby creating an alternative reality for supporters of the Russian narrative, leading to confusion and a lack of internal cohesion not just amongst Ukrainians, but also amongst western partners.

Similarities between Russian involvement in Ukraine and previous instances of hybrid warfare do however exist. The "blurring" of conflict and traditional warfare, the unfamiliar tactics, the use of non-military means and the asymmetrical relationship of this strategy with western, conventional strategies is not necessarily new (Reichborn-Kjennerud & Cullen, 2016). However, the effective focus on non-military methods and their integration with military

methods on the state level did evolve the concept of hybrid warfare, drew significant attention to it and furthered academic thinking on the topic.
With non-military methods at the core of its strategy, Russia sought to exploit underlying, already-present vulnerabilities within Ukrainian society and weaken the legitimacy of the Ukrainian state. Similarly, to the Islamic State in the previous section, Russia was able to effectively make use of information campaigns to shape and influence the opinion of the public, or at least a significant enough part thereof, a feat that further stresses the importance of this "media battlefield" within contemporary conflicts (Ganor, 2012; Wither, 2016).

The characteristics of Russian hybrid warfare, its objectives and methods, and especially their implementation will be discussed at length within the case studies on Estonia and the Netherlands. However, it is important to provide an overview and categorization of these characteristics, objectives and methods, as derived from the literature in order to fully comprehend the material that will be discussed within the case studies. Three key characteristics were attributed to Russian hybrid warfare in a 2017 testimony before the Committee on Armed Services of the U.S. House of Representatives:

1. **Economization of the use of force**. Russia is aware of the reality that it is unable to successfully engage in an open military conflict with NATO, especially a protracted conventional conflict. Therefore, the Kremlin seeks to use limit its overt use of conventional forces. This does not mean conventional and even nuclear forces are no part of its strategy, but Russia's hybrid strategy seeks to minimize the full-scale deployment of its conventional forces. One of the reasons for this is cost: cyber and information operations are much more affordable for the Russian state than traditional military operations (Chivvis, 2017). In the case of Russia hybrid warfare can thus, in a way, be seen as a weapon of the weak.
2. **Persistency**. In the contemporary world of armed and hybrid conflicts, there is no such thing as a time of peace and a time of war. Hybrid wars

are persistent and “break down the traditional binary delineation between war and peace”. The variable is no longer war or peace but rather intensity, with hybrid strategies being ever-present and evolving, albeit more acute and intense at certain moments (Chivvis, 2017, p.2). Russia sees itself as fighting an ongoing hybrid war with the west and in particular the U.S. and deploys a strategy of shaping its tools, both military and non-military, to win that war (Clark, 2020).

3. **Population-centric**. The largely unsuccessful campaigns of the U.S. and its western allies in conflict zones such as the Middle East, the Balkans and Africa have raised awareness amongst Russian military thinkers that exerting influence over local populations is of utmost importance in conflict. Russia attempts to influence the population of its target countries by, amongst other methods, orchestrating information campaigns, motivating proxy groups and influencing elections from within the already present “social and political frameworks” that exist within target countries (Chivvis, 2017, p.2).

3.5 The View of the Kremlin: Russia’s Objective & Toolkit

In order to sufficiently comprehend Russia’s hybrid actions in Europe, it is important to understand the discussions within Russian military circles on the concept. Even though some discourse is likely obscured from the view of the public, the discussions that happen in Russian military journals, government-supported news outlets, as well as Western sources and think tanks are still highly likely to act as a good indicator of overall thinking within the Russian military. An important note on Russian perception of hybrid warfare is that it differs from the view of many in the West in the sense that Russia sees hybrid war as a “type” of conflict rather than a toolkit or means of waging a war (Clark, 2020). The Kremlin believes it is engaged in an ongoing hybrid war with the West. As a direct war with Russia is assessed to be unlikely, Russia ought to invest in preparations for hybrid conflicts, as they are seen as the future of war.

The Russian has a holistic view towards hybrid warfare: it sees it as an activity that involves the entirety of the state and its institutions in which all efforts, even military ones, are subordinate to an information campaign (Göransson, 2022).

The Russian state deploys its hybrid strategy for several reasons. This dissertation identifies three main objectives:

1. **To capture territory without the use of conventional, overt force**. The Crimea annexation of 2014 is a prime example of this objective. In the case of Crimea, the so-called "little green men" became notoriously famous for seizing Crimea without suffering a single casualty (Howard & Pukhov, 2014). These men, wearing modern Russian uniforms but lacking any insignias, were in fact Russian special forces (Galeotti, 2015). The lack of insignias enabled Moscow to deny any involvement, thereby creating enough maskirovka[1], disguise, to confuse commanders in Kyiv and at the NATO headquarters. The Russians were able to take up strategic positions, block the ill-prepared Ukrainian garrisons and eventually force the surrender of the peninsula (Galeotti, 2015). This operation occurred in close conjunction with the deployment of local Russian proxies and an information warfare campaign (Chivvis, 2017). General Valery Gerasimov, the Chief of the General Staff in 2014 and the current commander of all Russian forces in the War in Ukraine has written on the use of non-military means on multiple occasions, arguing that the role of non-military means has grown significantly and have in many cases now exceeded the power and effectiveness of conventional weapons and are used four times more often in modern conflicts than their conventional counterparts (Gerasimov, 2016). Capturing territory without using conventional, overt forces has often been a prelude to a "frozen conflict", which hampers integration with the West for the

[1] Maskirovka translates literally into Russian as "disguise" and is a term often used to describe the Russian doctrine of military deception, developed from the start of the 20th century.

affected countries and forces them into the Russian sphere of influence. Examples of this outcome can be found in the frozen conflicts in Georgia, Nagorno-Karabakh, Moldova and Ukraine (Blank, 2008a; Bebler, 2015).

2. **To enable the use of conventional, overt force at a later stage of a conflict**. Russia's successful hybrid operation in Crimea has raised concern over the possibility of reiteration elsewhere. Concerns are especially high in the Baltic states, where Russia may seek to pursue a narrative that alienates Russian minorities from Baltic governments. For example, in Estonia, Russia could seek to justify an intervention on behalf of Russian minorities by depicting the Estonian government as repressive towards minorities (Chivvis, 2017). Such an information operation would be likely accompanied by cyber operations and attempts to influence the broader opinion within Europe and beyond, with proxies and covert operatives being active on the ground.
3. **To influence the politics and policies of foreign states**. Whereas democracy and the freedoms that are associated with it are seen as great assets in the West, they also constitute vulnerabilities. Actors such as Russia that seek hybrid interference see these freedoms as potential sources of exploitation and opportunity to drive wedges within societies and undermine governments, as well as alliances (Wigell, 2019). This third objective relates to the second objective mentioned above in the sense that it may act as a prelude to conflict escalation, even though this does not necessarily need to be the case. In many cases of target countries, Russia does not seek military intervention but rather internal instability. Further, the strategy intends to ensure that political outcomes in target countries favour the national interests of Russia. Naturally, countries with weaker legal frameworks and a higher rate of corruption are more vulnerable to these hybrid strategies but strong democracies are at risk too, as is visible in the case of the U.S. and Germany (Chivvis,

2017). This is not a strategy of overt confrontation. Rather, Russia covertly attempts to influence foreign politics in order to weaken the resolve of the target country and undermine internal cohesion. Because of their covert nature, the threat perception of this strategy is dispersed: a large part of the population is unaware of the threat and others that benefit from Russian involvement will attempt to downplay it (Wigell, 2019). When implanted successfully, this undermines the ability of the target country to counterbalance against its adversary, in this case Russia.

In order to attain these objectives, the Kremlin employs a large variety of methods. A total of six categories can be identified:

1. **Information warfare**. Strategic information campaigns have shown to be an effective tool for shaping political narratives within states. Both Sputnik News and Russia Today are well-known Russian media outlets that provide television programming and news coverage. Prior to their banning following the Russian invasion of Ukraine in 2022, these channels were available worldwide and were very active on social media platforms such as YouTube and Facebook (Stefan, 2021). Russia also financially supports European television programmes, think-tanks and employs so-called "troll farms". These farms are organised groups that convene with the single purpose of influencing public opinion by generating misleading information and/or fake information online (McCombie et al., 2020). It has been estimated that Russia spends at least 300 million USD annually on an "army" of disinformation spreaders counting at least 1000 individuals, however this may only constitute the "tip of the iceberg" (Grynszpan, 2017; Rademaker et al., 2017). As a result of these information operations, doubt may be cast upon truths and pro-Russian narratives that often lack factual evidence

are spread, shaping political discussions in ways that are beneficial to Moscow (Chivvis, 2017).

2. **Cyber warfare**. Gathering information by means of hacking is very valuable for Russia in order to successfully influence foreign politics. Other than gaining information for influencing campaigns, cyber warfare may be deployed in order to manipulate or affect vital information systems in the West, such as was the case in the allegedly Russian cyber-attacks on Estonia in 2007, wherein the Estonian parliament, most of its ministries, internet providers, banks and news organisations were targeted (Ottis, 2008). Russia also makes use of cyber warfare in order to attain or steal information that is relevant to its own global image or previous actions, as was visible when Dutch military intelligence accused Russia of attempting to hack into the headquarters of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Hague. The Netherlands expelled several Russian officers who allegedly attacked the OPCW, which was at the time carrying out an investigation into the poisoning of Sergei Skripal as well as chemical weapons attacks in Syria (Crerar et al, 2018; Henley, 2018).
3. **Proxy warfare**. Proxy groups that are deployed by Russia are often groups that share sympathies with the Kremlin's interests. These can be private military companies that can do "the dirty work" such as Wagner but may also be ultra-nationalist gangs such as the Night Wolves. The Night Wolves, originally a Russian motorcycle gang, receives funding from the Kremlin in order to "mobilize nationalist sentiment in Russians" through propaganda (Harris, 2020, p. 260). Abroad, Russia supports protest movements that suit the Russian narrative. Examples of such are Moscow's support for anti-EU groups in the 2016 Dutch referendum on the EU's Association Agreement with Ukraine and its backing of anti-shale gas protestors in Bulgaria, a move that complicated

Bulgaria's desire to reduce its dependency on Russia for its energy supply (Applebaum, 2016; Hope, 2014).

4. **Economic warfare**. Russia makes use of both direct and indirect economic policies to influence foreign politics. The Kremlin has a history of shutting off the gas supply to Ukraine over price disputes. Prior to the outbreak of the War in Ukraine, the Russian state-owned gas company Gazprom exerted great influence over European economies through its gas supply, being their largest single supplier of gas (Dickel et al., 2014). Notably, the Nordsteam gas pipelines made Europe even more dependent on Russian gas, enabling Russia to bypass Ukraine in its energy supply to Europe and thereby being able to exert greater geopolitical pressure on Kyiv (Goldthau, 2016). Despite the fact that these Russian investments were largely legal, they are still considered problematic for their ability to increase Russian influence in foreign politics (Chivvis, 2017).
5. **Covert/clandestine operations**. Clandestine operations such as traditional espionage, extortion and bribing remain amongst Russia's hybrid methods to exert influence abroad, especially over vulnerable political figures. Important in this regard are its special operations forces, tasked with infiltrating abroad and directing hybrid operations. These were already mentioned with the example of the Crimean annexation, the "little green men" but are also believed to have been involved in the 2016 attempted coup in Montenegro, where Russian officers allegedly planned to kill the Montenegrin prime minister Milo Djukanovic (Gardasevic, 2018).
6. **Political influencing operations**. Finally, traditional diplomacy continues to play an important role in Russia's political influence operations. This is done through high-level state visits and diplomatic support of politicians and political parties abroad, whilst discrediting and deriding the positions of opposing political figures (Chivvis, 2017).

3.6 Criticism

Ever since it was brought onto the scene of the field of strategic studies by authors such as Hoffman, and especially since its surge in popularity following the annexation of Crimea, the term hybrid warfare has received ample criticism. The following section will provide an overview of the criticism hybrid warfare has received and how these critiques may be countered.

Hybrid warfare, as discussed in the previous sections, is a term that tends to be used to describe and define wars that are not purely conventional. Perhaps some part of the popularity of the term lies in the word "hybrid", a catchy word since it implies that it can represent virtually anything (Bērziņš, 2015). As a result, some scholars have argued that the term hybrid warfare is too inclusive and vague to be analytically useful (Çalişkan, 2019; Wither, 2016; Gray, 2012). Furthermore, its definition is deduced from observing the enemy and thus shifting, which leads to a lack of conceptual clarity (Reichborn-Kjennerud & Cullen, 2016). This is clearly visible in the discussions on the term, which started out with a focus on violent non-state actors in conflict zones in Lebanon, Chechnya, Afghanistan and Iraq and now include state actors, such as Russia. Furthermore, hybrid warfare has been accused of not constituting something new, with some arguing that it is not needed as a concept to better explain and understand contemporary warfare. As discussed previously, hybrid warfare is not new, and unconventional activity has been a feature of war throughout the ages. Adding a new category of warfare for something that is not new is not fundamentally necessary for our understanding of wars, both past and present, as well as future challenges. Rather, historical accuracy and analysis are sufficient tools for comprehending warfare (Çalişkan 2016). Johnson (2018) even goes as far as to argue that using the term indicates that the West is self-delusional in the sense that it perceives war as something that can be limited, constrained and regulated by the international community and its institutions.

This notion stands in stark contrast with the Clausewitzian notion of war, namely that it is unrestrained. In this regard, hybrid warfare appeared, because as its enemies turned to unconventional strategies, the West came to the shocking realization that their expectations of warfare in the 21 st century were unrealistic and overly optimistic (Johnson, 2018).

Another potential problem of hybrid warfare is that the inclusive nature of the term could lead to ordinary inter-state competition being described as conflict or war, even in the event that violence or threat is absent (Wither, 2016). The realist school of thought in international relations already included a view of the world in which states are competitive and conflictive with each other, in favour of their own interests (Walt, 1998). Competition is natural, and the means of competition, such as economic force or diplomacy were never classified as "warfare". This begs the question of whether positioning non-military methods under the hybrid warfare umbrella is useful. On the contrary, however, one could argue that it is not the West, but rather Russia that has pushed for non-military methods to be included in the definition of hybrid warfare. As mentioned previously in this literature review, Russia has consistently stated it views itself as being engrossed in an ongoing war with the West, its democracy, culture and values. Such a posture is suggestive of the notion that the Kremlin has returned to the Cold War, Soviet perception of the Clausewitzian idea that "peace is a continuation of war by other means" (Wither, 2016; Von Clausewitz, 1976). In that case, the West ought to change its posture towards Russia, and it has arguably done so, albeit late, as Johnson (2018) highlighted.

3.7 Conclusion

Despite the valid points of criticism and the clear weaknesses of hybrid warfare as an analytical concept, in particular, its broad nature, the literature on the topic does provide a useful platform for discussion on the future of warfare, which holds value since history tells us that generating an effective response to security

and defence challenges is rarely an easy task for the West. Furthermore, discussions on hybrid warfare help the West understand the thinking of its adversaries' military intellectuals and the challenges they bring to the table. Clearly, the world differs substantially in how war is understood. On the one hand, the West is characterized by a rather rigid, kinetic, instrumentalist and technical understanding of war whilst its adversaries have made attempts at redefining warfare in order to increase flexibility (Reichborn-Kjennerud & Cullen, 2016). The lack of conceptual clarity that is associated with hybrid warfare is problematic but does not warrant ignoring the value of discussions on the topic. "War" in general is contested too and so are the distinctions between peace and conflict. War is the continuation of politics by other means, but it remains unclear where this line is drawn, or if it even exists at all. All in all, agreeing on a definition of hybrid warfare should not be our main concern. Rather, scholars ought to focus on devising ways of making the term a useful concept of study, as well as formulating effective strategies to counter the practices we describe as hybrid warfare. This dissertation will do that in the following sections, by looking at its case study countries Estonia and the Netherlands through a lens of Russian hybrid warfare. It will identify Russian hybrid strategies in the two states and seek to offer an overview of the implications of these strategies as well as potential ways of counterbalancing the Russian hybrid threat. If this is successful, hybrid warfare will have been used as an analytical concept to make states in the West safer from Russian aggression, be it overtly or covertly.

4. Case Studies: Estonia & the Netherlands

The following section will look at two case studies, Estonia and the Netherlands respectively. It will assess in what ways these countries have been targeted and affected by forms of Russian hybrid warfare. For each state, the following sections will provide an introduction to its position within international relations and organizations, and in particular its relation to Russia. Then, this dissertation will look at Russian activity in both states and categorize these forms of activity according to the categories of methods as provided within the literature review. These are 1) information warfare, 2) cyber warfare, 3) proxy warfare, 4) economic warfare, 5) covert/clandestine operations and 6) political influencing operations. Often, these categories of methods are heavily intertwined. For example, a Russian social media activist operating within Estonia may be placed within both the information and proxy warfare categories. These cases of overlap will be highlighted and duly explained. Within the analysis section that follows the case studies section, this dissertation will look at Russian objectives within the respective countries, assess the potential success of their operations and discuss countermeasures. However, before discussing both case studies in great detail, the role of small states within international relations and the impact their foreign policy can or cannot have will be addressed, as both Estonia and the Netherlands are small in geographical size but are arguably overachieving in the international arena.

4.1 Small state foreign policy: The case for the overachiever

Defining a state as "small" is yet another topic of discussion within the field of international relations. In the simplest definitions, states are deemed small when they have fewer than 10 million inhabitants (Thorhallsson & Bailes, 2016). Even though the Netherlands exceeds this number at 17,5 million inhabitants, for the sake of this research the Netherlands, together with Estonia, is discussed as a small state within this section. There are good arguments for this: both Estonia and the Netherlands operate within international organizations such as

the EU and the UN as full members but with limited diplomatic capacity due to their size. As a result, such states need to make use of special features they may have to gain influence and defend their interests. Historically, in a system of international relations dominated by Realpolitik, these smaller states have always been more vulnerable. Lennart Meri, the first President of independent Estonia, argued that Estonia and the Netherlands endured this fate simultaneously in World War II, when the Molotov-Ribbentrop Pact did not only act as a precursor of the annexation of the Baltic states but also for the invasion and subsequent annexation of the Netherlands, Belgium and France (Smith, 2001). Meri held that the Pact enabled Europe's Great Powers to carve up the continent and used this historical event to argue that the security of European states is indivisible and that Europeans should strive for greater integration with one another based on common values and ideas, which would make the distinction between big and small states irrelevant.

The number of small states has multiplied in the wake of the Cold War and decolonization during the latter part of the 20th century. As a result, their presence and roles on the world stage have changed. Generally, we see a trend of small states successfully being able to exert their diplomatic capacity positively when they are able to build upon solid economic and administrative foundations at home (Thorhallsoson & Bailes, 2016). Katzenstein (1985) calls this "democratic corporatism", i.e., a social partnership between capital and labour, mediated by the government, which enables small European states such as the Netherlands to be adaptable and flexible to counter possible international volatility. Decisive and independent policymaking is another prerequisite for the success of a small state's foreign policy; without it, the state is toothless abroad. Alternatively, small states could opt to join international alliances in search of protection, thereby making up for their inherent weaknesses (Keohane, 1969). Such can be argued to be the case for Estonia, which sought integration with the West following its independence from Russia. By joining alliances and institutions such as the EU and NATO it has possibly prevented a fate similar to

that of Ukraine, a state which, lacking strong embedment in Western alliances, is now facing aggression from its much larger neighbour. Similarly, although in a different geopolitical context, after the Second World War the Netherlands proceeded to be one of the founding members of both NATO and the European Coal and Steel Community (ECSC), the predecessor of the European Union. NATO membership was deemed essential in countering potential aggression from the East during the Cold War and economic integration with Europe has been vital to the country's prosperity, as the Dutch earn nearly 80% of its national income from European trade. The Netherlands' membership of the EU has allowed its GDP to grow by 3.1%, making the Netherlands one of the countries that benefit most from EU membership (Freeman et al., 2022). Without this international cooperation, the Dutch economy as well as the extent of international influence would arguably not have reached the levels it has today.

The fact that both Estonia and the Netherlands hold membership in important international organizations such as the EU, NATO and the UN gives them the opportunity to exert influence on the international system. The Netherlands actively uses these platforms to promote human rights, international development and security and could be argued to be one of the prosperous small states that act as "norm entrepreneurs", which is also exemplified by the multitude of international law institutions that reside in the country, such as the International Court of Justice (ICJ) and the International Criminal Court (ICC) (Ingebritsen, 2002). Estonia often aligns itself with its Baltic neighbours Latvia and Lithuania to generate more leverage but does not shy away from agenda-setting on its own. During its presidency of the Council of the European Union in 2017, it named digitalization as its core priority, aligning all its other priorities to it (Panke & Gurol, 2018). This is a good example of how a small state like Estonia, which does not have a history of economic prosperity like the Netherlands, is able to effectively "export" its expertise in the field of digitalization and therewith exert significant influence, to the benefit of all

members of the EU. The COVID-19 pandemic showed Estonia's value to act as a leading country due to its experience in digitalization; it was the first country to implement vaccination certificates and was one of the strongest advocates of the EU-wide certificate. The World Health Organization (WHO) recognized Estonia's value as well by actively cooperating with the country in pursuit of worldwide certificates of vaccination (Paraskevopoulos, 2021).

To summarise, it is possible for small states to effectively exert diplomatic influence abroad and successfully pursue a foreign policy. However, this depends on internal cohesion and organisation as well as external diplomacy. It is arguably better for the interests of small states to actively participate and contribute within the international arena instead of merely allying themselves with a bigger state; if successful this enables the small state to have a significant impact and overachieve. Both Estonia and the Netherlands are testament to this argument.

4.2 Estonia: An Introduction

Estonia, together with Latvia and Lithuania, is one of the Baltic states, located in north-eastern Europe. It borders Latvia to the south, Russia to the east and the Baltic Sea to the north and west. With a total land area of 45,340 km2 and a population that amounts to approximately 1,35 million, Estonia has a population density of 30,6/km2 and is therefore one of the more sparsely populated European states (ERR News, 2023).

The demographics of Estonia are the result of historical trends but have been particularly influenced by the Soviet occupation of the country between 1944-1991, leading to a great influx of ethnic Russians. This has resulted in a demographic in which nearly a quarter of the population is ethnically Russian, as made visible in figure 1 below. Additionally, Estonia is host to a contingent of stateless persons, about 7% of the population, of which the majority is ethnically Russian (Lanoszka, 2016). These ethnic Russians are mainly

concentrated in regions that directly border Russia as well as in the urban region that surrounds the capital Tallinn, as shown in figure 2.

Figure 1: Estonian population distribution by ethnic nationality in % of the population (Statistikameet, 2021).

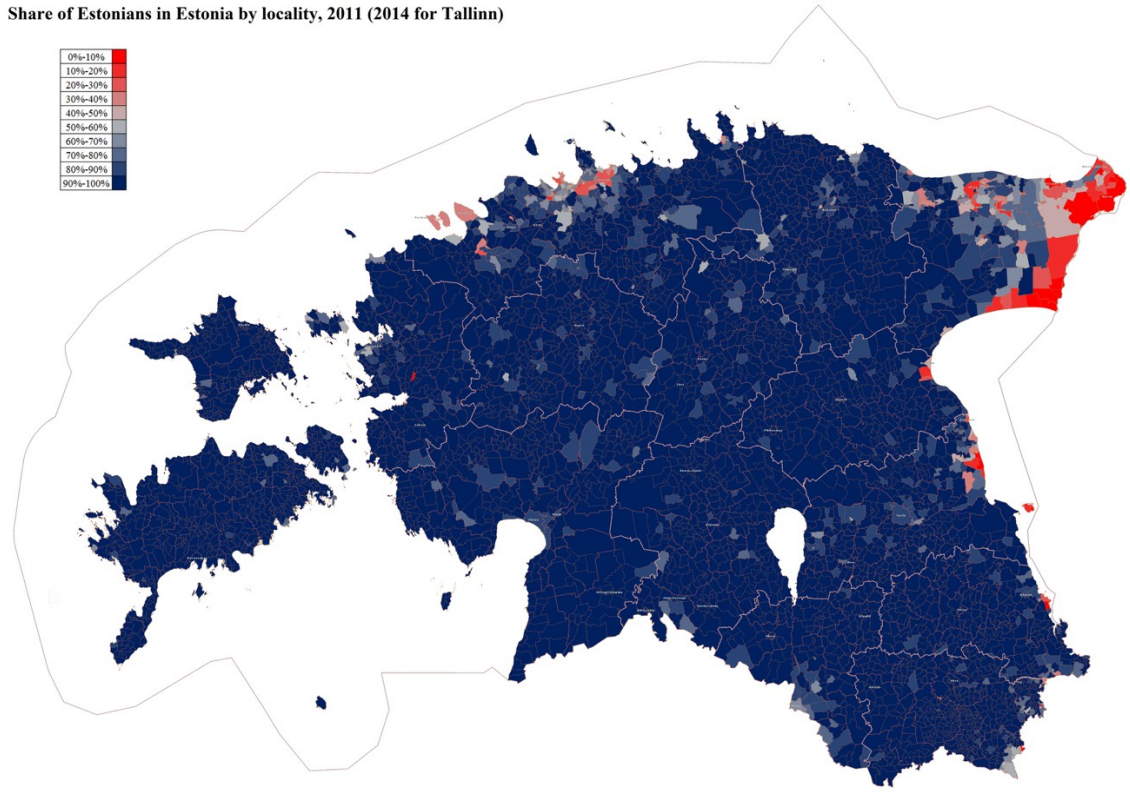

Figure 2: Share of Ethnic Estonians by locality (Statistikaamet, 2011).

Diplomatic relations between Estonia and Russia were established on the 2nd of February 1920, when the independence of the Republic of Estonia was

recognized by Soviet Russia. During the Second World War, Estonia was forcibly annexed by the Soviet Union in the summer of 1940 before being occupied by Nazi Germany in 1941. In the autumn of 1944, the Soviet Union reconquered Estonia. The Soviet occupation of Estonia lasted until 1991 when Russia officially re-recognized the Republic of Estonia. Since then, Estonia has progressively integrated itself within the Western international relations system, culminating in the country joining both the European Union and NATO in 2004, solidifying its attempt to move away from the Russian sphere of influence. Estonia has always seen the Soviet presence on its territory as a form of illegal occupation (Ashmore, 2009). These sentiments are particularly grounded in the Kremlin's attempt at Russifying Estonia by means of migrating hundreds of thousands of ethnic Russians to Estonia, a process that started as early as 1940 and was continuous throughout the Cold War (Herzog, 2011). It is thus needless to say that since Estonia regained its independence, bilateral relations with Russia have always been difficult. This difficult relationship is further highlighted by independent Estonia's refusal to grant automatic citizenship to ethnic Russians that settled within the country during Soviet occupation. Russia has used this "citizenship question" as a point of geopolitical leverage; it linked it to the issue of withdrawing of Soviet troops in the 1990s and later used it to question and undermine Estonian democratic credentials when the country was seeking to join the European Union and NATO (Smith, 2001).

Following its independence, Estonia's digital infrastructure was in a state of deficiency, with the World Bank declaring the country's telecommunication system "obsolete" (Budnitsky, 2022, p. 1919). Estonia urgently needed to modernize its digital infrastructure in order to be able to integrate with the West, all whilst having few (natural) resources at its disposal. Its industries were heavily integrated into the Soviet legacy of the past and under 50% of Estonians possessed a phone line. The first government of independent Estonia, a neoliberal coalition headed by 32-year-old prime minister Mart Laar, saw this

as an opportunity rather than a liability and opted to push for policies of extensive modernization and digitalization (e-Estonia, 2023). These policies catalysed Estonia's leap to gaining the reputation of being one of the most digitalized countries in the world today, a move that was characterised by its Tiigrihüpe (Tiger's Leap) program in 1996, which saw large-scale investments into Estonia's digital infrastructure through government partnerships with the private sector. The programme also put emphasis on education, resulting in 97% of Estonian schools having a functional internet connection by 1997 (Runnel et al., 2009). Continuous progress made Estonian society increasingly built upon its digital infrastructure. Today, 99% of Estonia's public services are available online, 24 hours per day, with divorce being the single service that still requires physical presence at a government office (e-Estonia, 2023). Services and activities such as banking, voting, studying and healthcare are all arranged online through a citizens' digital identification system. Whereas many of these services have become available in many countries in the space of the last decade, e-tax and e-banking were already started in Estonia at the turn of the century.

A heavily digitalized society holds many advantages but also makes Estonia an enticing target for cyber-attacks. A prime example of Russian interference in Estonia's cyberspace came in 2007 when Russia allegedly launched a large-scale series of cyber-attacks on the country, an event that later became known as "Web War I" (Blank, 2008b). In late April of that year, the Estonian government opted to relocate a Soviet-era World War II memorial from a park in the centre of Tallinn to a more remote military cemetery. Many Estonians saw the statue as a symbol of the Soviet occupation of Estonia and the site was regularly used as a gathering place for anti-Estonian extremists. Relocating the statue, however, immediately caused uproar and protests from the Russian minority in Estonia who clashed with the police in Tallinn, leaving a hundred injured and one dead (Kaiser, 2012).

What followed was a series of DDoS attacks on Estonian institutions such as the parliament, ministries, political parties, internet providers, news organizations and banks (Iasiello, 2013). Even though Russia denied any involvement in the attacks, and evidence of direct Russian involvement was not found, organizing the cyber-attacks would have been in Moscow's interests. Furthermore, experts as well as NATO and EU officials argued that such an attack could not have been orchestrated by a mere few individuals and "bore the hallmarks of something concerted (Herzog, 2011, p. 53). Furthermore, some of the IP addresses that were used by the hackers were in fact traced down to computers in use by Russian government officials. It is possible however that the perpetrators penetrated the Kremlin's networks in order to confuse investigators (Ruus, 2008). Whether the Kremlin gave the order for the attack or not, the event exemplifies the tense relationship between Estonia, Russia and the Russian minority within Estonia and definitely served as a wake-up call for Estonia. It also showed hybrid strategies at work; because the cyber-attacks were carried out covertly it was possible for Russia to make deniability plausible, whether Moscow was behind it or not. The unknown exact identity of the perpetrators also made it more difficult for the West to generate a clear and direct response, as the lack of clear evidence unwarranted any strong accusations towards Russia.

4.3 Russian hybrid warfare in Estonia post-2014

As discussed above, the historical relationship between Estonia and Russia is a burdened one, marked by decades of oppression (Ehin & Berg, 2016). Nevertheless, Estonia is host to a sizeable Russian minority and is thus seen as vulnerable to Russian hybrid warfare operations (Radin, 2017). In particular, since the annexation of Crimea in 2014, concerns that Russia may seek to exploit the Russian minority in Estonia in order to gain influence within the country and the larger Baltic region have become increasingly prevalent. Some in Estonia have compared the annexation of Crimea with the Soviet occupation

of Estonia in 1940, during which the Soviets orchestrated a rigged election that saw Estonia give up its independence "voluntarily" (Journeyman Pictures, 2017; Roberts, 1995; Kreegipuu & Lauk, 2007).

Russia's hybrid actions in Estonia are likely to be ambiguous, thereby impeding a swift response from the EU and NATO and undermining internal cohesion within the West. As we have seen within this dissertation, Russian hybrid warfare comes in various shapes and forms, and such is also the case within Estonia. Because of its successful development of resilient democratic institutions, Estonia is not a weak state. It is strongly embedded within Western organizations and alliances, which complicates Russian efforts to destabilize and manipulate the Estonian population. Tallinn is also not economically dependent on Russia and is in the process of separating its electrical grid systems from the Russian one, even though its gas supply, prior to the Russian invasion of Ukraine in 2022, did come primarily from Russia (Stoicescu, 2022) Furthermore, the political landscape does not feature a party that openly profiles itself as pro-Kremlin, although accusations of some party's connections with Russia do exist. Nevertheless, Estonia constitutes a different battlefield for Russia in comparison to Ukraine or Belarus and thus makes use of different hybrid weapons, that focus primarily on the Russian minority within Estonia as well as its highly digitalized society. The following section will look at cases of Russian hybrid interference within Estonia from 2014 onwards.

4.4 Information warfare: the Kremlin's prime tool in Estonia

In Estonia, Russian hybrid warfare is arguably most visible through its attempts at waging an information war within the country. The most principal tools of the Kremlin's information war against Estonia are its state-owned information channels Russia Today and Sputnik News which are specialized in spreading propaganda and disinformation. Following Estonian independence, these news organizations developed three main narratives about Estonia. First, they argued that Estonia is a fascist state, second, that the Russian minority in Estonia resides

in a divided nation and third, that Russia aims to protect the rights of Russian minorities abroad (Meister, 2018). In today's political context, in which Estonia is heavily embedded in Western international organizations such as the EU and NATO, these narratives remain. However, Estonia is no longer targeted on its own, as Russia understands that targeting a single state within a larger political body is not effective. Rather, Russian information warfare targets the organizations it has become a part of, thus constituting a shift in Russia's information warfare strategy. This shift is visible when we look at the most relevant government-discrediting narratives within Estonia. These include:

1. NATO is hostile, fragile and unpopular.
2. The West is corrupt, discriminatory, imperialistic and in decline.
3. Even though Russia is powerful, it remains a victim.
4. Poor governance plagues Estonia.
5. In Estonia fascism and Russophobia are prevalent.

(Veebel et al., 2021).

Pro-Kremlin narratives have been identified within Estonia as well. These include:

1. The West does not trump Russia, because the West is divided and weak.
2. There is no success in the liberal norms and values propagated by the West.
3. Migration, especially from the MENA and Sub-Sahel regions will disintegrate societies within the West.
4. Russia is the world's main defender of traditional values.

(Veebel et al., 2021).

This strategy of spreading anti-Western and pro-Kremlin narratives is chosen by Russia for several reasons. First of all, in Estonia, Russian TV channels are usually included in larger TV packages that are offered by the country's main internet and TV providers. As a result, nearly every Estonian TV customer has

access to Russian propaganda channels, thus providing a large spectrum of opportunities for information warfare. Because of this setup, the Estonian public contributes approximately 6 million euros in license fees and advertising to Russian channels (Ruussaar, 2018). Russian speakers within Estonia mainly consume these Russian state-controlled media channels and many within this group use TV as their prime source of information (Helmus et al., 2018). Even though much of the narratives that are being spread on these Russian channels would not pass a Western standard factual check, this is likely of little concern to the Kremlin as their strategic narratives are often aimed at those that are vulnerable or simply expect a certain worldview. This also makes it hard to debunk misinformation, as many websites or outlets that do so are not visited or believed by the main audience of pro-Russian sources (Veebel et al., 2021). Within Estonia, in order of prominence, language, geographical location, level of education and age are the most relevant variables in analysing support for Russian narratives. Illustrative of this is a 2020 study that found that 80% of Russian speakers in Estonia saw NATO as an aggressive organization whereas just 20% of Estonians viewed the alliance as such. Similarly, 70% of Russian speakers saw the Russian state as normal whereas less than 30% of Estonian speakers shared the same opinion (Veebel, 2020). It is important to note here that several Russian, as well as Belarussian TV channels have been banned following the outbreak of the War in Ukraine, for openly supporting or justifying Russia's military actions against Ukraine. However, these bans are often only temporary, and subject to review, with channels such as RTR Planeta, NTV Mir, Belarus 24, Rossia 24 and TV Center International receiving a 12-month ban in February 2022 (Vaino, 2022).

Discussing the leeway of Russian information campaigns in Estonia remains important even if some channels are receiving bans. These bans could be revoked or surpassed by means of the internet or VPN connections, and more importantly, TV channels are only one of many tools the Kremlin exploits to

spread disinformation. Social media such as Facebook, Twitter, Telegram and the Russian networks Odnoklassniki and Vkontakte are important in this regard, especially for the younger generations that prefer consuming news through the internet rather than traditional forms of media such as television. For example, prior to the European elections in 2019, automated bot accounts were reported to actively amplify content from Russia Today and other Kremlin-owned media outlets. Estonia was the main target of activity for anonymous Twitter accounts. Around NATO's "Spring Storm" military exercise in late April of 2019, 51% of all Russian Twitter messages were posted by bots, whilst groups on Vkontakte were also very active, posting approximately 70% of all posts concerning the military exercise (Biteniece et al., 2019).

Others are eager to disseminate pro-Kremlin rhetoric on social media without direct instruction or control from the Kremlin. This group of bloggers, social media activists, news sources or website moderators are best described as "useful idiots", a term attributed to Vladimir Lenin used to describe those individuals that promoted communist propaganda in the West (Safire, 1987). Today these are embodied in the abovementioned and their presence makes it more difficult to target Russian information warfare online because differentiating authentic views from state-spread narratives is often challenging. Accounts or websites may be genuinely attempting to have a discussion, albeit with pro-Russian arguments, or could be faking to do so, i.e., "trolling" (Helmus et al, 2018). The fact that this distinction is difficult to establish benefits the Russian state, for two reasons. First, it grants Russia plausible deniability from any involvement and allows the Kremlin to attack the West on its "infringement" of freedom of speech and second it hinders effective countermeasures due to confusion and ambiguity about the source of information.

Other tools at Moscow's disposal are pro-Russian NGOs, activists and discussion clubs such as Impressum. Impressum is known as a "discussion club" and acts as a platform for the circulation of pro-Kremlin talking points. It

actively contributes to the "construction of the mental characteristics of Estonian Russophones as a distinct community of conservative values, respectful attitudes toward the Soviet past, negative perception of Gorbachev's perestroika in the 1990s, and support for Russia's spill-over beyond the borders of the Russian Federation" (Makarychev, 2021, p. 57). These narratives are often both rational and emotional simultaneously, which, as Makarychev argues, attests to the argument that Russian propaganda is "cognitive", i.e. creating a set of beliefs within the Russian speaking communities within Estonia that circumvents rationality and reflective judgement (Makarychev, 2021; Brown, 2018). Impressum promotes a general sense of disdain for the West and its institutions and promotes their speakers' points as alternative narratives within global political debates, however rarely makes them engage in debates with speakers that hold opposing views, thus only widening the rift between Russian speakers in Estonia and the rest of the Estonian population, effectively contributing to the prevention of their integration into Europe by bringing upon them an environment of Kremlin-supported information.

Several NGOs and military-historical societies, such as "Front Line" play a significant role in promoting the concept of "Russkiy Mir", or Pax Russica, an ambiguous concept that is used to describe "Russianness". They participate in activities such as searching for remains of soldiers who fell in World War II (referred to by Russophones as the Great Patriotic War) and receive Russian awards for their merit (Postimees, 2011). Furthermore, even though there are no major pro-Russian political parties within Estonia, the Centre Party has shown its sympathy with the Russian minority and in part its pro-Kremlin narratives (Veebel et al., 2021). Other political parties, such as the nationalist, right-wing populist party EKRE (Conservative People's Party of Estonia) are ostensibly anti-Russian but nevertheless support and disseminate many narratives that are shared by the Kremlin, such as anti-EU, anti-same-sex marriage and anti-migration talking points (Petsinis, 2019). In 2019, the Russian Wagner Group

allegedly forged plans to support the party in the build-up to the 2019 European Parliament elections (Banco, 2023). The party was reportedly chosen for its talking points and its opposition to liberal parties. EKRE denied any ties with the Wagner Group and became Estonia's 2 nd largest political party at the 2023 parliamentary elections, which the party claimed were "stolen" due to the "unreliability" of e-voting (Mac Dougall, 2023). Furthermore, EKRE has openly questioned the military and economic support that Estonia continues to provide to Ukraine as well as Estonia's persistent welcoming of Ukrainian refugees (Jakobson & Kasekamp, 2023). All in all, EKRE is best placed with the abovementioned bloggers, social media activists, news sources and website moderators that fall within the "useful idiot" category. The party does not openly support Russia but does promote many of its eastern neighbour's narratives, thus aiding the Russian cause in the long term.

Arguing that parties such as EKRE, news channels or individuals are acting as Russian proxies is often difficult since money flows and funding patterns are usually obscured from the public eye. With the exception of TV channels that originate within Russia, such as Russia Today, declaring an entity a Russian proxy should be done cautiously. However, we do know that Russia persistently attempts to influence and support protest movements abroad that support its narratives. It is important to note that such support does not necessarily have to be embodied in money; support can also be given through the provision of relevant information, strategies, personal connections or other factors that can positively influence an information campaign. It is also rather unnecessary to have a semantic discussion on whether something is an example of a proxy or a "useful idiot". What is evident and important is that there is an information war being waged within Estonia, one that the Estonian authorities and population are aware of, but nevertheless remains difficult to navigate. Vigilance is required in regard to continuing to counter pro-Kremlin narratives going forward, because new narratives may arise every single day, narratives that ask new

questions and attempt to influence people in new ways. What is certain is that Moscow is playing the long game when it comes to information campaigns in Estonia and is making use of a great variety of actors, requiring a long-term as well as a short-term counter-strategy.

4.5 Cyber warfare & Estonia: lessons from 2007

Estonia is one of the most digitalized states in the world and thus potentially vulnerable to cyber warfare. Tallinn learned its lessons from the large-scale attacks in 2007, and cybersecurity is a top priority within Estonia, the necessity for which was once again made evident in August 2022, when Estonian officials claimed to have repelled the most extensive cyber-attacks since 2007, following the removal of Soviet memorials in the eastern city Narva, where the majority of the population is Russian speaking (Sytas, 2022). The pro-Russian and Russia-based hacker collective Killnet claimed responsibility for the attack (Davies, 2022).

The question that arises is whether Estonia remains vulnerable to Russian cyber-attacks more than 15 years after the events of 2007. At a glance, it would seem that Estonia has successfully invested in cyber defence in the wake of 2007. Despite the attacks of August 2022 being the most extensive since 2007, the attacks went largely unnoticed within Estonia (Davies, 2022). The successful repelling of attacks does however not mean that attempts at penetrating Estonia's cyberspace are decreasing; in 2022 a total number of 302 denial-of-service (DoS)[2] attacks were reported, primarily carried out by pro-Russian

[2] A denial-of-service (DoS) attack is a cyberattack that makes a computer or other device unavailable to its intended users. This is usually accomplished by overwhelming the target (e.g., government or bank website) with visitors until normal visitors can no longer be processed due to an overload or "flood" of requests (Frankenfield, 2023).

hackers, which was a fourfold increase in comparison to 2021 (Oyetunde, 2023). Even though most cases of DoS attacks originate from foreign electronic devices, some originate from Estonian IP addresses. In many of these cases, the owner of said device is not aware of the malware and the Estonian government is making efforts to raise its citizens' awareness to update their software frequently (Republic of Estonia Information System Authority, 2022). Regarding these attempts, it is important to note that distinguishing Russian cyber warfare from its efforts at information warfare is virtually impossible, the two are heavily intertwined (Geers, 2015). This points towards the broader notion that is relayed within this dissertation that Russia lives in a "constant state of siege", including various forms of hybrid warfare (Blank, 2016, p. 82). As a matter of fact, the Kremlin refers to terminologies such as the internet, telecommunication networks and information technologies as parts of its information infrastructure, thus hinting at its inherent connection with information warfare (Rashid et al., 2021).

The 2007 attacks showed Estonia and the world that cyber-attacks do not limit themselves to a single institution or target but are rather capable of threatening a state's national security as a whole. The wake-up call of 2007 brought about a series of changes within Estonia that were aimed at bolstering its cyber defence. The Estonian government adopted a number of policies such as the Action Plan to Fight Cyber-attacks (2007), the Cyber Security Strategy (CSS) (2008) and the National Security Concept (2010) to generate a comprehensive policy response to Russian cyber aggression (Czosseck et al., 2011). A "cyber security culture" were to be developed within Estonia, which requires organisational, legal and technical changes (Cyber Security Strategy Committee, 2008). The CSS formulated five main strategic objectives and policies:

1. The development and large-scale implementation of a system of security measures.
2. Increasing competence in cyber security.

3. Improvement of the legal framework for supporting cyber security.
4. Bolstering international cooperation.
5. Raising awareness on cyber security.

(Cyber Security Strategy Committee, p. 3-5, 2008).

Today, the Estonian government publishes a report on the status of its cyber security annually and is continuously working to improve the cyber security of the state and its citizens. Special awareness-raising campaigns have been aimed at the Russian-speaking population, who generally perform worse at "cyber hygiene", the efforts that one makes to improve their online security (Republic of Estonia Information System Authority, 2022).

For the Kremlin, cyber warfare cannot be seen as separate from information warfare and as we have seen Moscow's efforts in the latter have been extensive. Within the cyberspace however, the events of 2007 proved to be an effective admonition. Estonia developed a robust set of policies to improve its resilience to cyber warfare and even though the number of attempts to transcend these defences has not fallen but rather increased, they have not brought much inconvenience upon Estonian citizens. It can be said the Estonian efforts at securing its cyberspace have thus been rather successful, but the state must remain wary, as developments within the field of cyber warfare often come quickly, requiring effective and rapid response.

4.6 Economic warfare in Estonia: independence pays off

Even though Estonia is not economically dependent on Moscow, the close proximity of the two countries has naturally led to Russian attempts to gain influence within Estonia through means of economic warfare. The following section will discuss Estonia's economic relationship with Russia and the Kremlin's efforts to gain influence within Estonia by economic means. As of 2020, Moscow was Tallinn's fourth-largest import and export partner, however

the ongoing conflict in Ukraine is likely to affect this (World Bank, 2020). Estonia's economy saw its GDP grow by 8.3% in 2021, but again Russia's aggression towards Ukraine is likely to dent economic progress, with the country being less attractive for investors due to its close geographical proximity to Russia, the negative effects of which are expected to be most noticeable in the country's eastern regions (Tverdostup, 2022).

When it comes to economic warfare and Russia, emphasis is often put on the Kremlin's capability of exerting pressure abroad through its control of energy sources such oil and natural gas. In the case of Ukraine, Russia repeatedly cut off, or threatened to do so, Ukraine's energy supply. The Kremlin even went as far as to bypass Ukraine by constructing the Nord Stream gas pipeline, with the delivery of its successor Nord Stream 2 only being cancelled after the outbreak of the War in Ukraine.
Estonia is a state that was heavily and rapidly industrialized during Soviet occupation, a process that required fuel imports to continue to progress. Despite the need for these imports, Tallinn already produced 51% of the energy it consumed itself in 1991 (Clemens, 1999). Since then, Estonia has effectively navigated Russian attempts to frustrate its energy security and is today known as one of the most energy-independent nations worldwide, mainly due to its significant reserves of shale oil (Zeng et al., 2017).

What problematizes Russian efforts to exert economic pressure over Estonia is the fact that most Estonians are richer and enjoy better living conditions and services than most Russians. Unlike in Eastern Ukraine, a region that was economically neglected and under-developing for decades, the Estonian government actively invests in its Russian-speaking regions, taking away a potential argument for secession. As a matter of fact, many ethnic Russians would not move to Russia if given the chance, because of economic reasons. Efforts were made by citizens of the Russian town of Ivangorod, which borders

the Estonian city of Narva, to join Estonia on multiple occasions, due to better living conditions and the "feeling of neglect" on the Russian side (Lagnado, 1998; Radio Free Europe, 2010).

As a result of Estonia's relatively strong economic position, attempts at "economic warfare" by the Kremlin fall short and result in endeavours that try to spread instability, distrust and fear about the state of Estonia's economy and should therefore rather be placed within the "information warfare" category. For example, Russia attempted to convince its target audiences within Estonia that the crisis caused by the COVID-19 pandemic was negatively affecting its economy rapidly. Simultaneously, Moscow went for the bigger picture by claiming that the EU was no longer financially able (or interested) to provide aid to Estonia (Veebel et al., 2021). Rather than serious economic warfare, the Kremlin's attempts are better described as a sort of economic blackmail, deception and intimidation. However, it remains of utmost importance for Estonia to keep addressing existing socio-economic issues, especially those that concern its ethnic Russian minorities, as these are vulnerable targets for Russian (economic) narratives.

4.7 Russian political influencing operations & covert action within Estonia

Finally, Russia makes use of traditional diplomacy to support narratives within Estonia that the Kremlin prefers. Traditionally, Moscow does this by inviting leaders of pro-Russian factions to the Kremlin and openly supporting specific pro-Russian parties (Chivvis, 2017). In the case of Estonia, with its history of troubled relations with Russia, this is more difficult as openly friendly rhetoric with and towards Russia is generally not appreciated within Estonian society. Despite this, the Estonian Centre Party, described as populist and centre-left, signed a cooperation protocol with United Russia, the party of Russian President Putin in 2004. In the two-page document, the common interests and goals of the parties are declared, and a framework of mutual cooperation is defined (Cavegn,

2016; Bil, 2022). Even though the party declared on multiple occasions that the cooperation "has never been put in practice", it was only fully annulled following the Russian invasion of Ukraine in 2022 (Martyn-Hemphill, 2021; Whyte, 2022).

As discussed before, Russia makes use of (social)media and high-level meetings to support its allies and discredit its opponents but also offers them covert financial assistance if required (Thomas, 2020). Even though direct evidence of Russian financial support of Estonian political organizations is hard to obtain due to its covert nature, we know from other post-Soviet spheres such as Moldova, Georgia and Ukraine that financial support of such organizations is amongst the Kremlin's toolkit, making it highly likely that such support operations also occur in Estonia (Saari, 2014). They therefore constitute an important area of study.

Russian political influencing operations in Estonia are mainly focused on gaining a foothold in Estonia's democratic institutions, such as its parliament. These efforts naturally intertwine with its information warfare campaigns, because both aim to discredit the Estonian political establishment whilst propagating pro-Kremlin narratives. Russia is arguably succeeding in this process as the Riigikogu, the Estonian parliament, plays host to a sizeable opposition that includes both the EKRE and Centre parties that are known to promote standpoints that often fit and align with Russian interests.

4.8 Conclusion

Being its smaller neighbour, Estonia has had a long history of often difficult relations with Russia. These difficulties did not dissipate following the country's independence in 1991 but rather adopted different shapes and forms. Russia's prime tool in Estonia is its information warfare, which aims in particular at the Russian minority that makes up 1/4 th of the Estonian population. This is done through the spreading of various narratives that discredit the Estonian

government and its legitimacy, but also the international organizations that Estonia became part of following its independence, such as the European Union and NATO. Information warfare is the spearhead of Russian hybrid efforts within Estonia because the Kremlin sees it as having the most potential for reaping benefits. After all, Estonia has done a significant job of improving its capabilities to defend itself from cyber and economic warfare. On cyber, Estonia has learned valuable lessons from the cyber-attacks of 2007 and even though Russian cyber-attacks still almost occur daily, Estonia's defence systems are now up to par, resulting in Estonians noticing little to nothing from Russian efforts to breach their cyberspace. Economically, Estonia is not dependent on Russia due to successful efforts made at reforming its economy, especially its energy sector. Prior to the Russian invasion of Ukraine, Estonia annually exported more goods to Russia than it imported. It is important to note that there are significant groups of people within Estonia that either support Russian narratives or are unaware of the fact they support (political) organizations that disseminate pro-Kremlin views, intentionally or not. The Estonian Parliament is host to sizeable opposition that previously held links with Russia and propagates similar views on issues such as the EU, same-sex marriage and migration.

Estonia seems well aware of the threats it faces and has made many efforts to prepare itself for these threats as well as counter them. Vigilance is required, as the Russian effort is long-term and operates in intricate, ever-evolving ways. For those outside Estonia, it is important to remain watchful, take lessons where possible and provide aid where required.

4.9 The Netherlands: An Introduction

The Netherlands is a state in western Europe that is bordered by Germany to the east and Belgium to the south. Together with Belgium and Luxembourg, it is often grouped as the Benelux or Low Countries. It has a total land area of 42,531 km2, making it smaller than Estonia in size but it houses an approximate 17,8

million inhabitants, making it one of the world's most densely populated countries with a population density of 532/km2 (Centraal Bureau voor de Statistiek, 2023).

Unlike Estonia, the Netherlands is located far from Russia and therefore lacks a sizeable Russian minority. Interstate relations between the Netherlands and Russia do go back far, however, with Tsar Peter the Great visiting the country at the end of the 17 th century (Van Der Oye, 2010). Since its independence from Spanish rule in 1648, the Netherlands has only been occupied twice; by France, following the French Revolution, and in World War II by Nazi Germany. In both of these cases, Russia/USSR also faced invasions, by France in 1812 and by Nazi Germany in 1941. The Russian/Soviet efforts to repel these attacks indirectly played a major role in the restoration of Dutch independence in both cases, as the failure of the French and Nazi campaigns in Russia spiralled into the decline of these powers, enabling the Dutch to regain independence. In spite of this, the Dutch did not grant the USSR diplomatic recognition until 1942 when the USSR joined the allied coalition against Nazi Germany, in part because the Soviets' previous alliance with Nazi Germany had enabled the latter's aggression towards Western Europe at the beginning of the war (Ter Haar, 2017). Following World War II, the Soviet Union and its Warsaw Pact allies were seen as a severe threat to national security, a factor that motivated the Netherlands to become one of the founding members of both NATO and the ECSC. When the Cold War drew to a close, relatively amicable relations between the Netherlands and Russia ensued, with the two countries celebrating a "friendship year" in 2013 to mark 400 years of bilateral relations.

As the Netherlands is one of the founding members of the European Union and NATO, its post-World War II position on Russia is heavily related to these institutions' relations with Russia (David et al., 2013). As early as in 1974, Dutch foreign policy has been described as "reactive rather than active" and characterized by "sitting on the fence and reacting only to external impulses"

(Van Staden, 1974, p. 300). Fifty years later, this reflection still largely holds. Dutch security is guaranteed by the U.S. through the NATO alliance, for which the Netherlands supports American foreign policy in return. This relationship is visible in the Dutch support for U.S.-led military operations in Iraq as well as Afghanistan (Ter Haar, 2013). Recently, efforts in Europe and the Netherlands have been made to increase the EU's strategic autonomy from the U.S. and others, an effort to which the Netherlands is actively contributing, for example by producing several policy papers on the issue, together with the Spanish government (Korteweg et al, 2022). However, the idea of EU strategic autonomy is still relatively new, and it is highly likely the U.S. will remain an extremely important player in Dutch foreign policy for the foreseeable future.

The economy of the Netherlands is historically affluent, ranking 15th in the world as of 2022 (Rodriguez, 2022). In part, this is the result of a steady income from natural gas resources in the northern Groningen province as well as foreign trade. In 2021, Russia imported a total of 7.6 billion USD worth of goods from the Netherlands. On the other hand, the Netherlands imported 39 billion USD worth of goods, of which 87% were mineral fuels, making the Netherlands Russia 2nd largest export partner (Centraal Bureau voor de Statistiek, 2022; OEC, 2022). In 2007, the Dutch energy company Gasunie signed a multi-million deal with the Russian state-owned energy corporation Gazprom, effectively binding its energy supply to the fickle of the foreign policies of the Russian state (Brandt Corstius, 2007; Lazaroms, 2014). Despite concerns, the deal was pushed through by the Dutch government, which argued that economic relations with Russia could provide inroads to influence and promote the development of a stable democracy within Russia. The Netherlands' relative dependency on Russia for its supply of fossil fuels prior to the Russian invasion of Ukraine in 2022 naturally created a window of opportunity for Russia in the field of economic warfare vis a vis the Netherlands, which will be discussed further within the following sections. The Dutch energy dependency is not the

only field that might attract Russian interference through hybrid strategies. The Netherlands is renowned for its efforts to promote the principles of international law and human rights and has as such attracted various international organizations to the country, which reside primarily in The Hague. These include the International Court of Justice (ICJ), the International Criminal Court (ICC) and the Organization for the Prohibition of Chemical Weapons (OPCW) which form valuable targets for Russia, and in particular its networks of cyber attackers, as Russia has often been accused of breaching norms and laws set by these organizations.

The Netherlands is one of the most digitalized, open and free societies in the world and therefore eminently vulnerable to Russian interference. Its democracy is known to be strong, coming in at rank 9 in the 2022 Democracy Index (Economist Intelligence Unit, 2022). As discussed within the literature review, being a strong democracy is an asset but also has its vulnerabilities. Actors with malicious intent can attempt to exploit the freedom of expression, press and media by driving wedges within democratic societies, with the goal of undermining governments and other democratic institutions as well as weakening their resolve (Wigell, 2019). Such a threat also faces the Netherlands. We will see in the upcoming sections that Russian hybrid efforts have primarily focused on the opportunities granted to them by the Dutch democratic system. For example, Russians were accused of exploiting a referendum in relation to the proposed EU association agreement with Ukraine and making use of social media to spread Kremlin-supported narratives. Furthermore, individuals can be identified that, consciously or not, propagate Russian talking points, the so-called “useful idiots”.

4.10 Russian hybrid warfare in the Netherlands post-2014

As described above, there are many factors that make the Netherlands an attractive target for Russian hybrid warfare operations. It is a key member of the

EU as well as NATO and plays home to various international organizations, in which Russia has continuously attempted to drive a wedge. Furthermore, its open society opens up opportunity for Russian misinformation and its relative dependency on Russian gas make it energy sector vulnerable to Russian malintent. Whereas these points were evident prior to 2014 as well, Russian hybrid operations in the Netherlands have significantly increased post-2014. This development is heavily related to the Euromaidan protests that started on the 21st of November 2013 and culminated in the removal of Ukrainian President Viktor Yanukovych on the 22nd of February 2014 (Kuzio, 2018). This was the direct result of the Ukrainian President's sudden refusal to sign the European Union – Ukraine Association Agreement. The crisis that ensued, resulting in the annexation of Crimea and the start of the Russo-Ukrainian War, relates to the Netherlands' susceptibility to Russian hybrid warfare operations for three main reasons:

1. The Netherlands, as a member of the European Union, naturally became involved in the Euromaidan crisis. This was further highlighted by the Dutch Member of the European Parliament Hans van Baalen travelling to the Euromaidan protests, proclaiming to the crowd that "the will of the people has triumphed' (Lazaroms, 2014). The crisis caught the EU by complete surprise and spilt over into the national politics of the Union's member states (Zelinska, 2017).
2. The downing of the passenger flight Malaysia Airlines Flight 17 (MH17) over Russian-controlled eastern Ukraine on the 17th of July 2014 caused a huge international uproar and especially in the Netherlands since 196 of the 298 persons on board had Dutch nationality. It was described as the "greatest war crime against Dutch civilians since World War II" (Klein, 2019). The Netherlands declared a day of national mourning on the 23rd of July, the first time the country had done so since the passing of Queen Wilhelmina in 1962 (NOS, 2014). Following the disaster, the

Dutch hosted the Joint Investigation Team (JIT) which was responsible for leading the international investigation on identifying the culprits.

3. In April 2016, the Netherlands held an advisory referendum to approve or disapprove of the Dutch signature to the European Union – Ukraine Association Agreement. This referendum is clouded in controversy because of alleged Russian attempts to influence voters and the idea that many voters used the referendum to express their concerns about the EU in general rather than the Association Agreement itself (Otjes, 2016; Smeets, 2016).

Some cases of Russian hybrid interference in the Netherlands post-2014 relate to the factors mentioned above, but not all. In other cases, they are related to the Dutch (cyber) infrastructure or international organizations that reside within the country. The following sections will discuss these cases in greater detail.

4.11 Information warfare in the Netherlands: far from the Kremlin, yet vulnerable

In the Netherlands, information warfare is arguably the most well-known and prevalent form of Russian hybrid warfare. Even though the country is located far away from Russia, it remains a member of European institutions that the Russians perceive as a threat, such as the EU and NATO. Russia therefore continuously attempts to gain influence within the country and create and exploit divisions.

Even though the Russian state-owned information channels Russia Today and Sputnik News were banned following the 2022 Russian invasion of Ukraine, these media outlets have long spread antagonistic narratives about the Netherlands, which at times have even trickled and filtered into the mainstream as well as alternative Dutch media (Schellevis & Kasteleijn, 2022; Kouwenhoven & Heck, 2020). In 2020, the Dutch Ministry of the Interior

reported that pro-Russian media were conducting information campaigns within the Netherlands regarding the COVID-19 pandemic (Volkskrant, 2020). An interesting shift in the portrayal of the European Union, and thus the Netherlands, by Russia occurred following the 2014 Russian-Ukrainian crisis, as Russian narratives became more hostile and put "increased emphasis on the fragmented and therefore weak nature of the EU" (Chaban et al., 2017, p. 495). Chaban et al., argue that this change of narrative was a direct result of the EU publicly raising objections against Russia.

In the case of the Netherlands the turning point in relations with Russia, and the kickstart of the latter's information warfare in the Netherlands, was the downing of flight MH17 as described in the previous section. Because the largest portion of victims had the Dutch nationality, the international investigation team (JIT) operated from the Netherlands and charges were formulated by Dutch public prosecution. Alongside the JIT, the Dutch Safety Board carried out a simultaneous investigation. Both investigations concluded that MH17 had been shot down by a BUK-TELAR rocket system believed to have been transported from Russian territory on the day of the downing (Joint Investigation Team (JIT), 2016; Dutch Safety Board, 2015). The Dutch public prosecutor charged four individuals, three of whom were Russians, for shooting down the aircraft (Hoyle et al., 2021). From day one there were intense Russian efforts at spreading disinformation, bizarre theories and other pieces of information concerning the crash. Theories varied from the plane having been loaded with corpses at Amsterdam Airport by the CIA in an effort to discredit Russia, to the shooting having been a mistake with the real target being Russian President Vladimir Putin's private aircraft (De Vreij, 2016; Brown, 2015). The plethora of theories did not have the purpose of uncovering the true fate of MH17. Rather, their goal was to sow confusion, doubt and division among those that accused Russia. It serves as a classic example of creating a front of plausible deniability and deflecting blame, not only with the goal of dividing individuals, but also

with the intent of questioning the integrity and neutrality of judicial investigations and thereby one of the key pillars of the Dutch democratic system (Van Der Togt, 2016).

One could think that sentiments within the Netherlands took a negative turn for Russia in the aftermath of the downing of MH17. However, this is only partly the case, which is evidently shown by the referendum on the EU's Association Agreement with Ukraine that was held on the 6 th of April 2016. In the referendum, voters were asked the following question: "Are you for or against the Approval Act of the Association Agreement between the European Union and Ukraine?" (Visser, 2015). A majority of 61% voted "Against", with a turnout of 32.2%, just 2.2% above the 30% threshold for validity. Amongst some academics, policymakers and analysts there exists the belief that the primary concern of voters in this referendum was Ukraine and its Association Agreement with the EU. This is incorrect. Rather, the referendum was hijacked by anti-EU activists, bloggers and politicians, who declared "they did not care about Ukraine" (Heck, 2016). Additionally, the EU had previously adopted similar treaties with dozens of states, such as Chile, Georgia, Moldova and Jordan, to which no objections were made (De Jong, 2016; Applebaum, 2016). Before its repeal in 2018, included in Dutch law was the Advisory Referendum Act which made it possible to hold a non-binding referendum over most types of primary laws. The initiators of the referendum intended to hold a referendum on Dutch membership of the European Union, similar to the Brexit referendum, but this was impossible unless the government would initiate it. Therefore, they took on the case of the Association Agreement as a quasi-approval vote for Dutch membership of the European Union (Otjes, 2016).
For the Russian state, the true intention behind the referendum was less relevant since, in any case, the vote provided an opportunity for their anti-EU narratives. The Dutch rejection of the Association Agreement was therefore labelled a "propaganda triumph for Putin" (Umland, 2016). Anti-EU narratives were not

just spread by the Kremlin through their usual channels but also repeated by the "no" campaign. Many of the narratives spread by the no campaign in the lead-up to the vote had eerily close similarities with statements on Russian state media such as Russia Today and Sputnik News. Those propagating a no-vote made various false claims about Ukraine and the Ukrainian population such as:

1. As a condition for the treaty, Ukraine would have to give up its free trade with Russia.
2. Ukraine is thoroughly corrupt and ruled by fascists, anti-Semites and ultra-nationalists.
3. Half of the Ukrainian population opposes the treaty.

(Janmaat & Kuzio, 2016; De Jong, 2016)

Arguably one of the first examples of direct Russian influence within the Netherlands came in January 2016, in the build-up to the referendum, when a video was released in which the Dutch population was warned of terror attacks in the Netherlands if the Dutch were to vote "no" in the referendum. In the video, supposed members of the right-wing, anti-Russia Ukrainian Azov battalion could be seen setting fire to a Dutch flag, however the Ukrainian government held that the video was a provocation, and the video was later found to have been produced within Russia (Smeets, 2016). Despite this, the video was quickly disseminated by Dutch organizations that supported a no-vote in the referendum such as GeenStijl and The Post Online as a "threatening video from the Ukrainian camp" (Smeets, 2016). This event, amongst others, strongly raised awareness amongst the Dutch of the Russian hybrid threat and moved the Netherlands to increase its military cooperation with partner countries, such as Germany (Van Der Kaaij, 2016).

In 2017, The New York Times revealed how left-wing Member of Parliament Harry van Bommel made use of a so-called "Ukrainian team" in the run-up to

the referendum that attended public meetings, television programs and used social media to denounce Ukraine. Whereas the public was made to believe these individuals were discontented Ukrainians, most members of the team were in fact from Russia or the breakaway, "separatist" regions of eastern Ukraine (Higgins, 2017; De Boer, 2017). It remains unclear if these individuals were directed by the Kremlin or were merely acting out of shared interests. We see here a recurring problem with distinguishing people that genuinely want to voice their opinion and those that are trolls, sponsored by the Russian state. This ambiguity makes it relatively simple for Moscow to deny any involvement.
In 2020, the Dutch television program Zembla uncovered WhatsApp messages of far-right populist Thierry Baudet, which appeared to show discussions about payments received from Russia (Lamond & Bergmann, 2020). The politician denied the accusations, arguing the messages were merely a "playful exaggeration" (Schaart, 2020). As this dissertation has discussed, funding preferred political leaders is one of the most effective means of promoting one's own narratives abroad, but uncovering and identifying illicit forms of financial support often remains incredibly difficult.

The deterioration of relations between the Netherlands and Russia, in part described in the examples above, has contributed to Russian state-sponsored propaganda channels constructing an image of the Netherlands as a country in a state of "liberal chaos". Hoyle et al. identified six antagonistic narratives spread by Russia Today (2019):

1. The Netherlands is a dangerous society, violence and crime are prevalent. It is portrayed as a state that has rising (narco) crime and violence levels as well as a rise in terrorist attacks. Incidents such as shootings are amplified, including graphic imagery. The main objective of this narrative is to portray the Dutch state as weak and in disarray, therefore incapable of organizing its defence when required.

2. The Netherlands is a weird society, it is eccentric and dominated by hyberliberalism. Within this depressing and demeaning narrative, the Dutch state is shown to be overly progressive, too "woke" and disrespecting traditional values. This narrative is part of a larger Russian narrative that argues that European societies are in decay. By ridiculing the Dutch and attacking Dutch morals, an attempt is being made at tarnishing its international reputation.
3. The Netherlands has a vendetta against Russia and is home to extensive Russophobia. In this regard, Dutch politicians are cited, such as the far-right PVV MP Geert Wilders (RT, 2018). This narrative also responds to the MH17 investigation, in which RT claims counter explanations are being "ignored" and reporting is "biased". In the meantime, those in the Netherlands who propagate Russian-friendly narratives, such as Wilders but also Baudet, are granted positive reporting, with the goal of steering the political discourse within the Netherlands to a more pro-Kremlin direction.
4. The Netherlands is a nuisance and a troublesome international actor. This narrative portrays the Netherlands as a reckless and destructive geopolitical actor, arguing that it operates selfishly during financial crises in the Eurozone, and refuses to provide sufficient aid to other European states in the wake of the COVID-19 pandemic, thereby illustrating the Netherlands' damaging influence on European unity. The goal of this narrative is to damage the reputation of the Dutch as a reliable ally.
5. The Netherlands is a divided society, which is at war with itself. This narrative holds that there exist deep-rooted divisions within Dutch society. It addresses internal issues such as climate policy, COVID-19 deniers, anti-Islam movements and anti-racism protestors. Again, violence is amplified, as well as protests, together with extensive use of graphic imagery. The objective is to create an image of the Netherlands

as a state that is not in order, and incapable of organizing its defence, with a special focus on conservative groups that "fight" to cling on to "traditional values".

6. The Netherlands is home to foolish institutions which are incompetent, laughable and disingenuous. This narrative aims to discredit and denigrate Dutch institutions and authorities. Mere incidents are amplified, such as the damaging of fighter jets by the air force or false alarms at Schiphol airport (RT, 2020a; RT, 2020b). Other targets of degeneration are the police and political institutions. Portraying the institutions of the Netherlands as such heavily contributes to creating an image of a disorganized and disingenuous state, an image which aims to reduce citizens' trust in their institutions.

We have seen that even though the Netherlands is located far from Russia geographically, the Kremlin's efforts at waging an information war within the Netherlands are clearly visible. Russian state-sponsored media outlets such as Russia Today systematically spread antagonistic narratives about the country with the goal of destabilizing the country and disenfranchising Dutch citizens from its governmental institutions. Furthermore, several events, such as the Euromaidan protests, the downing of flight MH17 and the Dutch referendum on the EU's Association Agreement with Ukraine have advanced the Kremlin's targeting of the Dutch. Even though Dutch authorities seem aware of this development, and counter-efforts have been made, the Netherlands, with its highly volatile political climate, remains a breeding ground for individuals and groups that are susceptible to Russian disinformation. For the Dutch, the battle against Russian information warfare is likely to be a continuous one, since Russia is expected to continue its attempts at exploiting the various freedoms that are rooted within the Dutch democracy for their own benefit.

4.12 Russian cyber warfare operations in the Netherlands

The Netherlands is an attractive target for Russian cyber warfare due to its highly digitalized society and the presence of international organizations such as the Organisation for the Prevention of Chemical Weapons (OPCW) that engage in investigations and possess pieces of information that are sensitive to Russia.

The downing of flight MH17 and the subsequent criminal investigation as well as court case that was held in the Netherlands against the perpetrators brought upon the Netherlands an increased interest of Russian hackers. In 2017, it was revealed that the Dutch Security Board had narrowly avoided a Russian hack by a spear phishing email in 2015 (Meeus, 2017). The event took place two weeks after the Board's report on MH17 was finished and two weeks before its publication to the public. In 2016, cybersecurity company TrendMicro published a report which argued that the failed hacking attempt was part of a Russian hacking group participating in Operation Pawn Storm, a cyber espionage campaign with affiliations to the Russian government (TrendMicro, 2016).

In 2017, the Dutch police force, which at the time was also investigating the downing of MH17, was penetrated by Russian hackers. The intrusion, which was revealed only in 2021, was not noticed by the Dutch police force but came to light as a result of AIVD intelligence (Modderkolk, 2021). These events can be seen as a pattern of Russian attempts to sabotage and undermine the criminal investigation into the MH17 disaster.

Russia has been known to deploy hacker groups that target Western democracies, their elections and institutions. Two relatively well-known hacking groups are Cozy Bear and Fancy Bear, believed to be led by the Russian Foreign Intelligence Service (SVR) and the Russian Foreign Military Intelligence Agency (GRU) (Nakashima, 2016). In 2018, it was revealed that

the Dutch General Intelligence and Security Service (AIVD) discovered Cozy Bear's intrusion into the American Democratic National Committee, in an attempt to influence the U.S. Presidential elections of 2017 (Modderkolk, 2018). Cozy Bear and Fancy Bear also targeted the Netherlands itself. One of these intrusions, into the Dutch police force, was discussed above. Other events occurred in February 2017, when the AIVD announced both hacking groups had made several attempts to encroach on Dutch government ministries in an attempt to gain access to sensitive and secret documents (Modderkolk, 2017). In response, Dutch authorities moved to abandon electronic vote counting, opting for the votes to be counted manually in upcoming elections to avoid any risk of Russian interference (Limnell, 2018; Cerulus, 2017).

In October 2018, the Dutch Military Intelligence and Security Service (MIVD) announced that it had prevented a Russian hacking group from intruding into the OPCW (Ministerie van Defensie, 2018). The four Russians that were conducting the operation were identified as GRU agents and subsequently expelled to Moscow after they were found to attempt hacking into the Wi-Fi networks of the OPCW. The exact motives of this operation remain unknown, but at the time of the apprehension, the OPCW was carrying out research on alleged Russian involvement in the case of the poisoning of Sergej Skripal and the Douma chemical attack in Syria (Crerar et al, 2018; Henley, 2018; Boere & Kerstens, 2018). Regarding the incident, the MIVD made an extraordinary amount of evidence available to the public. Whilst this is unusual, the Dutch service opted to do so in an effort to complicate the GRU agents' operations abroad (NOS, 2018b). Another reason was provided by Defence Minister Ank Bijleveld, who stated, "The Netherlands is in a cyber war with Russia" and an unusually large amount of information was revealed because "We should get rid of our naivety on that front" (AD, 2018).

Similarly to its cyber warfare operations in Estonia, Russian cyber-attacks in the Netherlands cannot be seen separately from its attempts at information warfare. In the cases identified, such as the sabotaging of the investigation into MH17 or the attempted hacking of the OPCW, Russia arguably opted for this strategy to reduce the amount or severity of damage to its international reputation as well as aid in promoting its alternative narratives on events the West accuses Russia to be responsible for. To counter these developments, the Netherlands already founded the National Cyber Security Centre in 2012 and the Joint Sigint Cyber Unit in 2013. It also published its first national cyber security document in 2011 and is continuously updating it, with the latest document, titled "Dutch Cybersecurity Strategy 2022-2028", having been published in 2022 (Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 2022). Despite these valiant efforts at cyber defence, the Netherlands is likely to remain a target of Russian hackers because of the key role the country plays due to the plethora of international organizations it plays host to, as well as the Netherlands being a key contributor of military support to Ukraine in the ongoing Russo-Ukrainian War. It is therefore likely that the Netherlands must remain a vigilant cyber security actor for the foreseeable future and learn its lessons from previous Russian incursions into its cyberspace.

4.13 Russian economic warfare in the Netherlands: energy dependency as a pressure mechanism

As highlighted in the introduction of this section, the Netherlands and Russia have been important trade partners prior to the Russian invasion of Ukraine in 2022 and Dutch imports from Russia mainly consisted of energy imports and more specifically gas. In 2007, the Netherlands, together with Denmark, were the only EU member states with a negative gas dependency, indicating a net export of gas (Kircher & Berk, 2010). Despite being the largest European producer of gas after Norway in 2013, the gas production of the Groningen gas field was slowly halted due to various earthquakes and subsequent damages as

a result of the gas production (Dickel et al., 2014; Reuters, 2023). This gas field had provided the Dutch government with important revenue as well as energy security for decades but the phasing out of its own gas production, together with ambitious climate goals put the country in a position where it became reliant on foreign imports, especially from Russia (Patrahau & Van Geuns, 2021).

European energy dependence thus provides Russia with a geopolitical pressure instrument that can be implemented in an economic warfare strategy. The Netherlands is not the only country faced with this problem, in 2019 and 2020 Russia supplied 44.7% and 39.3% of Europe's total natural gas imports (Eurostat, 2022). The manner in which European countries can be affected by Russia's economic warfare regarding gas became evident during the various tensions that occurred between Russia and Ukraine over the gas supply chain through the country, such as those in 2006, 2009 and 2014 (Sterkx & De Jong, 2010; Patrahau & Van Geuns, 2021). However, in part, Russia is also dependent on the revenues it gains from its gas exports to Europe, as many of its petroleum companies such as Rosneft and Gazprom are state-owned (Van Den Beukel & Van Geuns, 2021). The strong economic ties, and partial interdependence, between Europe and Russia might make it unlikely for the Kremlin to disrupt gas supplies however they do pose certain geopolitical dilemmas to countries like the Netherlands. The Netherlands is a state that promotes itself internationally as a champion of human rights and the rule of law, elements that are not present in Russia. Furthermore, as discussed within this dissertation, relations between the Netherlands severely deteriorated over issues such as Crimea and MH17. Despite the continuous Dutch condemnation and opposition towards Russia, the latter did find itself in a position where it could interfere with the Dutch energy supply whenever it desired.

Thus, Russian economic influence in the Netherlands created a political dilemma and made the Dutch vulnerable. Albeit perhaps not concerning the

heating of citizens' homes, but rather concerning the credibility of the state as an international actor. Since the annexation of Crimea, the Netherlands, together with the EU, imposed a series of sanctions, travel bans and asset freezes on Russia, but has been unable to fully sanction its main area revenue: gas exports (Patrahau & Van Geus, 2021). It is here that the energy dependency of the Netherlands can coincide with the Russian narratives on the country that were described in the section on information warfare in the Netherlands, feeding into the Russian notion of the West as an accumulation of "hypocritical" actors.

Other factors at play here are that prior to the Russian invasion of Ukraine in 2022, European energy policies were largely fragmented, with many states having to choose between retaining energy autonomy and strengthening the EU as a whole (Van Beukel & Van Geuns, 2021). This lack of solidarity amongst EU members is naturally another dilemma the Russians may seek to exploit.

4.14 Russian political influencing operations & covert action within the Netherlands

As mentioned within the case study on Estonia, the Kremlin also engages in traditional diplomacy to support pro-Russian narratives abroad. In this regard, some Dutch politicians have been eager to accept invitations to visit Russia, such as PVV leader Geert Wilders who visited Moscow in February 2018. Wilders held that "Russia is not an enemy" and his visit to the Russian capital was meant to symbolize his aversion against "hysterical Russophobia" in the Netherlands (RTL Nieuws, 2018). During his week in Russia, Wilders visited the State Duma and several Russian ministers for meetings but did not discuss the annexation of Crimea nor did he critically discuss the MH17 disaster (Godfroid, 2018; Trouw; 2018). This led to the relatives of MH17 victims demanding an apology from Wilders, which the latter refused to give (NOS, 2018a). Other politicians such as Forum voor Democratie leader Thierry Baudet have received invitations to visit the Kremlin, but did not visit. As discussed

above, there have been speculations about potential Russian financing of Baudet's party, but hard evidence has not been revealed. Similar to Estonia, Russian political influence operations in the Netherlands focus on gaining influence within Dutch democratic institutions and therefore intertwine with information warfare operations, in an effort to tilt narratives to the Kremlin's favour, or at least install doubt about institutions into the Dutch population.

The cases of cyber warfare and cyber espionage that have been discussed in the previous sections in part involved "traditional" forms of espionage and covert action, as the hackers that targeted the OPCW headquarters were operating on the ground in The Hague, attempting to hack into the OPCW's Wi-Fi networks by means of parking a car with hacking equipment in close vicinity of the OPCW building (Ministerie van Defensie, 2018).

4.15 Conclusion

Despite the long geographical distance between the two countries, the Netherlands and Russia have historically had a strong connection that has been founded on trade and economic cooperation. However, Dutch relations with Moscow became increasingly problematic following the annexation of Crimea and the downing of flight MH17 by Russian-backed separatists in which 196 Dutch nationals lost their lives. Ever since these events, Russian hybrid warfare operations in the Netherlands have intensified. In the case of the Netherlands, the Russian effort is versatile: the Kremlin clearly attempts to gain influence with various means, with a particular focus on information warfare and cyber warfare, whilst the economic ties between the two countries also put the Dutch in a difficult predicament.

In terms of information warfare, the various freedoms that exist within Dutch society, such as the freedom of expression, are exploited to spread misinformation, create doubt and undermine institutions. This effort

concentrates itself on events or organizations that may be harmful to Russian interests, such as the Dutch referendum on the Association Agreement with Ukraine or the criminal investigation into the MH17 disaster. Also, Russian state media such as Russia Today actively work to construct narratives that negatively portray the Netherlands, Dutch society and its democratic institutions in an attempt to rally pro-Kremlin voices and gain a foothold in public debates within the country.

On the other hand, cyber warfare has been used by Russia to influence, undermine and sabotage the criminal investigation into the MH17 disaster. Russians have attempted, and at times successfully penetrated, organizations such as the Dutch police force. Moreover, the threat of Russian hacker groups has forced the Dutch government to abandon all electronic voting. International organizations, to many of which the Netherlands plays host to, are also targeted by the Kremlin. Most notably, Russians attempted to hack into the internet networks of the OPCW, which at the time was investigating a number of events that involved the Russian state. These attempts at intrusion are likely to continue, especially since the ICC issued an arrest warrant for Russian President Putin over alleged war crimes (Borger & Sauer, 2023).

Economically, the Dutch, together with a plethora of other Western European states, have developed a relative energy dependency on Russia over the years. Not only did this make the Netherlands the subject of the vagaries of Russian (foreign) politics, but it also put a dent into its international credibility as a champion of human rights and international law. Even though the provisional results of the decoupling efforts that were made after the Russian invasion of Ukraine in 2022 seem successful, this reliance on a foreign power that is not congruent with one's own norms and values ought to teach the Dutch a valuable lesson for the future.

The Russian threat seems to have only truly penetrated Dutch society after the events of February 2022. Partially, this may be explained by the sheer distance

to Russia, or by the lack of a negative historical relation similar to the Estonian one. For the Netherlands, it will be of vital importance not to allow naivety to seep through into its society again and to work with its partners to remain vigilant of changing Russian approaches to gain influence as well as attempt to gain autonomy from undemocratic autocracies such as the Russian Federation.

5. Analysis: Differences & Similarities between Estonia & the Netherlands

The previous sections have thoroughly discussed the topic of hybrid warfare in general, its implications, and its difficulties. The case studies on Estonia and the Netherlands described at length how the Russian state makes use of various hybrid instruments to exert influence abroad. We have also seen why it is relevant to study these smaller states, as they are often able to wield significant power in terms of agenda-setting and pursuing their foreign policies. Furthermore, globally, and in organisations such as the EU and NATO, the number of states that we consider "small" is considerable, making the findings of research on small states relevant for many. The following section will aim to provide an analysis by looking at several differences and similarities between the two cases.

5.1 Similarities between Russian hybrid warfare in Estonia and the Netherlands

No matter where cases of Russian hybrid warfare are identified, the Russian objective is often similar: to exert influence over the (political) narratives within a country. Such is the case for both Estonia and the Netherlands, as Russia has attempted to drive wedges, promote pro-Kremlin narratives and undermine institutions in order to further its own policies and ideology, form alliances and improve its international posture.

Five key similarities between the two case studies can be identified:

1. **Focusing on information warfare and exploiting democratic freedoms**. For the Kremlin, information warfare is its most appealing instrument, due to a positive cost-reward balance as well as low risk. Implementing and operating disinformation campaigns is inexpensive and does not require an extensive number of personnel, thus an effective way of economizing its use of force. Such operations are effective in

Estonia and the Netherlands due to the transparency of these societies, which enables information to reach people through a plethora of ways, and increasingly through non-traditional forms of media such as the internet. In both states, Kremlin-owned information channels such as Russia Today and Sputnik News were found to be very active up until February 2022, creating a set of negative narratives about both countries in an attempt to create divisions amongst the population.

Both Estonia and the Netherlands are well-developed, strong democracies that benefit from various freedoms such as the freedom of expression, assembly or religion. The case studies have shown that Russia makes use of these freedoms, the freedom of expression in particular, to spread misinformation, create a sense of doubt and undermine democratic institutions. As such, these democratic freedoms make Western societies vulnerable.

Countering these exploitations is difficult because of the complicated nature of differentiating between sincere individuals exerting their opinions or Russian state-sponsored trolls. For Russia, this strategy poses little risk because it can always deny its involvement and argue the West is infringing on the rights of its citizens in case countermeasures such as censorship are implemented. In general, countering these information campaigns is often a struggle due to confusion as well as ambiguity about the source of information. On top of that, individual governments and international organisations continue to struggle to hold large social media companies to account in order to limit the spread of misinformation on online platforms.

2. **Being targeted as a part of international organizations instead of as an individual state**. The Kremlin understands that its information campaigns are more effective when they target the international organisations states are part of rather than the state individually. This is because states like Estonia and the Netherlands are heavily embedded in

these organisations. Therefore, Russia shifted its narratives after Estonia's accession to the EU and NATO. In the case of the Netherlands, narratives were already aimed primarily at the international organisations the Dutch were part of since the Netherlands was one of the founding members of both the EU and NATO. This particular similarity also holds relevance for other members of the EU and NATO, be it smaller or larger states, Russia is likely to make attempts at discrediting a state's membership of these organisations and instilling an idea into a state's population that a state's membership of such organisations is unbeneficial or even harmful.

3. **Attractive targets for cyber warfare**. Estonia and the Netherlands both are heavily digitalized societies, which makes them attractive targets for Russian cyber warfare operations. In both cases, Russia has had considerable success at cyber warfare, most notably in 2007 in Estonia and on several occasions from 2015 onwards in the Netherlands. However, both countries have acted upon this threat and implemented several counter strategies that vary in success. Especially Estonia has made significant progress with regard to its cyber defence up to the point where citizens barely notice the still prevalent Russian attempts at cyber interference.
4. **Different hybrid warfare elements are fundamentally interlinked**. In both cases, a strong link between various forms of Russian hybrid warfare can be identified. Most notably in the field of information and cyber warfare since these forms of hybrid warfare have generally been found to be the most prevalent. The connection between these elements is not strange: Russia believes it is engaged in an ongoing war with the West and views war as essentially holistic, as an activity that involves all elements of the state. In this, hybrid war is seen as a type of conflict rather than consisting of various elements that can be used as tools to

wage a war. Thus, it only makes sense information warfare and cyber warfare overlap and interlink significantly.

Russia arguably deploys its cyber warfare to influence or aid its information campaigns and vice versa. For example, in the case of the Netherlands, Russia attempted to hack and sabotage the MH17 investigation with the aim of mitigating the risk of being accused as the sole perpetrator, rallying supporters to its side and preserving its international reputation. In Estonia, the attempted hacking of government institutions is arguably done in an effort to solidify the Russian narrative that Estonia is fragile, poorly governed and part of failing Western institutions. The utilization of other elements such as economic warfare, covert operations and supporting foreign politicians are other examples that show how the entirety of the state is deployed in the effort to gain the upper hand in the hybrid conflict.

5. **Russia's hybrid warfare is tenacious**. The Kremlin views itself as fighting an ongoing war with the West, and in particular the U.S., NATO and the EU. In the 21st century, the traditional binary distinctions between peace and wartime no longer exist. Russia's efforts at hybrid warfare are therefore unlikely to cease in the near future. Naturally changes in intensity or focus occur, as is visible in Moscow's increased efforts at targeting international organisations in the Netherlands at times when these are investigating Russia's involvement in cases of breaches of international law. Following the Russian invasion of Ukraine in 2022, the Western response to Russia has been similarly persistent. However, the democratic nature of the West also entails that this persistence cannot be taken for granted and may change or attenuate, whereas a change in the Russian attitude towards the West would arguably require a much more unlikely and revolutionary change. It is therefore important to learn lessons from the past and present and make attempts to retain the levels of attentiveness towards autocratic regimes like Russia within

European societies, something that is possibly simpler for Estonia than the Netherlands because of its more burdened history with Russia.

5.2 Differences between Russian hybrid warfare in Estonia and the Netherlands

There are many factors that contribute to the differences that exist in Russian hybrid warfare approaches to Estonia and the Netherlands, such as the two countries' different historical relations with Russia or their distinct demographical and economic features. These differences are important to highlight, because they may prove to be useful guides in shoring up weaknesses.

Five key differences between the two case studies can be identified:

1. **Economic dependency**. Whereas Estonia has been rather successful at averting economic dependence on Moscow, this is not the case for the Netherlands, which has made the latter vulnerable to Russian economic warfare. Most notably, the Dutch, as well as a number of other Western European countries, manoeuvred themselves into a position where they became reliant on gas imports from Russia. This has enabled Russia to exert significant geopolitical pressure on the Netherlands. Whereas Russia also has much to gain from this trade economically, the trouble for the Netherlands mainly originates from the fact that intensive trade with Russia does not rhyme with the Dutch efforts at promoting human rights, democracy and the rule of law. These are evidently not present in Russia and thus hurt the credibility of the Netherlands as an international champion of the abovementioned. This situation fits the malicious Russian narrative that the Netherlands is a hypocritical actor and should therefore be avoided.
2. **International organisations**. In contrast to Russian cyber warfare in Estonia, where the Kremlin mainly targets government institutions or media organizations, in the Netherlands international organisations are

the preferred targets of the Kremlin, even though Dutch government institutions such as the police force have faced attempted interferences as well. This is mainly because of the simple fact that the Netherlands plays host to an extensive number of international organisations and Estonia does not. Since the Netherlands is responsible for both the physical as well as non-physical defence of international organisations on its territory, the Dutch could learn from Estonia, which, in an effort to protect its highly digitalized society, opened a data centre in Luxembourg to safeguard a backup of its citizens' data (Talmazan, 2019).

3. **Overt support of Russia**. Because of Estonia's troublesome historical relationship with Russia, overt support of the Kremlin is not appreciated and is rather met with scorn. This does not mean however that pro-Kremlin views are not disseminated within the country; as the case study shows politicians, bloggers, social media activists, news sources or website moderators are found to be eager to spread Moscow's talking points, be it consciously or not. The Netherlands on the other hand has a completely different history with Russia which becomes evident in the fact that it is much more common for politicians or journalists to openly show their support of the Kremlin and its policies. These are not minor groups either, with parties that have shown sympathies towards Moscow in the past or present currently holding 20-25% of the seats in Parliament. Political leaders have visited Moscow and praised Russia as well as President Putin for his efforts in standing for conservative and "anti-globalist" ideals (Pauwels, 2022).
4. **Political naivety**. Between the two cases, there is arguably a difference in urgency visible. On the one hand, throughout the period studied, Estonia seems well aware of the Russian threat whereas the Netherlands does not, not after the annexation of Crimea, the downing of flight MH17 or the various Russian hacking attempts. Arguably, the Dutch

only truly changed their attitudes towards Russia following the inception of the latter's all-out violence against Ukraine in February 2022. This naivety is also visible in the abovementioned economic dependency but also on a plethora of other terrains, such as the systematic cutbacks on defence spending within the Netherlands. Whereas the Netherlands spend 4.12% of its GDP on defence in 1962, in 2015 this number had dropped to a mere 1.13% (World Bank, 2023b). In comparison, Estonia has steadily invested a greater amount of funding into its defence since its independence with 0.76% of GDP being used for defence in 1993 and 2.36% in 2020 (World Bank, 2023a). Naturally, these differences are grounded by differing historical relationships with Russia, but the 2022 Russian invasion of Ukraine clearly shows that a positive relationship, nor geographical distance, will obstruct an authoritarian power from harassing a country such as the Netherlands, if such as country becomes the victim of its own poor judgement by making itself dependent on the authoritarian power, be it by means of energy dependency or other factors. For countries like the Netherlands, it will therefore be vital to improve strategic awareness going forward and attempt to avoid naivety.

5. **Population centric vs**. **narratives**. In the Netherlands, Russian hybrid warfare is mainly implemented in order to spread pro-Kremlin narratives in order to improve Russia's posture, as well as disrupt international organisations and international cooperation in general. In Estonia, we observe similar targeting, but also specific targeting of the 25% of the Estonian population that is Russian speaking and has Russian heritage, a demographic element simply not present in the Netherlands. Russia understands that influence over the local population is of the essence in military conflict and has thus attempted to gain influence over Russian Estonians by means of its state propaganda channels, which were widely available in Estonia prior to February 2022. On top of that, various social media networks play an important role in targeting the population with

information warfare and have certainly contributed to the outbreak of protests over issues such as the removal of various Soviet war memorials. However, convincing the population to support Russian narratives unequivocally remains a challenge for the Kremlin. Even though there certainly are large groups of people in Estonia that share significant sympathies with Russia, the superior economic situation in Estonia makes it difficult to truly rally the Russian speakers in Estonia to Moscow's side. This is evidenced by the repeated efforts of citizens of the Russian border city Ivangorord to join Estonia, because of the much better economic conditions across the border.

6. Conclusion

This dissertation has discussed arguably one of the most frequently discussed topics in strategic and war studies over the last decade: hybrid warfare. The term, despite having been around since the 1990s, gained more prominence during the 2000s but its popularity truly skyrocketed after the Russian annexation of Crimea in 2014, which shocked many in the West and lead some to believe hybrid wars would replace warfare in general for the decades to come. Following the Russian invasion of Ukraine in 2022 we know that presumption to be false, although the hybrid element in war has arguably cemented itself in the modern art of war and any conventional war is highly likely to have several hybrid elements in the build-up or during a conflict.

Although the concept of hybrid warfare, and its usage by Russia, has been discussed frequently, little research has been done to compare and contrast Russian hybrid strategies in various European states. Some research has been done to compare Russian strategies in various states that were formerly part of the Soviet Union, but little to no research had been conducted to compare Eastern European states with Western European states and especially not with a particular focus on smaller states. This dissertation has conducted such research by producing a comparative case study analysis on Russian hybrid warfare in Estonia and the Netherlands.

Even though Estonia and the Netherlands differ substantially in history, geographical location and demographics, there arguably are more similarities than differences when it comes to Russian hybrid warfare. In the 21st century, where information is disseminated into societies quickly, information warfare is a tool that is frequently used by the Kremlin in an effort to instil a sense of confusion and doubt into societies, undermine democratic institutions and frustrate international cooperation in organisations such as the EU and NATO. Estonia and the Netherlands, being democratic states, are vulnerable to information warfare because they are characterized by freedoms such as the freedom of expression and media, which enable anyone to voice their opinion,

even if it is with the goal of spreading false narratives with malicious intent. This works to the advantage of an interfering actor such as Russia because it is often difficult to distinguish a sincere concerned citizen from a Russian troll and the Kremlin thus has plausible grounds to deny its involvement, which is a strategy that is recognizable along the entire spectrum. Both states are also attractive targets for cyber warfare due to their highly digitalized societies and are at the end of campaigns that target their membership of organisations such as the EU and NATO. We see that Russian efforts at hybrid warfare are interlinked and support one another; cyber-attacks are used to sabotage investigations that may discredit Russia and information campaigns work to improve Russia's image abroad, or at least rally enough people to its cause to undermine the effectiveness of foreign government and international cooperation.

Differences mainly originate from the different historical perspectives towards Russia that exist within the countries studied. Due to its history of Russian oppression, Estonia is significantly more aware of the Russian threat, be it to its people, economy or politics. The Netherlands, despite facing many of the same threats from Moscow as mentioned above, has shown this awareness to a lesser extent, which has led to the awkward situation of being dependent on Russia for energy whilst attempting to maintain a critical position of Russian politics. In this regard, the West can learn from the East in the sense that Eastern European countries have greater experience in dealing with Russian threats and are well aware of what is required to counter the Kremlin's influence.

In the greater scheme of things, the lessons drawn from this dissertation should not only apply to Estonia and the Netherlands but rather to any small state that engages in significant relations with Russia, especially in Europe. For one because it teaches us what to expect from an authoritarian great power but on the other hand because in the Europe of the 21st century states rarely are targeted on their own, but rather in the greater political constructs they are part of. For example, when Estonia integrated itself into the EU and NATO Russian

narratives changed to target these organisations rather than Estonia itself. This also means that Russian hybrid attacks on Estonia or the Netherlands should be a concern for all members of these organisations, as these attacks seek to undermine their coherence.

This dissertation has established the extent and workings of Russian hybrid warfare in Estonia and the Netherlands and has conveyed the reasons why it matters as a field of study. This opens up avenues for future research for which there was only little space within this dissertation. In particular, countermeasures towards Russian hybrid warfare, and the possible cooperation between states such as Estonia and the Netherlands on this front, could be insightful and worthwhile to be further researched in the future.

As this dissertation has discussed, Russian hybrid warfare is highly likely to be persistent, as Russia views itself at war with the West which involves all elements of its state, from propaganda to cyber to diplomacy. The Kremlin has adopted this strategy because it is economically viable and produces valuable results at relatively low risk. It is expected that the populations of European democracies will continue to be targeted by Russia in an effort to disenfranchise them from their democratic institutions. This is a tenacious struggle in which an end is not in sight. Whereas Russia would need a change of revolutionary proportion to alter its attitude the West is far more vulnerable due to the volatility of democracy. It is up to politicians, policymakers and academics to continue to provide a thorough analysis of Moscow's attempts at interfering with our societies in order to effectively bolster our defences and repel the Russian hybrid threat.

7. References

AD. (2018, October 14). Bijleveld: Nederland in cyberoorlog met Russen. https://www.ad.nl/buitenland/bijleveld-nederland-in-cyberoorlog-met-russen~ac0b5320/

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (2023). 24/2 - De Russische aanval op Oekraïne: een keerpunt in de geschiedenis. https://www.aivd.nl/documenten/publicaties/2023/02/20/24-2---de-russische-aanval-op-oekraine-een-keerpunt-in-de-geschiedenis

Anton, M. (2016). Hybrid Pedagogies for Hybrid War. Scientific Research and Education in the Air Force, 18(2), 509–516. https://doi.org/10.19062/2247-3173.2016.18.2.3

Applebaum, A. (2016, April 9). Opinion | The Dutch just showed the world how Russia influences Western European elections. Washington Post. https://www.washingtonpost.com/opinions/russias-influence-in-western-elections/2016/04/08/b427602a-fcf1-11e5-886f-a037dba38301_story.html

Ashmore, W. H. (2009). Impact of Alleged Russian Cyber Attacks. U.S. Army Command And General Staff College. School of Advanced Military Studies. http://indianstrategicknowledgeonline.com/web/Impact%20of%20Alleged%20Russian%20Cyber%20Attacks.pdf

Balan, S. (2016). Hybrid War- Old, but New (What is New and What is Not). International Scientific Conference "Strategies XXI," 1, 319–323. https://www.proquest.com/docview/1785756865?pq-origsite=gscholar&fromopenview=true

Banco, E. (2023, February 18). Inside the stunning growth of Russia's Wagner Group. POLITICO. https://www.politico.com/news/2023/02/18/russia-wagner-group-ukraine-paramilitary-00083553

Bebler, A. (2015). Crimea and the Russian-Ukrainian Conflict. Romanian Journal of European Affairs, 15(1), 35–54. http://rjea.ier.ro/sites/rjea.ier.ro/files/articole/RJEA_2014_vol15_no1_art.3.pdf

Bērziņš, J. (2015, September 11). A New Generation of Warfare. Per Concordiam. https://perconcordiam.com/a-new-generation-of-warfare/

Bil, J. (2022). The Effectiveness of the Russian Impact in Estonia Measured With Quantitative Methods. Security Dimensions, 42(42), 22–35. https://doi.org/10.5604/01.3001.0016.0733

Biteniece, N., Fredheim, R., & Rodriguez, B. C. (2019). Robotrolling 2019/2. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/robotrolling-20192/114

Blank, S. (2008a). Russia and the Black Sea's Frozen Conflicts in Strategic Perspective. Mediterranean Quarterly, 19(3), 23–54.

Blank, S. (2008b). Web War I: Is Europe's First Information War a New Kind of War? Comparative Strategy, 27(3), 227–247. https://doi.org/10.1080/01495930802185312

Blank, S. (2016). Cyber War and Information War à la Russe. In G. Perkovich & A. E. Levite (Eds.), Understanding Cyber Conflict: Fourteen Analogies (pp. 81–98). Georgetown University Press.

Boere, R., & Kerstens, B. (2018, October 4). Nederland verijdelt hackaanval Russen op OPCW. AD. https://www.ad.nl/buitenland/nederland-verijdelt-hackaanval-russen-op-opcw~a4c7f2c8/

Borger, J., & Sauer, P. (2023, March 18). ICC judges issue arrest warrant for Vladimir Putin over alleged war crimes. The Guardian. https://www.theguardian.com/world/2023/mar/17/vladimir-putin-arrest-warrant-ukraine-war-crimes

Brandt Corstius, J. (2007, November 7). Gasunie en Gazprom sluiten een miljardenakkoord. Trouw. https://www.trouw.nl/nieuws/gasunie-en-gazprom-sluiten-een-miljardenakkoord~b0cff273/

Brown, A. (2015, January 22). Russian media claims Vladimir Putin assassination attempt to blame for MH17 crash. Express.co.uk. https://www.express.co.uk/news/world/490530/Russian-Media-Coverage-Vladimir-Putin-assassination-attempt-Malaysia-Airlines-MH17
Brown, É. (2018). Propaganda, Misinformation, and the Epistemic Value of Democracy. Critical Review, 30(3–4), 194–218. https://doi.org/10.1080/08913811.2018.1575007
Budnitsky, S. (2022). A Relational Approach to Digital Sovereignty: e-Estonia Between Russia and the West. International Journal of Communication, 16, 1918–1939.
Çalişkan, M. (2016). A Critique of Hybrid Warfare. International Conference on Military and Security Studies. http://hdl.handle.net/2078.1/207050
Çalişkan, M. (2019). Hybrid warfare through the lens of strategic theory. Defense & Security Analysis, 35(1), 40–58. https://doi.org/10.1080/14751798.2019.1565364
Cavegn, D. (2016, November 8). Overview: Center Party's cooperation protocol with Putin's United Russia. ERR. https://news.err.ee/119629/overview-center-party-s-cooperation-protocol-with-putin-s-united-russia
Centraal Bureau voor de Statistiek (CBS). (2022). How much did the Netherlands import from and export to Russia? Statistics Netherlands. https://www.cbs.nl/en-gb/faq/rusland-oekraine/how-much-did-the-netherlands-import-from-and-export-to-russia-
Centraal Bureau voor de Statistiek (CBS). (2023, April 26). CBS Statline. Statline. https://opendata.cbs.nl/statline/#/CBS/en/dataset/83474ENG/table?ts=1616407710127
Cerulus, L. (2018, January 28). Dutch go old school against Russian hacking. POLITICO. https://www.politico.eu/article/dutch-election-news-russian-hackers-netherlands/
Chaban, N., Elgström, O., & Gulyaeva, O. (2017). Russian Images of the European Union: Before and after Maidan. Foreign Policy Analysis, orw055. https://doi.org/10.1093/fpa/orw055
Chivvis, C. S. (2017). Understanding Russian "Hybrid Warfare" And What Can Be Done About It. In RAND Corporation. RAND Corporation. https://www.rand.org/pubs/testimonies/CT468.html
Clark, M. (2020). Russian Hybrid Warfare. In Institute for the Study of War. Institute for the Study of War. https://www.understandingwar.org/report/russian-hybrid-warfare
Clemens, W. C. (1999). The Baltic Republics, Russia, and Energy: From Dependency to Interdependence? SAIS Review, 19(1), 190–208. https://muse.jhu.edu/journals/sais_review/v019/19.1clemens.html
Complex crises call for adaptable and durable capabilities. (2015). The Military Balance, 115(1), 5–8. https://doi.org/10.1080/04597222.2015.996334
Crerar, P., Henley, J., & Wintour, P. (2018, October 5). Russia accused of cyber-attack on chemical weapons watchdog. The Guardian. https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body
Cyber Security Strategy Committee. (2008). Cyber Security Strategy. Ministry of Defence Estonia.
Czosseck, C., Ottis, R., & Talihärm, A. (2011). Estonia after the 2007 Cyber Attacks. International Journal of Cyber Warfare and Terrorism, 1(1), 24–34. https://doi.org/10.4018/ijcwt.2011010103
David, M., Gower, J., & Haukkala, H. (2013). National Perspectives on Russia (1st ed.). Routledge. https://kclpure.kcl.ac.uk/portal/en/publications/national-perspectives-on-russia(76410934-ca4d-4c67-ab45-6476792fade0)/export.html
Davies, P. (2022, August 19). Estonia hit by "most extensive" cyberattack since 2007 amid tensions with Russia over Ukraine war. Euronews. https://www.euronews.com/next/2022/08/18/estonia-hit-by-most-extensive-cyberattack-since-2007-amid-tensions-with-russia-over-ukrain

De Boer, M. (2017, February 18). Van Bommel: Geen samenwerking met Russen. https://www.trouw.nl/nieuws/van-bommel-geen-samenwerking-met-russen~b0c8e18d/
De Jong, S. (2016, April 4). Why the Dutch referendum on Ukraine is a joke. EUobserver. https://euobserver.com/opinion/132908
De Vaus, D., & De Vaus, P. D. (2001). Research Design in Social Research. SAGE.
De Vreij, H. (2016, September 27). De kronkels in de Russische versies over de MH17 - Raam op Rusland. https://www.raamoprusland.nl/dossiers/nederland-en-europa/283-de-kronkels-in-de-russische-versies-over-de-mh17
Deep, A. (2015). Hybrid War: Old Concept, New Techniques. Small Wars Journal. https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques#_ednref5
Dickel, R., Hassanzadeh, E., Henderson, J., Honoré, A., El-Katiri, L., Pirani, S., Rogers, H., Stern, J., & Yafimava, K. (2014). Reducing European Dependence on Russian Gas: Distinguishing Natural Gas Security from Geopolitics. Oxford Institute for Energy Studies.
Dutch Safety Board. (2015). MH17 Crash. https://safetyboard.nl
Economist Intelligence Unit. (2022). Democracy Index 2022. Economist Intelligence.
e-Estonia. (2023, February 1). Story - e-Estonia. https://e-estonia.com/story/
Ehin, P., & Berg, E. (2016). Incompatible Identities? Baltic-Russian Relations and the EU as an Arena for Identity Conflict. Routledge eBooks, 1–14. https://doi.org/10.4324/9781315587745-1
ERR News. (2023, January 18). Statistics: Estonia's population grew by 2 percent on year to January 2023. ERR. https://news.err.ee/1608854255/statistics-estonia-s-population-grew-by-2-percent-on-year-to-january-2023
Eurostat. (2022, March 28). The EU imported 58% of its energy in 2020. Eurostat. https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20220328-2#:~:text=In%202020%2C%20the%20EU%20imported,and%2011%25%20solid%20fossil%20fuels.
Frankenfield, J. (2023). Denial-of-Service (DoS) Attack: Examples and Common Targets. Investopedia. https://www.investopedia.com/terms/d/denial-service-attack-dos.asp#:~:text=A%20DoS%20(denial%2Dof%2D,single%20computer%20launches%20the%20attack.
Freeman, D., Meijerink, G., & Teulings, R. (2022). Trade benefits of the EU and the Internal Market. CPB Netherlands Bureau for Economic Policy Analysis.
Galeotti, M. (2015). 'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't. In A. Pikulicka-Wilczewska & R. Sakwa (Eds.), Ukraine and Russia: People, Politics, Propaganda and Perspectives. E-international Relations.
Ganor, B. (2012). The Hybrid Terrorist Organization and Incitement. In A. Baker (Ed.), The Changing Forms Of Incitement To Terror And Violence: The Need for a New International Response (pp. 13–19). Jerusalem Center for Public Affairs and the Konrad-Adenauer-Stiftung.
Gardasevic, I. (2018). Russia and Montenegro: How and Why a Centuries' Old Relationship Ruptured. Connections: The Quarterly Journal. https://doi.org/10.11610/connections.17.1.04
Geers, K. (2015). Cyber War in Perspective: Russian Aggression Against Ukraine. NATO Cooperative Cyber Defence Centre of Excellence.
Gerasimov, V. (2016). The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Military Review, 96(1), 23. https://www.questia.com/library/journal/1G1-440822326/the-value-of-science-is-in-the-foresight-new-challenges
Godfroid, D. J. (2018, March 3). "Wilders sprak in Rusland wel over MH17, maar ging niet in discussie." NOS. https://nos.nl/artikel/2220334-wilders-sprak-in-rusland-wel-over-mh17-maar-ging-niet-in-discussie

Goldthau, A. (2016). Assessing Nord Stream 2: regulation, geopolitics & energy security in the EU, Central Eastern Europe & the UK. European Centre for Energy and Resource Security (EUCERS).
Göransson, M. B. (2022). Russian scholarly discussions of nonmilitary warfare as securitizing acts. Comparative Strategy, 41(6), 526–542. https://doi.org/10.1080/01495933.2022.2130675
Grant, G. (2012, January 17). Hybrid Wars. Government Executive. https://www.govexec.com/magazine/features/2008/05/hybrid-wars/26799/
Gray, C. S. (2012). Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional. Strategic Studies Institute. https://doi.org/10.21236/ada559162
Grenkevich, L. D. (2013). The Soviet Partisan Movement, 1941-1944: A Critical Historiographical Analysis. Routledge.
Grynszpan, E. (2017, March 2). Russian official: Information war part of 'battle for the consciousness of the masses.' StopFake. https://www.stopfake.org/en/russian-official-information-war-part-of-battle-for-the-consciousness-of-the-masses/
Guerra, J. M. (2012). An Introduction to Clausewitzian Strategic Theory: General Theory, Strategy, and their Relevance for Today. Infinity Journal, 2(3), 30–34.
Harris, K. (2020). Russia's Fifth Column: The Influence of the Night Wolves Motorcycle Club. Studies in Conflict and Terrorism, 43(4), 259–273.
Heck, W. (2016, June 30). 'Oekraïne kan ons niets schelen.' NRC. https://www.nrc.nl/nieuws/2016/03/31/oekraine-kan-ons-niets-schelen-1606419-a969298
Helmus, T. C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., Bega, A., & Winkelman, Z. (2018). Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. RAND Corporation.
Henley, J. (2018, October 4). Visual guide: how Dutch intelligence thwarted a Russian hacking operation. The Guardian. https://www.theguardian.com/world/2018/oct/04/visual-guide-how-dutch-intelligence-thwarted-a-russian-hacking-operation
Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 4(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3
Higgins, A. (2017, March 6). Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote. The New York Times. https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html
Higgins, A., & Nechepurenko, I. (2018, August 7). In Africa, Mystery Murders Put Spotlight on Kremlin's Reach. The New York Times. https://www.nytimes.com/2018/08/07/world/europe/central-african-republic-russia-murder-journalists-africa-mystery-murders-put-spotlight-on-kremlins-reach.html?pagewanted=all&src=pm
Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
Hope, K. (2014, November 30). Bulgarians see Russian hand in anti-shale protests. Financial Times. https://www.ft.com/content/e011d3f6-6507-11e4-ab2d-00144feabdc0
Howard, C., & Pukhov, R. (2014). Brothers Armed: Military Aspects of the Crisis in Ukraine. East View Press.
Hoyle, A., Van Den Berg, H., Doosje, B., & Kitzen, M. (2021). Portrait of liberal chaos: RT's antagonistic strategic narration about the Netherlands. Media, War & Conflict, 175063522110647. https://doi.org/10.1177/17506352211064705

Iasiello, E. (2013). Cyber Attack: A Dull Tool to Shape Foreign Policy. International Conference on Cyber Conflict, 1–18. http://ccdcoe.org/publications/2013proceedings/d3r1s3_Iasiello.pdf
Ingebritsen, C. (2002). Norm Entrepreneurs. Cooperation and Conflict, 37(1), 11–23. https://doi.org/10.1177/0010836702037001689
Jakobson, M., & Kasekamp, A. (2023). The impact of the Russia-Ukraine War on right-wing populism in Estonia. European Center for Populism Studies (ECPS).
Janmaat, J. G., & Kuzio, T. (2016, July 21). The no camp in Netherlands resorts to stereotypes, half-truths and demeaning propaganda - Apr. 06, 2016 | KyivPost. Kyiv Post. https://archive.kyivpost.com/article/opinion/op-ed/jan-germen-janmaat-and-taras-kuzio-the-no-camp-in-netherlands-resorts-to-stereotypes-half-truths-and-demeaning-propaganda-411422.html
Johnson, R. E. (2018). Hybrid War and Its Countermeasures: A Critique of the Literature. Small Wars & Insurgencies, 29(1), 141–163. https://doi.org/10.1080/09592318.2018.1404770
Joint Investigation Team (JIT). (2016, September 28). JIT presentation of first results of the MH17 criminal investigation (28-09-2016). Public Prosecution Service. https://www.prosecutionservice.nl/topics/mh17-plane-crash/criminal-investigation-jit-mh17/jit-presentation-first-results-mh17-criminal-investigation-28-9-2016
Journeyman Pictures. (2017, July 20). Estonian Wargames: How NATO is Preparing Estonia for Potential War with Russia [Video]. YouTube. https://www.youtube.com/watch?v=v32zCR5Zujk
Kaiser, R. (2012). Reassembling the event: Estonia's 'Bronze Night.' Environment and Planning D: Society and Space, 30(6), 1046–1063. https://doi.org/10.1068/d18210
Katzenstein, P. J. (1985). Small States in World Markets: Industrial Policy in Europe. Cornell University Press.
Keohane, R. O. (1969). Lilliputians' Dilemmas: Small States in Internatinal Politics. International Organization, 23(2), 291–310. https://doi.org/10.1017/s002081830003160x
Kirchner, E. J., & Berk, C. (2010). European Energy Security Co-operation: Between Amity and Enmity. Journal of Common Market Studies, 48(4), 859–880. https://doi.org/10.1111/j.1468-5965.2010.02077.x
Klein, P. (2019, July 13). Vijf jaar na MH17: "Waarom zegt niemand sorry?" RTL Nieuws. https://www.rtlnieuws.nl/nieuws/nederland/artikel/4774356/mh17-kroniek-vijf-jaar-later-5-sorry-vliegtuigramp-drama-rusland
Korteweg, R., Ortega, A., & Otero, M. (2022). A Spanish-Dutch view on open European strategic autonomy in trade, industry and digital policy: seven pitfalls to avoid. Real Instituto Elcano & Clingendael Institute. https://www.realinstitutoelcano.org/en/analyses/a-spanish-dutch-view-on-open-european-strategic-autonomy-in-trade-industry-and-digital-policy-seven-pitfalls-to-avoid/
Kouwenhoven, A., & Heck, W. (2020, September 29). Hoe Russische desinformatie hier in een gratis krant belandt. NRC. https://www.nrc.nl/nieuws/2020/09/28/hoe-rusland-desinformatie-hier-verspreidt-a4013918
Kreegipuu, T., & Lauk, E. (2007). The 1940 Soviet Coup-d'État in the Estonian Communist Press: Constructing History to Reshape Collective Memory. Westminster Papers in Communication and Culture. https://doi.org/10.16997/wpcc.111
Kuzio, T. (2018). Euromaidan revolution, Crimea and Russia–Ukraine war: why it is time for a review of Ukrainian–Russian studies. Eurasian Geography and Economics, 59(3–4), 529–553. https://doi.org/10.1080/15387216.2019.1571428
Lagnado, A. (1998, July 31). The Moscow Times. The Moscow Times. https://www.themoscowtimes.com/1998/07/31/town-petitions-to-join-estonia-a287105

Lamond, J., & Bergmann, M. (2020, May 7). The Weakest Link: Russian Influence Operation in the Netherlands Reveals Vulnerabilities in EU Foreign Policy Powers. Center for American Progress. https://www.americanprogress.org/article/weakest-link-russian-influence-operation-netherlands-reveals-vulnerabilities-eu-foreign-policy-powers/

Landler, M., & Gordon, M. R. (2014, July 9). NATO Chief Warns of Duplicity by Putin on Ukraine. The New York Times. https://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html

Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. International Affairs, 92(1), 175–195. https://doi.org/10.1111/1468-2346.12509

Lazaroms, I. J. (2014). The Netherlands - From the Fringes of Europe and Back Again: Responses to the Crisis in Ukraine. Herder Institut. https://digital.herder-institut.de/publications/frontdoor/deliver/index/docId/58/file/Lazaroms_The_Netherlands_From_the_Fring.pdf

Limnell, J. (2018). Russian cyber activities in the EU. In Hacks, Leaks and Disruptions: Russian Cyber Strategies (pp. 65–73). European Union Institute for Security Studies (EUISS). http://www.jstor.com/stable/resrep21140.10

Mac Dougall, D. (2023, March 7). Estonia election analysis: Why the liberals won, the far-right lost, and other key takeaways. Euronews. https://www.euronews.com/2023/03/06/estonia-election-analysis-why-the-liberals-won-the-far-right-lost-and-other-key-takeaways

Makarychev, A. (2021). Russian "cognitive propaganda": the case of Impressum Club in Tallinn. Post-soviet Affairs, 37(1), 45–64. https://doi.org/10.1080/1060586x.2020.1804259

Martyn-Hemphill, R. (2021, January 13). Estonia's New Premier Comes From Party With Links to Russia. The New York Times. https://www.nytimes.com/2016/11/21/world/europe/estonia-juri-ratas-center-party.html

Mattis, J. N., & Hoffman, F. G. (2005). Future Warfare: The Rise of Hybrid Wars. Proceedings Magazine, 132, 30–32. http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf

McCombie, S., Uhlmann, A. J., & Morrison, S. M. (2020). The US 2016 presidential election & Russia's troll farms. Intelligence and National Security, 35(1), 95–114. https://doi.org/10.1080/02684527.2019.1673940

McCulloh, T., & Johnson, R. (2013). Hybrid Warfare. In JSOU Report. Joint Special Operations University. https://apps.dtic.mil/sti/citations/ADA591803

Meeus, T. (2017, January 13). Russische poging tot hack van OVV. NRC. https://www.nrc.nl/nieuws/2017/01/13/russische-poging-tot-hack-van-ovv-6202180-a1541257

Meister, S. (Ed.). (2018). Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia. ifa Edition Culture and Foreign Policy.

Mills, A. J., Durepos, G., & Wiebe, E. (2009). Encyclopedia of Case Study Research. SAGE Publications.

Ministerie van Defensie. (2018, October 4). Statements betreffende de verstoring van een cyberoperatie van de GRU door de MIVD op 4 oktober in Den Haag [Press release]. https://english.defensie.nl/topics/cyber-security/russian-cyber-operation

Modderkolk, H. (2017, February 4). Russen faalden bij hackpogingen ambtenaren op Nederlandse ministeries. De Volkskrant. https://www.volkskrant.nl/cultuur-media/russen-faalden-bij-hackpogingen-ambtenaren-op-nederlandse-ministeries~b77ff391/

Modderkolk, H. (2018, January 25). Dutch agencies provide crucial intel about Russia's interference in US-elections. De Volkskrant. https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/

Modderkolk, H. (2021, June 8). Russen zaten ten tijde van MH17-onderzoek door hack diep in systemen politie. De Volkskrant. https://www.volkskrant.nl/nieuws-achtergrond/russen-zaten-ten-tijde-van-mh17-onderzoek-door-hack-diep-in-systemen-politie~b0e044e1/
Moreland, S., & Jasper, S. (2014). The Islamic State is a Hybrid Threat: Why Does That Matter? Small Wars Journal.
Murray, W., & Mansoor, P. R. (2012). Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge University Press.
Nakashima, E. (2016, June 14). Russian government hackers penetrated DNC, stole opposition research on Trump. Washington Post. https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html#:~:text=Russian%20government%20hackers%20penetrated%20the,who%20responded%20to%20the%20breach.
Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2022). Nederlandse Cybersecuritystrategie 2022-2028. https://www.nctv.nl/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-2022-2028
NOS. (2014, July 22). Vandaag dag van nationale rouw. NOS. https://nos.nl/artikel/678095-vandaag-dag-van-nationale-rouw
NOS. (2018a, February 28). Nabestaanden MH17 eisen excuses van Wilders om bezoek aan Moskou. NOS. https://nos.nl/artikel/2219844-nabestaanden-mh17-eisen-excuses-van-wilders-om-bezoek-aan-moskou
NOS. (2018b, October 4). MIVD: we hebben Russische hack van OPCW in Den Haag voorkomen. NOS. https://nos.nl/artikel/2253313-mivd-we-hebben-russische-hack-van-opcw-in-den-haag-voorkomen
OEC. (2022). Russia (RUS) and Netherlands (NLD) Trade | OEC. OEC - the Observatory of Economic Complexity. https://oec.world/en/profile/bilateral-country/rus/partner/nld?dynamicBilateralTradeSelector=year2021
Otjes, S. (2016, January 26). Could the Netherlands' referendum on Ukraine really create a 'continental crisis'? EUROPP Blog. http://bit.ly/1Sh7w4T
Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. In Cooperative Cyber Defence Centre of Excellence. Cooperative Cyber Defence Centre of Excellence.
Oyetunde, B. (2023, April 3). Estonia saw a record number of cyber attacks in 2022 - e-Estonia. e-Estonia. https://e-estonia.com/in-2022-estonia-had-the-highest-number-of-cyber-attacks/
Panke, D., & Gurol, J. (2018). Small States as Agenda-setters? The Council Presidencies of Malta and Estonia. Journal of Common Market Studies, 56, 142–151. https://doi.org/10.1111/jcms.12767
Paraskevopoulos, D. (2021, December 21). Estonia - a European and global leader in the digitalisation of public services - e-Estonia. e-Estonia. https://e-estonia.com/estonia-a-european-and-global-leader-in-the-digitalisation-of-public-services/
Patrahau, I., & Van Geuns, L. (2021). Gas Supply Security in the Netherlands: Geopolitical and Environmental Dilemmas. The Hague Center for Security Studies. https://hcss.nl/wp-content/uploads/2021/03/Gas-Supply-Security-final-web.pdf
Pauwels, P. (2022). Interview Baudet veroorzaakt rel: 'Fantastisch dat Poetin bestaat' Metronieuws.nl. https://www.metronieuws.nl/in-het-nieuws/binnenland/2022/10/interview-baudet-fantastisch-poetin-bestaat/
Petsinis, V. (2019). Identity Politics and Right-Wing Populism in Estonia: The Case of EKRE. Nationalism and Ethnic Politics, 25(2), 211–230. https://doi.org/10.1080/13537113.2019.1602374

Postimees. (2017, April 17). Военно-исторический клуб из Эстонии отмечен митрополитом Санкт-Петербургским и Ладожским Владимиром. Postimees. https://rus.postimees.ee/429534/voenno-istoricheskiy-klub-iz-estonii-otmechen-mitropolitom-sankt-peterburgskim-i-ladozhskim-vladimirom
Rademaker, M., Sweijs, T., & Voorhoeve, J. (2019). HOE BESCHERMEN WIJ ONS TEGEN RUSSISCHE DESINFORMATIE? Hague Centre for Strategic Studies. https://www.jstor.org/stable/pdf/resrep12632
Radin, A. (2017). Hybrid Warfare in the Baltics. Threats and Potential Responses. In RAND Corporation. RAND Corporation. https://www.rand.org/pubs/research_reports/RR1577.html
Radio Free Europe. (2010, April 13). Russian Border Town Seeks To Join Estonia. RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/Russian_Border_Town_Seeks_To_Join_Estonia/2011276.html
Rashid, A., Khan, A. I., & Azim, S. W. (2021). Cyber hegemony and information warfare: A case of Russia. Liberal Arts & Social Sciences International Journal, 5(1), 648–666. https://doi.org/10.47264/idea.lassij/5.1.42
Rauta, V. (2020). Towards a typology of non-state actors in 'hybrid warfare': proxy, auxiliary, surrogate and affiliated forces. Cambridge Review of International Affairs, 33(6), 868–887. https://doi.org/10.1080/09557571.2019.1656600
Reichborn-Kjennerud, E., & Cullen, P. (2016). What is Hybrid Warfare? Norwegian Institute for International Affairs (NUPI). http://www.jstor.com/stable/resrep07978
Renz, B. (2016). Russia and 'hybrid warfare.' Contemporary Politics, 22(3), 283–300. https://doi.org/10.1080/13569775.2016.1201316
Republic of Estonia Information System Authority. (2022). Cyber Security in Estonia 2022.
Reuters. (2023, January 22). Netherlands sticks to plan to close Groningen gas field by October - FT. Reuters. https://www.reuters.com/markets/commodities/netherlands-sticks-plan-close-groningen-gas-field-by-october-ft-2023-01-22/
Reynolds, N. (2019). Putin's Not-so-secret Mercenaries: Patronage, Geopolitics, and the Wagner Group. In Carnegie Endowment for International Peace. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/07/08/putin-s-not-so-secret-mercenaries-patronage-geopolitics-and-wagner-group-pub-79442
Roberts, G. (1995). Soviet policy and the Baltic States, 1939–1940 a reappraisal. Diplomacy & Statecraft. https://doi.org/10.1080/09592299508405982
Rodriguez, C. (2022, August 7). The Richest Countries In The World: Tiny Luxembourg At The Top. Forbes. https://www.forbes.com/sites/ceciliarodriguez/2022/08/07/the-richest-countries-in-the-world-tiny-luxembourg-at-the-top/?sh=6a9de9ee0725
RT. (2018, March 3). Wilders: I criticize Putin's policies, but applaud the way he stands for Russian people. RT International. https://www.rt.com/news/420348-geert-wilders-exclusive-interview/
RT. (2020a, April 17). 'At least we know the button works': Dutch Twitter responds with memes after false hijacking alarm at Schiphol airport. RT International. https://www.rt.com/news/472809-schiphol-false-alarm-reactions/
RT. (2020b, May 26). Frothing mad: Dutch Air Force douses 1st F-35A with corrosive firefighting foam by mistake (PHOTOS, VIDEOS). RT International. https://www.rt.com/news/472365-dutch-air-force-damages-f35a/
RTL Nieuws. (2018, February 24). Wilders in Moskou voor afspraak met Russische politici. https://www.rtlnieuws.nl/nederland/politiek/artikel/3871421/wilders-moskou-voor-afspraak-met-russische-politici
Runnel, P., Pruulmann-Vengerfeldt, P., & Reinsalu, K. (2009). The Estonian Tiger Leap from Post-Communism to the Information Society: From Policy to Practice. Journal of Baltic Studies, 40(1), 29–51. https://doi.org/10.1080/01629770902722245
Ruus, K. (2008). Cyber War I: Estonia Attacked from Russia. European Affairs, 9(1).

Ruussaar, A. (2018, October 21). Eesti vaataja maksab Kremli kanalitele ligi kolm miljonit aastas. Postimees.ee. https://www.postimees.ee/6434613/eesti-vaataja-maksab-kremli-kanalitele-ligi-kolm-miljonit-aastas
Saari, S. (2014). Russia's Post-Orange Revolution Strategies to Increase its Influence in Former Soviet Republics: Public Diplomacypo russkii. Europe-Asia Studies, 66(1), 50–66. https://doi.org/10.1080/09668136.2013.864109
Safire, W. (1987, April 12). On Language. The New York Times. https://www.nytimes.com/1987/04/12/magazine/on-language.html
Sakwa, R. (2012). The problem of 'the international' in Russian identity formation. International Politics. https://doi.org/10.1057/ip.2012.10
Scahill, J. (2008). Blackwater: The Rise of the World's Most Powerful Mercenary Army. Gardners Books.
Schaart, E. (2020, April 17). Dutch far-right leader Baudet had ties to Russia, report says. POLITICO. https://www.politico.eu/article/dutch-far-right-leader-baudet-had-ties-to-russia-report/
Schellevis, J., & Kasteleijn, N. (2022, March 8). Sites RT en Sputnik geblokkeerd door grootste internetproviders. NOS. https://nos.nl/collectie/13888/artikel/2420302-sites-rt-en-sputnik-geblokkeerd-door-grootste-internetproviders
Schroefl, J., & Kaufman, S. S. (2014). Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War. Studies in Conflict & Terrorism, 37(10), 862–880. https://doi.org/10.1080/1057610x.2014.941435
Sietsma, S., & Houthuijs, P. (2023, January 27). Miljoenen chips Nederlandse fabrikanten belanden in Rusland ondanks sancties. NOS. https://nos.nl/artikel/2461459-miljoenen-chips-nederlandse-fabrikanten-belanden-in-rusland-ondanks-sancties
Smeets, H. (2018, July 3). Propagandastrijd rond GeenPeil. NRC. https://www.nrc.nl/nieuws/2016/01/20/propagandastrijd-rond-geenpeil-1582952-a111069
Smith, D. J. (2001). "The Devil and the Deep Blue Sea": Foreign Policy between East and West. In Estonia: Independence and European Integration (1st ed., pp. 147–175). Routledge.
Standish, R. (2019, July 25). Inside a European Center to Combat Russia's Hybrid Warfare. Foreign Policy. https://foreignpolicy.com/2018/01/18/inside-a-european-center-to-combat-russias-hybrid-warfare/
Statistikaamet. (2011). 2011 Population and Housing Census | Statistikaamet. https://www.stat.ee/en/statistics-estonia/population-census-2021/2011-population-and-housing-census
Statistikaamet. (2021). Demographic and ethno-cultural characteristics of the population | Statistikaamet. https://rahvaloendus.ee/en/results/demographic-and-ethno-cultural-characteristics-of-the-population
Stefan, B. G. (2021). Understanding sputnik news agency strategic state narratives. Bulletin of the Transilvania University of Braşov, 13(62)(1 Special Issue), 165–174. https://doi.org/10.31926/but.ssl.2020.13.62.3.17
Steinberg, P. I. (2015). Can We Generalize from Case Studies? Global Environmental Politics, 15(3), 152–175. https://doi.org/10.1162/glep_a_00316
Sterkx, S., & De Jong, S. (2010). The 2009 Russian-Ukrainian Gas Dispute: Lessons for European Energy Crisis Management after Lisbon. European Foreign Affairs Review, 15(Issue 4), 511–538. https://doi.org/10.54648/eerr2010037
Stoicescu, K. (2022, October 18). The Evolution of Russian Hybrid Warfare: Estonia. CEPA. https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-estonia/
Sytas, A. (2022, August 18). Estonia says it repelled major cyber attack after removing Soviet monuments. Reuters. https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/

Talmazan, Y. (2019, June 25). Data security meets diplomacy: Why Estonia is storing its data in Luxembourg [Video]. NBC News. https://www.nbcnews.com/news/world/data-security-meets-diplomacy-why-estonia-storing-its-data-luxembourg-n1018171
Ter Haar, B. (2017). Dutch narratives about Russian-Western relations. In Security Narratives in Europe: A Wide Range of Views' (pp. 89–97). Nomos Verlagsgesellschaft.
Thomas, T. (2020). Estonia Reacts: Confronting Russian Manipulation Techniques. In MITRE Corporation. MITRE Corporation.
Thorhallsson, B., & Bailes, A. J. K. (2016). Small State Diplomacy. In C. M. Constantinou, P. Kerr, & P. Sharp (Eds.), The SAGE Handbook of Diplomacy. SAGE Publications Ltd. https://doi.org/10.4135/9781473957930
TrendMicro. (2016, January 16). Operation Pawn Storm: Fast Facts and the Latest Developments - Wiadomości bezpieczeństwa. https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/operation-pawn-storm-fast-facts
Trouw. (2018, March 2). Wilders troebele reis naar Rusland. https://www.trouw.nl/opinie/wilders-troebele-reis-naar-rusland~b6d1d520/
Tverdostup, M. (2022). Estonia: Heading into the unknown. In Wiiw Forecast Reports: Overshadowed by War and Sanctions. The Vienna Institute for International Economic Studies.
Umland, A. (2016, July 21). Gratitude for mass murder. Kyiv Post. https://archive.kyivpost.com/article/opinion/op-ed/andreas-umland-gratitude-for-mass-murder-411508.html
U.S. Government Accountability Office (GAO). (2010). Hybrid Warfare. https://www.gao.gov/products/gao-10-1036r
Vaino, R. (2022, February 25). Four Russian TV channels banned from Estonian airwaves. ERR. https://news.err.ee/1608512162/four-russian-tv-channels-banned-from-estonian-airwaves
Van Den Beukel, J., & Van Geuns, L. (2021). Russia's Unsustainable Business Model: Going All In on Oil and Gas. The Hague Center for Strategic Studies. https://hcss.nl/wp-content/uploads/2021/01/Russias-Unsustainable-Business-Model.pdf
Van Der Kaaij, M. (2016, October 7). Samen met de Duitsers tegen Rusland. https://www.trouw.nl/nieuws/samen-met-de-duitsers-tegen-rusland~bb006e57/
Van Der Oye, D. S. (2010). Russian Orientalism: Asia in the Russian Mind from Peter the Great to the Emigration. http://ci.nii.ac.jp/ncid/BB02133006
Van Der Togt, T. (2016). Internationaal recht versus harde realpolitik : Hoe MH17 de Nederlands-Russische relatie nog lang zal belasten. Clingendael Institute.
Van Staden, A. (1974). Een trouwe bondgenoot: Nederland en het Atlantische Bondgenootschap (1960-1971).
Veebel, V., Ploom, I., & Sazonov, V. (2021). Russian information warfare in Estonia, and Estonian countermeasures. Lithuanian Annual Strategic Review, 19, 69–98.
Visser, J. (2015, October 29). Referendum EU-verdrag met Oekraïne is op 6 april. https://www.volkskrant.nl/nieuws-achtergrond/referendum-eu-verdrag-met-oekraine-is-op-6-april~b6960e5d/
Volkskrant. (2020, May 13). Minister: Rusland verspreidt ook in Nederland misleidende informatie over het coronavirus. https://www.volkskrant.nl/nieuws-achtergrond/minister-rusland-verspreidt-ook-in-nederland-misleidende-informatie-over-het-coronavirus~bd21fbe5/
Von Clausewitz, C. (1976). On War (M. Howard & P. Paret, Trans.). Princeton.
Walt, S. M. (1998). International Relations: One World, Many Theories. Foreign Policy, 110, 29. https://doi.org/10.2307/1149275
Whyte, A. (2022, March 6). Center Party board annuls agreement with United Russia. ERR. https://news.err.ee/1608522557/center-party-board-annuls-agreement-with-united-russia

Wigell, M. (2019). Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy. International Affairs, 95(2), 255–275. https://doi.org/10.1093/ia/iiz018
Wither, J. K. (2016). Making Sense of Hybrid Warfare. Connections: The Quarterly Journal, 15(2), 73–87. https://doi.org/10.11610/connections.15.2.06
World Bank. (2020). Estonia Trade. https://wits.worldbank.org/CountrySnapshot/en/EST
World Bank. (2023a). Estonia Military Spending/Defense Budget 1992-2023. MacroTrends. https://www.macrotrends.net/countries/EST/estonia/military-spending-defense-budget
World Bank. (2023b). Netherlands Military Spending/Defense Budget 1960-2023. MacroTrends. https://www.macrotrends.net/countries/NLD/netherlands/military-spending-defense-budget
Yin, R. K. (2003). Case Study Research: Design and Methods. SAGE.
Zelinska, O. (2017). Ukrainian Euromaidan protest: Dynamics, causes, and aftermath. Sociology Compass, 11(9), e12502. https://doi.org/10.1111/soc4.12502