UNIVERSITY OF TARTU
Faculty of Social Sciences
Johan Skytte Institute of Political Studies

Liis Massa

THE FRAMING OF INFORMATION WARFARE: A COMPARATIVE ANALYSIS OF ESTONIAN AND IRISH ONLINE NEWS MEDIA IN 2014-2017

MA thesis

Supervisor: Maili Vilson, MA

Tartu 2018

I have written this Master's thesis independently. All viewpoints of other authors, literary sources and data from elsewhere used for writing this paper have been referenced.

.....

/ signature of author /

The defence will take place on ..... / date / at ..... / time /

..... / address / in auditorium number ..... / number /

Opponent ..... / name / (..... / academic degree /),

..... / position /

THE FRAMING OF INFORMATION WARFARE: A COMPARATIVE ANALYSIS OF ESTONIAN AND IRISH ONLINE NEWS MEDIA IN 2014-2017

Liis Massa

Abstract

In recent years, information warfare has become one of the top priorities on the international security agenda. The significant rise of the respective threats originates from 2014, when Russia's invasion and annexation of Crimea as well as Daesh's extensive engagement in conventional and unconventional warfare caused the escalation of information war to an unprecedented scale. The severe threats of information warfare were recognised by the EU, NATO, and the Member States who have been developing defence mechanisms while emphasising the importance of social freedoms. Therefore, debates on the threats of information warfare in media, with a particular focus on digital media, have gained momentum. In turn, information warfare has also become a highly topical matter in media. Therefore, the thesis studies the framing of information warfare in Estonian and Irish online news media in 2014-2017 and interprets the differences and similarities in the media frames. The thesis employs articles on information warfare published in the three most visited Estonian and Irish online news media and applies the method of qualitative framing analysis. Three frames are identified in the media coverage of both countries: Russia-West confrontation frame, national security frame, and truth frame for Estonia, and national security frame, Russia-West confrontation frame, and technology and extremism frame for Ireland. The comparative analysis finds that the media frames reflect the different historical backgrounds of the countries, as the Estonian media frames tend to be politically more motivated to reinforce the hostility of Russia and call the Western democracies for unity. The second main difference in the frames is the coverage on extremism, principally on the example of Daesh, which was largely neglected in Estonian media for the perceived distance, but more covered in Irish media for relative closeness through the impact on the UK. Nevertheless, above all, the frames emphasised the common values and principles of the two countries.

Contents

Introduction

Technological developments in the past few decades have had a remarkable impact on warfare. Faster communication times, closer international networks, and more complex dynamics of conflicts are only few examples of the profound changes that are currently in progress. While in the 20th century, wars were described as large-scale multi-year conflicts between states through ground invasion, then the 21st century warfare is visibly shifting to the digital frontier with limited operations on the ground conducted by special forces (Slaughter, 2011). The increasing importance of the digital dimension has also entailed greater interest in information warfare by states, non-state actors, and individuals, as such non-kinetic forms of warfare can be employed at minimum cost with extensive damage. Both offensive and defensive capabilities are being researched and developed in all subareas of information warfare, of which cyber warfare and psychological operations appear as particularly topical in current public debates.

Information warfare is also a highly topical matter on the European Union's (EU) security agenda. The leaders of the EU and Member States have unanimously recognised information warfare as a threat to the security of the union and work is in progress to develop coordinated defence mechanisms, which also involve deepened cooperation with NATO. (European Commission, 2017) Therefore, building resilience and advancing the ability to counter the threats of information warfare have been set as priorities both at the supranational and state level. While there is general political consensus on acknowledging the threats, the perception of information warfare differs across the Member States, as states have different exposure to information warfare. For this reason, it is essential that the Member States would comprehend the varying perspectives in order to facilitate more informed communication and efficient interstate cooperation, as well as accommodate greater awareness within and between societies.

The rise of the digital dimension has also increased the power of media. Although media has long been an influential tool of communication for shaping attitudes in societies, the emergence of online media has multiplied the opportunities of states and other actors to spread their ideas and narratives. Therefore, online media has become a strategic battlefield of information warfare, which is used by various actors to gain superiority. Research on information warfare in online media has so far mainly focused on the questions how actors conduct information warfare and how to counter such attacks. Case studies commonly revolve around Russia and Daesh, but extensive research on information warfare has also been carried out in the context of hybrid warfare. (See Ingram, 2014; Jaitner, 2015; Wither, 2016) While authors have published studies on the framing of certain events that represent cases of the use of information warfare, there appear to be no published studies on the framing of the phenomenon of information warfare in media. Therefore, considering the influential role of media in shaping public opinion, the need for research on the framing of information warfare is evident.

Acknowledging the priority given to countering the threats of information warfare in the EU and recognising the influential role of online media in shaping public opinion, the thesis aims to fill the gap in research and study how information warfare has been framed in online news media. The author seeks to provide a comprehensive analysis on the media frames of information warfare specific to Estonia and Ireland and add value by comparing the similarities and differences in the two cases. Therefore, the thesis seeks to contribute both to the country-specific research on the framing of information warfare as well as to the EU-level research to create a better understanding of the different perspectives on information warfare. The thesis is structured in three main parts: theoretical framework, methodology, and framing analysis. First, the theoretical framework is divided into two parts: the concept of information warfare, involving the key developments and definitions, and framing theory, involving definitions and media frames. Second, the methodology comprises four parts: case selection, online news media, time frame, and qualitative framing analysis. Finally, the framing analysis has

four parts: Estonian media frames, Irish media frames, comparative analysis, and limitations.

The empirical analysis is designed as a comparative study of two cases, involving Estonia and Ireland as small EU Member States with different positions on military alignment. The time frame for the study is 2014-2017, which covers the latest period characterised by the rise of information warfare challenges. The research is based on articles retrieved from the three most visited online news media of Estonia and Ireland, which according to Alexa's country-specific rankings (2018a) are Postimees.ee, Delfi.ee, and Err.ee for Estonia (Alexa, 2018b) and Independent.ie, Irishtimes.com, and Thejournal.ie for Ireland (Alexa, 2018c). The author uses the search phrase "infosõda" (i.e., the Estonian equivalent for information warfare and information war) in Estonian media and the phrases "information warfare" and "information war" in Irish media. Adding the phrase "information war" is substantiated by the common use of the phrase as the equivalent of "information warfare" (see *Qualitative framing analysis* p. 26). Therefore, the research employs the method of qualitative framing analysis and takes the inductive approach to identifying the media frames. The author uses an individual news article as unit of analysis and identifies the media frames through the combination of multiple readings of the articles and searching for framing devices in the texts. In terms of framing devices, the study involves the rhetorical devices of keywords, word choice, and exemplars as well as the technical devices of sources of information and quotes in the articles. Finally, the identified media frames in Estonian and Irish online news media are examined independently and comparatively. The study aims to answer the two following research questions:

> Research question 1: *How has information warfare been framed in Estonian and Irish online news media in 2014-2017?*
>
> Research question 2: *What are the main differences and similarities in the framing of information warfare in Estonian and Irish online news media in 2014-2017?*

As the main sources of information, the author would highlight the works of Entman (1993), Scheufele (1999), Ventre (2016), Johnson-Cartee (2005), Hutchinson (2006), de Vreese (2005), Linström and Marais (2012), and as described above, the three most visited Estonian and Irish online news media, which provided the data for conducting the framing analysis. The author would also like to thank the thesis supervisor Maili Vilson for the support and guidance.

Theoretical framework

Concept of information warfare

Information warfare is set as the central concept of the thesis and the following chapter aims to create a conceptual framework for the analysis below. In order to place the concept in a political context, the first part will provide an overview of the key developments in information warfare and describe how has information warfare been employed by different actors. The second part will then examine three definitions of the concept and explain the approach to information warfare in this study.

Developments

Although information warfare is often discussed in the context of information age, the roots of the concept date back to the 5th century BC. From the time originates the military classic and the first known study of the planning and conduct of military operations *The Art of War*, which is attributed to the Chinese general and strategist Sunzi or Sun Tzu. One of the most famous statements in the work declares: "All warfare is based on deception" (Smith, 2017), which emphasises the fundamental role of the use or misuse of information in warfare and thus captures the core idea of information warfare. Therefore, until the emergence of modern communications technology in the 20th century, information warfare remained limited to subareas, such as misinformation, deception, and propaganda. Then the invention of the radio laid the foundation for electronic warfare, but the most rapid development of information warfare began with the invention of the microchip, which led to the use of computers on the battlefield and the rise of cyber warfare. (Mackey, 2017) The following chapter will

introduce the political context and discuss some of the key developments since the late 20th century that have shaped the modern thinking of information warfare. The events include the Gulf War of 1990-1991, 9/11 terrorist attacks and the subsequent invasion of Iraq, Russia's cyber attacks against Estonia in 2007, Russia-Georgia war of 2008, Russia's annexation of Crimea in 2014, and Daesh's information warfare.

In the early 1990s, as the Cold War was ending, the focus of information warfare was shifting from propaganda to the electronic computing and communications technology, which was employed in battlefield intelligence, targeting, and command and control. Although the use of information warfare was principally military in character and relevant in the context of war, states also engaged in media management. (Hutchinson, 2006, p. 214) According to Hutchinson (Ibid., p. 214), the US actions in the Gulf War of 1990-1991 provided a prime example of both overwhelming technological superiority and a masterful media campaign, which reflected the lessons learned from the failures of the Vietnam War of 1955-1975, where the spreading of uncontrolled information and images had led to the loss of public support and subsequently the war. Stauber (1995) describes that the US government and military officials used sophisticated tactics of information control in the Gulf War, which involved the constraining and controlling reporters and running a comprehensive public relations campaign to ensure the prevalence of the government version of events. As Hutchinson (2006, p. 214) notes: "It was becoming clear that modern wars were also media wars."

The importance of communications is inevitable from the perspective of information warfare. Buchanan (2018) explains that the most influential developments in communications originate from before or during World War II, such as television services becoming media of mass communication. Since then, the lines of development have remained largely the same, but in the 21st century, the advanced technological capabilities have become even more merged with media management (Hutchinson, 2006, p. 215). Similarly, manipulations with information in mass media was already a common practice in World War II, but the techniques for influencing the public have

been refined and today manipulations are used in combination with modern communications technology also during peacetime (Rose, 2000, p. 34). Kumar (2006, p. 54) describes the given developments in the early 2000s in light of the 9/11 terrorist attacks and the subsequent invasion of Iraq. The article argues that the US administration used the favourable public opinion and principal compliance of media to take advantage of the misconceptions about Iraq's connections with the 9/11 attacks in order to advance the government's interests through the invasion. Therefore, as there had been a rise of national sentiments after the 9/11 attacks and media followed the administration's line, the government had possessed remarkable influence over the mass perception in the US. (Ibid., p. 54) In the development of information warfare, the case presents an example of large-scale psychological warfare through the spread of misinformation, which was used to affect the audiences in the US and abroad.

In 2007, the world's first "coordinated cyber-attack against a nation state" was carried out, as Estonia experienced a series of denial of service attacks shortly after relocating a Soviet-era war memorial (Keating, 2010). The attacks were described as the first time when the national security of a nation was threatened by a botnet, which was particularly true because Estonia is an "online country" reliant on Internet connectivity (Davis, 2007). Evron (2017) explains that both government and public websites were targeted, including that of the Estonian prime minister, president, and government, as well as banks, news media, telecommunications companies, schools, etc. There had also been calls to unrest on Russian-language Internet forums, which were aimed to amplify the outrage for relocating the memorial and thus incite hostility within the society (Ibid.) Although there was no official evidence, Estonia accused Russia of the attacks, referring to the circumstances, while Russia denied government involvement, calling the claims groundless. (Davis, 2007) Nevertheless, the cyber attacks against Estonia are often viewed as the first in the series of cases, in which Russia demonstrates its information warfare capabilities (Tamkin, 2017).

According to Iasiello (2017, p. 52), during the war against Georgia in 2008, Russia was able to simultaneously employ cyber attacks and conventional military operations for the first time, while also engaging propaganda, information control, and disinformation campaigns. White (2018, p. 4) describes that in media, Russia's aim was to control the international flow of information, endorse the narrative of Russian troops protecting Russian citizens on Georgian territory, and present Georgia as the aggressor in the conflict. However, Vendil Pallin and Westerlund (2009, p. 401) argue that due to the self-admitted deficiencies in the information-technical and information-psychological domains of Russia's information warfare, including failures with command and control, electronic warfare, and disinformation campaign, Georgia was able to gain victory in the information sphere regardless of their loss on the physical battlefield. Therefore, as reflects from the literature, the war with Georgia forced Russia to rethink its tactics to avoid similar shortcomings in the future, as the victory in such confrontations depends largely on whose narrative will prevail.

In 2014, six years after the war against Georgia, Russia engaged in a conflict against Ukraine and annexed Crimea, which has been recognised as a case of hybrid warfare. Russia demonstrated that it had learned the lessons from Georgia and improved its tactics in several aspects. According to Ruiz (2017), in the information-technical area, Russia employed cyber attacks and cyber espionage against Crimea throughout the operation from early stages until after the annexation. In the information-psychological area, it was described that the main tactics included propaganda, disinformation, denial, and deception (Ibid.). Further, in order to influence the public opinion towards supporting the pro-Russian version of events, Russia engaged in creating favourable television broadcasts as well as news items, blog content, and social media posts (Kofman, Rojansky, 2015). Finally, Snegovaya (2015, p. 15) explains how Russia was able to keep the US and NATO from intervening thanks to firmly denying its involvement in Crimea and managed to annex Crimea in a way that would seemingly follow the democratic procedures. The article also notes that only after the annexation of Crimea, Russia accused the Western states of having double standards on foreign

troop deployment, as the aggressor did not need to rely on the tactics of denial any longer (Snegovaya, 2015, p. 15).

However, information warfare has not only been employed by states, and the most prominent example is the terrorist organisation Daesh, also known as the Islamic State, IS, ISIS or ISIL. The origins of Daesh date back to 1999 and the organisation expanded from then on, culminating with the caliphate announcement and establishment of the Islamic State in 2014. (Zgryziewicz, 2015, p. 15) Although by 2018, Daesh has lost 98% of the territory it once held in Iraq and Syria (Mills, 2018), the organisation has enjoyed success in terrorism activities and information campaigns in recent years. As Misra (2015) explains, aiming to fulfil the apocalyptic prophecy of the victory of the Islamic State by defeating all enemies, Daesh has developed a powerful information strategy, which includes gaining supporters, uniting Sunni Muslims, frightening adversaries, and spreading information about the caliphate. Daesh has been described to used both direct communication as well as social media platforms, whereas the gains from the effective and flexible use of social media have been considered particularly remarkable (Awan, 2017). Zgryziewicz (2015, p. 41) then discusses in greater detail how the social media platforms are organised in large and small communities, which enables to recover quickly from attacks on the communities, making Daesh difficult to eliminate.

The discussion above has provided an overview of some of the key developments in information warfare since the end of the Cold War. Although the author acknowledges that the earlier events have had a remarkable impact on the thinking of information warfare, the more recent developments were preferred to introduce the modern issues, which are of greater priority considering the focus of the empirical analysis on media frames from 2014-2017. In other words, the introduction of the recent events also carried the purpose of providing background information for the analysis and discussing the political context, in which the media frames will be viewed. Further, the chapter has presented the evolving character of the concept and illustrated how different actors

conduct information warfare. The cases also demonstrate the complex challenges of information warfare, which are principally related to the diversity of subareas and battlefields. However, in order to gain a more concise understanding of information warfare, the following chapter will examine three definitions to the concept.

Definitions

As the overview of the developments in information warfare has illustrated the complex nature of the concept, the author will now seek to narrow the discussion and focus on the definitions of information warfare. Three widely cited definitions will be discussed and they then used to formulate the approach to information warfare in this thesis.

The first definition has been proposed by Winn Schwartau in 1994:

> *"Information warfare is an electronic conflict in which information is a strategic asset worthy of conquest or destruction. Computers and other communications and information systems become attractive first-strike targets."* (cited in Ventre, 2016, p. 267)

The definition is very characteristic to the understanding of information warfare in the 1990s, as it concentrates on the military domain and the context of war as well as prioritises the role of information and communications technology (see *Developments*, p. 10). As Schwartau's definition limits the concept only to electronic conflicts, it takes a narrow and essentially military approach on security. On the other hand, emphasising the importance of information *per se* and recognising it as a strategic asset also implies more modern thinking of information in warfare, as the shift from focusing on technology to include information as such appeared more broadly around the turn of the millennium (Hutchinson, 2006, p. 213).

The author of the second definition is Daniel Ventre and it originates from 2008:

> *"The aggressive/defensive use of information space components (which are*

> *information and information systems) to reach/protect the sovereignty of a nation through actions conducted in times of peace, crisis or conflict."* (cited in Ventre, 2016, p. 271)

In many aspects, Ventre's definition characterises the modern approach to information warfare. First and foremost, Ventre places information warfare not only in the context of war, but also connects the concept with periods of peace and crisis. Therefore, unlike in the 1990s, the thinking of information warfare had changed to consider it as a constant phenomenon in the previous decade. The reference to the use of information environment components, which can be both tangible and intangible elements, also provides a broader set of tactics compared to the electronic or cyber warfare in Schwartau's definition. However, Ventre limits the aim of information warfare to "reaching or protecting the sovereignty of a nation", which may be too restrictive in regard to the type of actors, given the example of Daesh that is essentially a Sunni religious group.

The third definition is by Rianne van Vuuren (2015) from 2015:

> *"Information warfare is defined as actions focused on destabilising or manipulating the core information networks of a state or entities in society with the aim to influence the ability and will to project power as well as efforts to counter similar attacks by an opposing entity and/or state."*

The definition by van Vuuren illustrates the fundamental shift in the conceptual thinking of information warfare in the past two decades: while Schwartau placed information warfare in the narrow context of war, then van Vuuren has moved further to also include the civilian and social sphere. Further, as van Vuuren's definition involves both states and entities in societies, it overcomes the limits of Ventre's state-centric approach to correspond to the modern circumstances and capture the different types of actors engaged in information warfare. The focus on core information networks as the object of destabilisation or manipulation allows to fit the broad spectrum of subareas and security issues in the definition.

In the following analysis, the understanding of the concept of information warfare will be based upon the same principles as presented in the definition by van Vuuren. The discussion on the elements of the definition has proven the good fit of the approach with the contemporary circumstances, particularly in regard to the inclusion of the civilian sphere and different kind of actors. However, the author will also take an element from Ventre's definition, which is the understanding of information warfare as a constant phenomenon, visible throughout the periods of peace, crisis, and conflict. Therefore, the thesis will be based on a comprehensive approach to information warfare and aim to involve diverse type of instances in the framing analysis.

Framing theory

This chapter will introduce framing theory, which serves as the theoretical foundation of the empirical analysis. The first part examines the definitions of frames and framing as well as explains the conceptual distinction between individual and media frames. The second and final part focuses on media frames and discusses the concept in greater detail.

Definitions

According to van Gorp (2007, p. 60), the roots of framing theory date back to the first half of the 20th century and originate from cognitive psychology and anthropology. From the 1970s, the concept of framing has also been taken over by other disciplines, e.g., sociology, economics, linguistics, communication science, and public relations research (Ibid.). Therefore, because of the diverse use of the concept, there are different kind of definitions available for the concepts of frames and framing. In order to avoid conceptual vagueness, the author will examine four definitions of key importance from the perspective of the thesis.

One of the most recognised definitions to framing has been proposed by Entman (1993, p. 52), who emphasises social interaction as the essence of framing:

> *"Framing essentially involves selection and salience. To frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described."*

Although not explicitly stated, the definition implies the presence of a communication source, which can be a news medium, political leader, news consumer, etc (Johnson-Cartee, 2005, p. 24). In the process of framing, communicators interact with their

sources and other actors, and the receivers interact with the content and other receivers, which then becomes a multi-level interplay (van Gorp, 2007, p. 64). As the definition suggests, framing is about determining certain problems, identifying the reasons for the problems, evaluating the causal forces and their effects, and finally proposing solutions and outcomes for the matter. However, all of the four functions may not be included in one frame occurring in a text, as framing can also involve fewer. (Entman, 1993, p. 52)

Second, the concept of frame has been defined by Tankard, Hendrickson, Silberman, Bliss, and Ghanem (1991, cited in Johnson-Cartee, 2005, p. 24) as follows:

> *"A frame is a central organising idea for news content that supplies a context and suggests what the issue is through the use of selection, emphasis, exclusion, and elaboration."*

Although the definition describes frame as "a central organising idea", it shall be emphasised that the actual frame does not appear in the content, thus the text and the frame have to be distinguished from each other (van Gorp, 2007, p. 63). Frames and their social construction are both invisible, as the use of frames is natural and often goes unnoticed (Gamson et al., 1992, p. 374). Further, there are frames that are applied as well as frames that could be applied and outnumber the former as alternatives. Distinguishing the different frames helps to understand potential approaches to certain events, as the interpretation can depend to a great extent on the frame. (van Gorp, 2007, p. 62) The reason for such influence is that frames spotlight certain elements of reality and conceal others (Entman, 1993, p. 53), as also explained in the definition above by Tankard et al.

Third, from the perspective of the following empirical analysis, it is essential to elaborate on the conceptual distinction between individual and media frames. Scheufele has based the distinction on Kinder and Sanders (1990, cited in Scheufele, 1999, p. 106):

> *"(...) frames serve both as "devices embedded in political discourse," which is equivalent to the concept of media frames, and as "internal structures of the mind," which is equivalent to individual frames."*

Rather than focusing on individual frames and studying the "mentally stored clusters of ideas that guide individuals' processing of information" (Entman, 1993, p. 53), the author has chosen to concentrate on media frames and interpret how has information warfare been presented in media. The essence of media framing is captured in the following definition:

> *"By framing social and political issues in specific ways, news organisations declare the underlying causes and likely consequences of a problem and establish criteria for evaluating potential remedies of the problem."* (Nelson, Clawson, Oxley, 1997 cited in Johnson-Cartee, 2005, pp. 25-26)

The definition is close to the definitions of framing and frame discussed above, but it is more specific in defining the fields of research, as the authors focus more specifically on social and political issues. Therefore, the three definitions form an integral conceptual foundation for the study of the media frames of information warfare.

Media framing

As described above, media frames are understood as abstractions or devices that organise and structure the meaning of certain problems. Media frames are prioritised for their ability to shape individuals' perception of the problems and thus impact public opinion, which in turn explains the importance of conducting research on media framing and effects. Therefore, in order to gain a deeper understanding of media framing, the following chapter will discuss the concept of media framing in relation to the framework of social constructivism, framing as part of the communication process, approaches to identifying media frames, and the key characteristics of media frames.

According to Scheufele (1999, p. 105), the current stage of research on media effects, which started in the early 1980s, is characterised by social constructivism. In principle, social constructivism is concerned with "the creation and institutionalisation of reality in social interaction" (Berger, Luckmann, 1966 cited in van Gorp, 2007, p. 62). Therefore, in a constructivist media effects model, audiences create their own version of reality, which is a combination of personal experience, interactions with other actors, and selected media frames (Neuman, Just, Crigler, 1992 cited in Scheufele, 1999, p. 105). Acknowledging the importance of media frames, one also has to consider the role of media makers. Entman (1993, p. 54) and other authors have recognised the influence of applying a range of persistent frames in media, which implies certain control over alternative frames. Consequently, when individuals construct the social reality, they are partly dependent on the frames made available by journalists. (van Gorp, 2007, p. 62) The described model of dependency illustrates the nuanced characters of both social interactions as well as media framing.

The discussion on the constructivist media effects model has implied the two-sided nature of media frames: on the one hand, it emphasises the effects on the audience, and on the other hand, it involves research on the media content (Knudsen, 2014, p. 209). Therefore, focusing on the latter can be conditionally considered as the first step in studying the communication process in framing, although the influences of media frames are also inseparable from the content creators. In a more nuanced approach to framing, Entman. Matthes, and Pellicano (2009, p. 178) distinguish between the categories of strategic framing, journalistic framing, frames in media content, and framing effects. Due to the limited scope of the thesis, the empirical analysis will focus on frames in media content, which entails examining "the selection and salience of certain aspects of an issue by exploring images, stereotypes, metaphors, actors, and messages" (Ibid., p. 180). Matthes and Kohring (2008, p. 259) distinguish between five methodological approaches for identifying media frames: hermeneutic, linguistic, manual holistic, computer-assisted, and deductive approach. The first two, the hermeneutic and linguistic approach, belong to the broader category of qualitative frame

analysis (Entman et al., 2009, p. 180), which appears as a more common term in literature and will thus be used in the empirical analysis (see *Qualitative framing analysis*, p. 26).

The final part of the discussion will address some of the key characteristics of media frames. According to Entman (1993, p. 52), frames in the news can be identified by "the presence or absence of certain keywords, stock phrases, stereotyped images, sources of information, and sentences that provide thematically reinforcing clusters of facts or judgments." In a similar manner, Pan and Kosicki (1993, p. 56) find that frames appear in media content through different framing devices, such as metaphors, exemplars, catchphrases, depictions, and visual images. In other words, framing devices that make a reference to the same idea are identifiable as parts of a distinguishable theme or frame (van Gorp, 2007, p. 64). Further, frames illuminate certain information about a subject and thereby aim to make it more memorable for the audience. In order to make some information more salient, media makers apply different techniques, such as placement, repetition, but also using cultural links and symbols. (Entman, 1993, p. 53) However, the effect on the audience cannot be automatically assumed, as it also depends on the individual frames of the receivers (van Gorp, 2007, p. 63), which then reinforces the idea of individual and media frames as distinct but integrated categories.

Methodology

This chapter introduces the methodological approach to the empirical research. The first part discusses case selection and the reasons for choosing Estonia and Ireland as the two cases for the comparative study. The second part presents the three Estonian and three Irish online news media, where the content for the framing analysis was extracted. The third part provides the timeframe for the analysis, and finally, the fourth part explains how the qualitative framing analysis was conducted. Therefore, the chapter creates a methodological basis for answering the following research questions in the empirical analysis:

> Research question 1: *How has information warfare been framed in Estonian and Irish online news media in 2014-2017?*
>
> Research question 2: *What are the main differences and similarities in the framing of information warfare in Estonian and Irish online news media in 2014-2017?*

Case selection

Estonia and Ireland are relatively small European countries with populations of comparable size: approximately 1.3 million (Statistics Estonia, 2017) and 4.8 million (Central Statistics Office, 2017) people respectively. Both states are democratic parliamentary republics and members of the United Nations (UN) (United Nations, 2018), Organisation for Economic Co-operation and Development (OECD) (OECD, 2018), Organisation for Security and Co-operation in Europe (OSCE) (OSCE, 2018), and the EU (European Union, 2018a). While Ireland accessed the EU in 1973 (European Union, 2018b), then Estonia over three decades later, in 2004 (European Union 2018c). In addition, both countries have adopted the euro, but only Estonia is a member of the Schengen area, as Ireland has negotiated an opt-out from the Schengen

agreement. (European Union, 2018b; European Union 2018c) In light of current political developments in the EU, particularly Brexit, the leaders of both countries have emphasised their support for the unity of the EU (Cooper, 2017). Moreover, Estonia and Ireland along with other small liberal EU states view each other as natural allies for sharing common values and a vision for deepening the Economic and Monetary Union (EMU) (Donohoe, 2018).

However, there is a particular difference between Estonia and Ireland, which is related to their positions on the alignment with military alliances. Since the 1930s, Ireland has been committed to a policy of military neutrality, which is understood as "non-membership of military alliances" (Department of Foreign Affairs and Trade, 2018). In Cottey's view (2018, p. 175), the anti-militarist and normative foreign policy is not only traditional to Ireland's political culture, but it has become part of their national identity. In terms of EU membership, Ireland's military neutrality is guaranteed under the Lisbon Treaty (Department of Foreign Affairs and Trade, 2018). Nevertheless, as the later prime minister Enda Kenny put it in 2006: "Truth is, Ireland is not neutral. We are merely unaligned" (cited in Smyth, 2017a). Kenny seems to have been right, considering that Ireland joined NATO's Partnership for Peace programme in 1999 (NATO, 2018) and has since become increasingly involved in the European military cooperation and integration, including the low-profile NATO partnership as well as the EU structures (Cottey, 2018). Some of the examples of Ireland's participation in the EU military cooperation structures are the Nordic Battlegroups and most notably the Permanent Structured Cooperation (PESCO) as one of the 25 EU member states involved. (Finn, 2018; European Council, 2017)

Estonia, on the other hand, accessed NATO in 2004 and considers active involvement as a strategic priority of Estonian security and defence policy. In fact, Estonia started participating in international operations already in 1995, only four years after regaining its independence from the Soviet Union in 1991. (Ministry of Foreign Affairs, 2017a) For Estonia, the broader European integration process along with the accession to

NATO and the EU were of vital importance for historical reasons, and are now seen as the fundamental elements for the country's lasting endurance. For this reason, Estonia has been in strong favour of such developments as establishing PESCO, bringing the EU battlegroups in actual use, securing the Nordic-Baltic region with NATO troops, etc (Ministry of Foreign Affairs, 2017b). Therefore, as reflects from the discussion, the key difference compared to Ireland is Estonia's NATO membership as aligning with a military alliance. Given the relative similarity of Estonia's and Ireland's political profiles, the matter of military alignment along with the different historical and geopolitical backgrounds provide an interesting nuance worth further investigation also in the context of media frames, which will be discussed in the comparative analysis (see *Comparative analysis*, p. 51)

Online news media

The empirical analysis on the framing of information warfare concentrated on online news media as data sources. Online news media were chosen because of the increasing use of computers and reliance on Internet sources. According to Eurostat (2018), 71% of people living in the EU used the Internet on a daily basis or almost every day in 2016, whereas 70% of all Internet users read news online. Furthermore, online news media publish more articles than print media and thus provide more data for analysis. Finally, online news media enable an efficient and precise search for articles, as users are able to search for certain words or phrases in a preferred time frame. Therefore, for the purpose of collecting sufficient amount of data for the framing analysis, the research involvesd the three most visited online news media of Estonia and Ireland, which were selected according to Alexa's country-specific ranking. Alexa (2018a) is recognised as one of the most reputable competitive intelligence tools around the world and thus counts as a reliable source of information. The calculation for a country-specific rank of a website combines the estimated average of daily unique visitors and estimated number of page views in the past month, using data from Alexa's global traffic panel that samples

millions of Internet users as well as data from direct sources that have installed the Alexa script on their website and allow Alexa to measure the traffic. (Alexa, 2018a) As the country-specific rankings combine websites of all kinds and origins, the top three Estonian and Irish news media were found from the respective country's list through a careful manual search. Due to the limits of Alexa's public data, it was not possible to access the rankings from the time period covered in the study, 2014-2017, therefore, the rankings have been referred to as of 25 April 2018. However, given the timely proximity, the choice of sources can be considered valid.

Table 1. Most visited Estonian online news media. (Alexa, 2018b)

Online news media	Position in the country-specific ranking
Postimees.ee	6.
Delfi.ee	7.
Err.ee	25.

Table 2. Most visited Irish online news media. (Alexa, 2018c)

Online news media	Position in the country-specific ranking
Independent.ie	17.
Irishtimes.com	24.
Thejournal.ie	39.

Time frame

The time frame for the analysis was limited to four years from 2014 to 2017, thus covering the most recent developments in the framing of information warfare. Given that the thesis does not study a certain event but the phenomenon of information warfare, the author faced the inevitable issue of selecting a particular time frame.

Although the decision to focus on the most recent period provided the natural choice of the previous year as an ending point, one could argue for several starting points as being most suitable for the study. Consequently, the author acknowledges that the starting point of 2014 can be contested, but there are indeed two influential reasons for selecting this particular year. First, the 2014 Russia's invasion and annexation of Crimea has been recognised as the escalation of information war to an unprecedented scale (Applebaum, 2014; Shekhovtsov, 2015), which together with the subsequent war in eastern Ukraine "represent the culmination of an evolutionary process in Russian information warfare theory and practice" (Giles, 2016, p. 4). Second, in the same year, Daesh engaged in extensive conventional and information warfare, which allowed them to capture territory in Iraq and Syria as well as enabled the organisation to become a global phenomenon (Gambhir, 2016). The increasing threats of information warfare were recognised by the EU, NATO, and the member states, which led the organisations to discuss advanced cooperation and establish the European Centre of Excellence for Countering Hybrid Treats in 2017 (European Union External Action, 2017). The author finds that the cases demonstrate the rise of information warfare issues in 2014, but emphasises that the framing analysis covering the period of 2014-2017 also included all other cases of information warfare in the selected online news media.

Qualitative framing analysis

As discussed in the section *Media framing* (see p. 20), there are various methodological approaches to conducting framing analysis, which are in nature qualitative, quantitative, or a combination of the two. Given the aim of the thesis to gain an in-depth understanding of how information warfare has been framed in online news media, the author has chosen the qualitative approach, which facilitates the quality of context-sensitivity and enables to emphasise the cultural and political content of news frames (Linström, Marais, 2012, p. 27). Qualitative framing analysis requires comprehensive work with the texts and approaching the content in a holistic manner to identify the

frames. Connolly-Ahern and Broadway (2008, p. 369) have highlighted the following advantages of qualitative framing analysis:

> *"(...) it (a) examines the key words, metaphors, narratives, and so on, in context of the text as a whole; (b) identifies what was left out of the frame as well as what was included; and (c) recognises that the words repeated most often in a text may not be the most important."*

Therefore, as opposed to the quantitative approach, qualitative framing research does not entail creating categories of news texts and discourse with the aim to measure their size or count their frequency (Reese, 2007 cited in Linström, Marais, 2012, pp. 25-26), but it is rather an interpretative approach to examine phenomena in a holistic manner.

In order answer the first research question and explain how information warfare has been framed in Estonian and Irish online news media in 2014-2017, the author had to begin by collecting the articles on information warfare from the selected Estonian and Irish online news media in the given time frame. For Estonia, the employed search word was "infosõda" (i.e., the Estonian equivalent for information warfare and information war), and for Ireland, the search phrases were "information warfare" and "information war". The reason for adding the phrase "information war" was the limited number of results to the original search phrase (see *Irish media frames*, p. 40), which appeared to be a matter of the use of language in media, as the articles including the phrase "information war" provided sufficient information also on "information warfare". Therefore, as the articles were collected separately for both countries, the next step was to identify the frames. The unit of analysis was an individual news article, which provided a clear and comprehensible structure for working with the articles. The selection of frames was based on the inductive approach, which means that the frames were identified in the process of analysing the content of each individual article. (de Vreese, 2005, p. 53) Although the inductive approach is criticised as being subjective, it is in turn flexible and context-sensitive, which enables the researcher to identify the frames more precisely (Touri, Koteyko, 2014, 602). In identifying the frames, the author

first read the articles multiple times and followed the four-step process proposed by Wimmer and Domincik (2006 cited in Linström, Marais, 2012, p. 31):

- Articles were comparatively distributed into categories;
- The categories were refined;
- Themes were found among the categories;
- The categories were simplified and integrated into coherent frames.

The author also searched for the presence or absence of framing devices in order to identify the frames. The choice of the framing devices was guided by the research problem (Ibid., p. 31) and to reach the aim of producing a comprehensive analysis of framing, both rhetorical and technical devices were included. Therefore, the rhetorical devices involved keywords, word choice, and exemplars (Ibid., p. 32), while the technical devices included sources of information and quotes in the articles (Pan, Kosicki, 1993, p. 60). Combining the two processes of creating categories through multiple readings and searching for framing devices enabled to identify three dominant frames in both Estonian and Irish online news media. Due to the limited scope of the thesis, secondary frames in the articles were not identified. The discussion on the frames was substantiated by examples of the quotes, which in parallel illustrated the use of sources. In addition, the author aimed to provide diverse examples of the instances covered by the frames to create a comprehensive overview of the media frames. Finally, the comparative analysis examined the main differences and similarities in the framing of information warfare in Estonian and Irish online media in 2014-2017 to answer the second research question regarding the differences and similarities of Estonian and Irish media frames. For this purpose, the analysis discussed the frames, key aspects of the frames, and framing devices in Estonian and Irish media, while elaborating on the differences and similarities along with the causes and peculiarities.

Framing of information warfare

Estonian media frames

Following the criteria for the selection of articles as described above (*Online news media*, p. 24), the author found 142 articles from 2014-2017 that employed the term "infosõda" (i.e., the Estonian equivalent for information warfare and information war): 83 articles from Postimees.ee, 17 articles from Delfi.ee, and 42 articles from Err.ee. Three major frames were identified in the media coverage: Russia-West confrontation frame, national security frame, and truth frame.

Table 3. Identified frames by online news media.

Online news media	Russia-West confrontation frame	National security frame	Truth frame
Postimees.ee (n=83)	40	19	24
Delfi.ee (n=17)	6	6	5
Err.ee (n=42)	18	13	11
Total (n=142)	64	38	40

Russia-West confrontation frame

The Russia-West confrontation frame was most commonly utilised in the coverage of information warfare. The frame was constructed through the description of Russia's robust information operations against the Western states along with the discussion on the defensive capabilities and reactions of the West. Some of the main keywords that

characterised the frame were “war”, “influence”, “division”, “propaganda”, and “manipulation”. The defining idea of the Russia-West confrontation frame was thus to illuminate Russia’s war-like assertive actions related to the hostile and manipulative use of information against the West with the purpose of dividing the unity of the Western organisations, states, and societies to gain superiority. (Tagel, 2016a) In addition, there were two decisive judgements about the confrontation: first, Russia is the offender and uses its negative reputation to gain an advantage, and second, the West is losing the information war. (Nael, 2017) In order to gain a deeper understanding of the Russia-West confrontation frame, the following discussion will elaborate on the constructed roles of both Russia and the West in the context of information warfare.

The questions why and how Russia conducts information warfare against the West were of particular importance in this frame. There was remarkable consistency in describing the aims of Russia’s information warfare, both in terms of wording and tone, in line with the following example:

> *“The aim of the authoritarian Russia’s information warfare has always been to undermine the democracies of the Western states, cause instability within the societies, amplify the existing ideological, racial, sexual orientation, religious, and other such divisions.”* (Kiin, 2017)

The emphasis on the governance regime, i.e., authoritarian Russia versus democratic West, was often used to stress the opposition and presumably create a positive cultural connection for the Western audiences. On the other hand, the frame favoured democracies by describing them as being more vulnerable in information war, given that as for their values, democracies cannot equally respond to the type of actions employed by the authoritarian Russia (Nael, 2017). For the same reason, Russia’s arguments of only engaging in information warfare to answer to the similar hostile actions by the West were rejected and ridiculed (Laaneots, 2015). As the frame separated the causes of Russia’s information warfare from any allegedly provocative actions of the West, it insisted that Russia’s aims were predominantly related to increasing its influence and achieving information superiority (Tagel, 2016a).

The discussion on how Russia conducts information warfare focused on a broad range of elements, such as institutions, media, methods, and narratives. Russia's information warfare was understood as a total and exceptionally powerful phenomenon:

> *"Russia's kind of information warfare not only means a maze of disinformation, fabrications, information leaks, and cyber sabotage. Russia goes way beyond by creating "new reality" and mass hallucinations."* (Kooli, 2014)

The frame reinforced the notion of Russia's superiority in information warfare, as it described the state's extensive engagement in developing the respective capabilities. For example, several articles addressed the Russian defence minister's presentation before the State Duma, which confirmed the creation of more advanced special information forces (Postimees.ee, 2017a). In this case, the utilisation of a high level official source also amplified the effect of the announcement. On the contrary, there was an interview with a former employee of the Russian troll fabric, which aimed to portray the true reality behind the information campaigns through personal experience (Postimees.ee, 2015a). Further, the discussion on Russia's information warfare involved Russia's cyber operations and diverse use of media in psychological operations, including news media, social media, political blogs, and others of the kind. The spreading of fake news and posting pro-Russian comments in media were recognised as the present time threats (Tagel, 2016b). Finally, the frame cautioned against Russia's narratives about the internal divides in the Western societies, high terrorist attack threats, and the incapability to deal with the migration crisis (Ehand, 2017), which were denied and condemned as hostile propaganda.

A particular characteristic of the Russia-West confrontation frame was the focus on the opposition in general rather than describing concrete instances in detail. For example, in recent years, Russia has been repeatedly accused of intervening in the domestic politics and attempting to manipulate with the elections of several Western states, including the US, France, Germany, and the Netherlands (Tagel, 2016a; Nael, 2017; Kiin, 2017). However, instead of providing detailed overviews of the events, the instances were

mostly utilised as a set of examples to illustrate the more principal or technical discussions on Russia's information warfare:

> *"It is well known in Kremlin that when there are elections in some country, it is time to intervene — then the conditions for influencing opinions are most favourable. The US elections took place, we witnessed that Russia was very active. The same will surely happen in France, Germany, and the Netherlands."* (Tagel, 2016b)

Therefore, although the different elements of Russia's information warfare, which were discussed in the previous paragraph, were more dominantly represented in the frame than concrete events, the instances of Russia's interventions were included as part of the broader opposition. Moreover, the repeated use of the same set of examples could have carried the purpose of making the issue more memorable for the audiences, along with the subtle reference to the togetherness of the West under the attacks by Russia.

Finally, the frame discussed the defensive capabilities and reactions of the West. There was common recognition that the Western states needed more efficient coping mechanisms against Russia's information operations, especially while dealing with complex matters like Brexit and the rise of populism (Tagel, 2016c; Weber, 2017). In the discussions on the defensive measures, the term "propaganda" was much rather utilised than "information warfare", as in the following example:

> *"Should we organise counter-propaganda? I think it will not work. We need to spend more money to fight with propaganda. First, states need to have their own attractive news channels. It is a good idea to create new Russian language television channels, analyse facts, rise public awareness, fight with trolls, and tell the truth."* (Tagel, 2016a)

The frame assured that the Western democracies were going to take constructive measures against Russia's information warfare, as described in the example above, while opposing their approach to that of Russia. It was prioritised that media freedom and ideational pluralism would prevail, while emphasising the need to educate the audiences about the threats of Russia's manipulations with information. (Szostek,

Randlo, 2015; Tagel, 2016c) As a concrete counter-measure, the creation of European External Action Service was highlighted, which would focus on investigating Russian propaganda and collaborating with the eastern partners on media freedom (Aasaru, 2015). However, despite some optimism, the overall tone of discussion was serious, as the Western states have come to realise the severity of the challenges posed by Russia's information warfare.

National security frame

The second frame, which was utilised in the coverage of information warfare, was the national security frame. This frame described information warfare as a threat to national security and it was constructed through three subcategories: threats of information warfare to Estonia's media, Estonia's psychological security, and the threats of information warfare to the national security of other states. The frame involved keywords and phrases, such as "integration", "information space", "psychological defence", and "information hygiene". The diverse challenges of information warfare were inspected at the state level and exclusively from the defence perspective. Abstaining from public debates on offensive capabilities can be related to the Western democratic value system and the opposing position that the Western states have taken towards the offenders. In this way, the national security frame communicated with the Russia-West confrontation frame that was examined in the previous part. However, the national security frame was in character more inwards looking and it was concerned with the domestic effects as opposed to the international level of analysis of the Russia-West confrontation frame.

The main concern of the national security frame was the threat of information warfare to media. The discussion focused on the information space of the Russian population in Estonia and the available information channels, but also on broader integration issues.

The frame utilised a quote by the Estonian president to stress the necessity to ensure both the availability of reliable information as well as public awareness about the trustworthy channels:

> *"We can hear very Estonian-minded opinions in Russian and very Russian-minded opinions in Estonian. The language does not determine anything. What is important, that people know that the Estonian Public Broadcasting is the channel where they receive reliable information. This is what you must keep here* [Estonian Public Broadcasting]." (Kook, 2017a)

The Russian language television channel under the Estonian Public Broadcasting was established only recently and it has not become a prime source of information for the Estonian Russian population. For this reason, certain Estonian political powers, most prominently the Centre Party, have justified cooperating with the Russian television channel PBK (Kook, 2017b), while it has been widely criticised by others. The national security frame endorsed the disapproving position, as it condemned the channel for serving the interests of the imperialist minded Russia and echoed the criticism towards the choice to cooperate with PBK. (Kross, 2017; Velsker, 2017) The frame also emphasised the risks related to the Russian government controlled news agency Sputnik and was open about the threat of hostile information reaching the Estonian audiences (Helme, 2014). The recommended solution in the frame was more direct and constant communication with the Russians living in Estonia, which was stressed to require comprehensive work with the whole media field, not only the television (Gamzejev, 2014).

The second element in the national security frame was the psychological security of the Estonian society. On the one hand, the frame was concerned with psychological defence and discussed the state engagement in different areas, such as how the state ensures trust for the government and defence organs, prevents the spreading of disinformation, counters hostile influence operations, etc (Einmann, 2015). Concrete initiatives, such as the non-military part of the national defence development plan, were highlighted with the purpose of deepening the trust for state institutions in providing psychological

defence against information warfare (Salu, 2014). The frame again utilised a quote by a high-level source, the chairman of the Foreign Affairs Committee of the Riigikogu (i.e., the Estonian parliament), to increase the salience of psychological defence:

> *"(...) it is important to understand that those win in information wars who protect their values and principles."* (Nael, 2014)

In addition to the government-centric approach, the frame discussed the societal aspects of psychological security. In a call for "information hygiene", paraphrasing the more well-known phrase of cyber hygiene, a political scientist explained in a playful and approachable tone how target audiences engage in information warfare without acknowledging it:

> *"I mean our own dear compatriots, neighbours, and family members who either out of boredom or sincere desire spread this garbage information. Who share stories and pictures on their social media accounts without bothering themselves even with a brief background check."* (Tüür, 2017)

As the final point on psychological security, the frame rose the issue of psychological warfare within societies through an article, which drew parallels between the situations where hostile groups attack experts in public debates and information warfare between states, as in both the offenders label, ridicule, or question the authority of the target (Minnik, 2016). The comparison allowed to combine the social and political issues in a clever manner and educate the audience on the highly prioritised matter of information warfare.

Although the frame concentrated in greater detail on the threats of information warfare to Estonia's national security, it also had an international dimension, which discussed the threats in an alternative context. The aim of integrating foreign issues into the frame could have been increasing the validity of domestic concerns, as presenting similar challenges from elsewhere expands the scope of the problem and makes the case more plausible for both the domestic and international audiences. Moreover, it could be seen as an aligning device, which demonstrates Estonia as one of the countries under attack and fosters solidarity through mutual experiences. Several of the instances covered in

the frame concerned Latvia and Lithuania (Laugen, 2016; Postimees.ee, 2014a; Postimees.ee, 2015b), who share a similar geopolitical position with Estonia and also identify themselves as targets of Russia's information warfare. For example, the frame included a quote by the Lithuanian president on an amendment of legislation that would impose severe fines on companies promoting war propaganda:

> *"We are facing new and daily information attacks. Their target is our population. (...) The constitution obliges us to defend the information space of Lithuania. We cannot be weaponless in this war."* (Postimees.ee, 2014a)

Similarly, Finland was of high interest in this frame (Laugen, 2015; Postimees.ee, 2014b), which can be explained by its role as a neighbouring country and a close partner that shares border with Russia. However, there were also examples from darker realities, which represent few of the severest cases of information warfare — Ukraine and Russia. (Kannel, 2015; Treufeldt, 2014) The descriptions of the total information warfare could be used to raise support for Ukraine, warn the society about the worst case scenarios, or highlight the human rights issues in Russia to claim moral superiority. The frame utilised saddening narratives and tones of hopelessness when depicting the current situation in Russia, which could be concluded with a quote by a Russian human rights activist:

> *"It is not war anymore but the same kind of occupation that at the level of foreign policy is taking place in Crimea. We have no free speech anymore, definitively."* (Ibid.)

Truth frame

The final frame in the coverage of information warfare was the truth frame. It was constructed through discussions on truth and valid information, or the lack thereof, in information warfare. The keywords and phrases in this frame were "ethical", "freedom of speech", "information overload", "trust", and "believe". Therefore, the truth frame

functioned as an organising idea for articles concerning the principal ethical problems of information warfare, the role of media in the context of information warfare, and the lack of truth in information warfare. Moral considerations were central to the frame, as the theme was inseparable from one's values and principles. In this regard, the social freedoms of the Western democratic value system were prioritised, including the freedom of expression, freedom of press, and others of the kind. The frame made a negative moral judgement about neglecting the freedoms by the same token, emphasising that countering information warfare could not come at the cost of the democratic values.

The ethical concerns in the truth frame were primarily focused on the options that democratic states hold for defending themselves against information warfare. Given the core principle to protect the social freedoms, the frame highlighted the great challenges that the democratic states experience, as they also need to commit to protecting their sovereignty from hostile foreign influence. (Allik, 2014) The issue was illuminated through a quote by a recognised journalist who took a deeply concerned tone on the matter:

> *"But when one side uses all (true, already known from the antique time) rhetorical devices and in addition, manipulations enabled by the new media — editing videos and audio files, ripping segments out of context, priming, framing, etc, based solely on the Jesuit principle that the end justifies the means... then what exactly remains for those who play on the so-called white side?* (Hõbemägi, 2014)

The use of the "white side" metaphor reinforces the moral contrast between the opposing sides and implies the innocence of those included in the abstract group of the "wide side". The frame prioritised moral superiority over winning in the information war, as the latter was considered impossible in such asymmetric confrontations, where one side employs means that are unthinkable for the other. Moreover, the frame contended that the democratic states do not even possess the means, such as state

controlled media agencies, to bend the truth on such a scale to engage in extensive information warfare. (Mihkelson, 2014)

The truth frame also focused on the role of media in information warfare. From the ethical perspective, the frame insisted that in the context of information warfare, media agencies carry particularly high responsibility for the information they communicate to the audiences. There was an article by a deputy chancellor of the Estonian Ministry of the Interior, which addressed the elements of trust and responsibility in media to highlight the threats of information warfare:

> *"An institution, publication, or a person with a fine and trustworthy reputation has taken direction according to the moral compass. Deviating from the course or letting one's critical sense and attention fade is dangerous, because an uncontrolled half-truth or total lie will then quickly transform into a plausible fact."* (Koort, 2014)

The strong emphasis on morality and the fading lines between truth and lies was used to draw attention to the risks of information warfare to media freedom, both at the domestic and international level. While the frame recognised Estonia's free media, it expressed concern over the global decrease in media freedom, largely caused by information warfare. (Postimees.ee, 2015c) The negative influence of information operations was also discussed in regard to social media, which was seen to have an increasing influence over how the audiences understand certain events or phenomena. The frame utilised the example of Daesh that has not only reached the audiences through social media, but has managed to catch the attention of news agencies who cover Daesh's social media activity and thus present it to even wider audiences. (Allik, 2014)

Finally, the truth frame covered the issue of valid information in the context information warfare. The same problem was risen in the quote above in the previous paragraph, as it referred to the dangers of uncontrolled half-truths and total lies. Therefore, as the cause of the concerns over information validity, the frame described the practice in hostile

information operations that blends lies with selected facts to make the lies more plausible or confuse the audience (Masso, 2015). True information was said to be manipulated and used in a way that would present the subject, for example, a state or person, as unreliable and incompetent, while the reason for it may stay unclear for the audience. In addition, the speed of presenting information and the large amount of it were identified as risks to information validity. (Koort, 2014) Reflecting on the challenges that audiences face in information warfare, the frame utilised a capturing quote by a journalist:

> *"People are learning the grammar of the new reality — distinguishing between truth and lies."* (Rebane, 2016)

Further, the frame included a particular idea about the purpose of establishing multiple truths through information warfare, which was seen as part of the status policies of global powers. The frame took a severely critical tone regarding such aims of certain authoritarian and totalitarian states (Kiin, 2015), most prominently Russia and North Korea, and emphasised the need to provide "objective truth" to the populations that only have access to the state's "alternative truth" (Postimees.ee, 2017b). There was an example of an organisation that secretly imported memory sticks with information from the "free world" to North Korea, which was envisioned to liberate the population's awareness from the strict limits of the regime-controlled information and give the people a chance to create their own vision (Ibid.). The frame endorsed the normative approach and thus reflected the moral judgments on truth that were characteristic also to the other aspects of the frame.

Irish media frames

Following the criteria for the selection of articles as described above (*Online news media*, p. 24), the author found in total 74 articles from 2014-2017 that employed the phrases "information warfare" and "information war". First, 18 articles were found that included the phrase "information warfare": 3 articles from Independent.ie, 12 articles from Irishtimes.com, and 3 articles from Thejournal.ie. Second, 56 articles were found that included the phrase "information war": 7 articles from Independent.ie, 42 articles from Irishtimes.com, and 7 articles from Thejournal.ie. Three major frames were identified in the media coverage: national security frame, Russia-West confrontation frame, and technology and extremism frame.

Table 4. Identified frames for the search phrase "information warfare" by online news media.

Online news media	National security frame	Russia-West confrontation frame	Technology and extremism frame
Independent.ie (n=3)	3	0	0
Irishtimes.com (n=12)	4	4	4
thejournal.ie (n=3)	2	0	1
Total (n=18)	9	4	5

Table 5. Identified frames for the search phrase “information war” by online news media.

Online news media	National security frame	Russia-West confrontation frame	Technology and extremism frame
Independent.ie (n=7)	3	3	1
Irishtimes.com (n=42)	21	8	13
thejournal.ie (n=7)	4	1	2
Total (n=56)	28	12	16

National security frame

In Irish online news media, the most commonly used frame was the national security frame. The frame was constructed through describing information warfare as a threat to the national security of various Western states, but also to that of Ukraine. Three main subcategories were distinguished in the frame: threats to the US national security, threats to Ireland’s national security, and threats to the national security of other states. Some of the main keywords and phrases were “elections”, “intervene”, “manipulation”, and “fake news”. The frame approached the matter of information warfare from the defence perspective and the threats were predominantly identified as deriving from an external source. (Emmott, 2017; McLaughlin, 2016; Scally, 2017) However, there was one peculiarity related to the subcategory of threats to the US national security, which also involved the dimension of internal threats and thus provided a multi-level discussion on the threats. (Derrig, 2016; Edwards, 2017a) In addition, the incidents in the given subcategory were described in greater extent and detail compared to the other two subcategories. The particular interest in the US national security by the Irish media could be explained by the US status as a superpower with higher relevance to the very

current topic of information warfare compared to Ireland, but also for the ancestral and economic ties between the two countries.

The US national security frame was primarily focused on the state's 2016 presidential elections, in regard to both external and internal threats of information warfare. As the source of the external threat, the frame identified Russia for arguably intervening in the respective elections. (Schmidt, Mazzetti, Apuzzo, 2017) The frame utilised a quote by the chairman of the House of Representatives homeland security committee, who expressed concern over the impact of the intervention in the severest tone:

> *"The threat is worse than just espionage. Our democracy itself is at risk. Last year, there's no doubt in my mind that the Russian government tried to undermine and influence our elections. They broke into political institutions, invaded the privacy of private citizens, spread false propaganda. They created discord in the lead-up to a historic vote."* (Edwards, 2017a)

The quote referred to the intervention as an existential threat to democracy, the underlying value of the state, in order to increase the salience of the issue. The claims about the intervention originated from the US security agencies, which were identified as the initial source of information about Russia's "influence campaign" during the elections. Russia's aims were described as to support the candidacy of Donald Trump and damage that of Hillary Clinton, as the former would fit Russia's interests better. (Lipton, Sanger, Shane, 2016) While the intervention was described as a Soviet style propaganda campaign, it was recognised that the effective use of cyberspace enabled Russia to carry out a very large-scale operation (Shane, 2017). Finally, the intervention was also interpreted as Russia's response to the US' attempts to promote democracy and thus undermine Russia's power in its "near abroad", most prominently in Georgia and Ukraine (Ibid.).

The internal threats of the US national security were related to the presidential campaign of Donald Trump. The frame involved an article, which described the services of the political consultancy company Cambridge Analytica and their contribution in the

final phase of Trump's campaign. It was argued that the campaign engaged in sophisticated propaganda to manipulate with the voters:

> *"Data mining by political campaigns is nothing new, but individualising these statistical presumptions through psychological theory, coupled with media that can choose who sees which messages, is new."* (Derrig, 2016)

While it was recognised that the method proved to be highly effective, there were deep concerns about the morality of the approach, considering that the main keywords used to describe the method were "propagandist" and "manipulative". (Ibid.) However, Trump was not only criticised for hiring the services of Cambridge Analytica, but also for his reaction to the claims of Russia's intervention in the elections. The frame took a disapproving tone on Trump's rejection of the intelligence agencies' findings on Russia's intervention and considered his attitude improper in the given circumstances. (Lipton, Sanger, Shane, 2016) Moreover, there were considerable suspicions that Trump had colluded with Russia during the presidential campaign, as various links between the members of Trump's campaign and the Russian government were pointed out, but due to the lack of official evidence, the accusations remained moderate. (Irishtimes, 2017) Trump's response was to label the claims as "fake news" (Shear, 2017).

The second subcategory in the national security frame was Ireland's national security. Although Ireland's defence matters were not as widely covered in media as the issues of the 2016 US presidential elections, there were concerns about the threats of information warfare to Ireland's national security:

> "*There is growing evidence which shows that manipulation is underway by various State actors aimed at undermining the democratic process. It's important that we do all we can to protect the integrity of our democratic process here in Ireland."* (Doyle, 2017)

The quote by an Irish politician addressed the threats of information warfare and emphasised the fundamental need to protect the democratic order from the treats. In the same way, the frame introduced the new legislation, which criminalised the use of internet bots to influence political debate as well as the promotion of fake news on

social media. (Doyle, 2017) It was stressed that the aim of the legislation was to counter information warfare on social media to protect the democratic process in Ireland from interventions similar to the US presidential elections (Ibid.), which reflected the priority given to the democratic values. Finally, Ireland's national security was discussed in the context of deepening the EU cooperation in security and defence and the establishment of PESCO. Closer cooperation with the EU partners was encouraged in the frame, as it was seen to advance the protection of cyberspace and support countering the manipulation of information in the future. (Tonra, 2017)

The final subcategory in the national security frame discussed the threats to the national security of several Western states, such as Spain, France, Germany, and Estonia, but also that of Ukraine. The frame portrayed the instances of information warfare in the given states from the defence perspective and connected the attacks with different offenders. For example, the frame described the information attacks of groups based in Russia and Venezuela against Spain during Catalonia's independence referendum, aimed to promote the separatist cause and destabilise Spain (Emmott, 2017). Estonia's national security was discussed in relation to the 2007 cyber attacks by Russia and the development of the state's defensive capabilities since then (McLaughlin, 2016). Russia was also associated with the hacks into the German parliament's computer network (Scally, 2017), but likewise were there concerns about the US espionage in Germany, which included spying on the chancellor Angela Merkel's mobile phone (Thejournal.ie, 2014). Similarly, the frame described how a French television network was hacked by Daesh (Independent.ie, 2015), but also presented the sabotage accusations against Kremlin controlled media by the French then presidential candidate Emmanuel Macron in his words as follows:

> *"(...) agents of influence which on several occasions spread fake news about me personally and my campaign."* (McLaughlin, 2017a)

Although the frame was in general supportive of the accusations, it took a more critical stance on Ukraine, as the state decided to block access to Russian social networks due to the threats of propaganda and cyber attacks (McLaughlin, 2017a). The disapproving

attitude reflected the idea that social freedoms could not be restricted for the sake of countering information warfare, which was in turn approved in the responses of the Western states.

Russia-West confrontation frame

The second frame in the Irish media coverage of information warfare was the Russia-West confrontation frame. The frame described Russia's information campaign against the West and the reactions of the Western states. The keywords and phrases utilised in the frame included "divide", "destabilise", "manipulate", "propaganda", and "cyber attack". The frame focused on a range of elements that characterise the confrontation: the aim of Russia's information warfare, Russia's narratives about the West, and the cultural dimension of the confrontation. The attitudes in the frame were supportive of the Western states and opposed to Russia, which also reflected from the use of sources. On the one hand, Russian sources were quoted to present the opposing ideas and hostile messages (Smyth, 2017b), and on the other hand, Western sources were utilised to criticise Russia (McLaughlin, 2017b). Therefore, it was evident that the frame reinforced the confrontation for the audiences. While the frame involved various Western states, it did not include Ireland in the discussion. The reason might have been Ireland's limited exposure to direct information warfare so far, but the attitudes in media make a clear statement about the state's position on the matter.

The aims of Russia's information warfare were broadly discussed in the frame and there was general consensus that engaging in information warfare served Russia's interests at the highest level. The primary importance of information warfare for Russia was interpreted by a senior fellow at the American Foreign Policy Council:

> *"For President Vladimir Putin, information warfare aimed at destabilising its geopolitical opponents is nothing less than a cornerstone of Russian foreign policy."* (Cluskey, 2017)

While the quote referred to Russia's core aim of destabilising the geopolitical opponents, it did not specify how the instability would be achieved. The general methods were introduced by the former Estonian foreign minister:

> *"I think Russia has the more abstract and much broader goal of creating confusion in our societies, and discrediting democratic governments and our structures, institutions and elections."* (McLaughlin, 2017b)

The emphasis on "our societies", "democratic governments", and "our structures (…)" reflected Estonia's perception and aims, as the state has been directly affected by Russia's information warfare and for defence purposes, continually seeks to reaffirm the unity of the Western allies. The frame recognised that despite some delay, Western states other than the eastern European countries have also come to realise the severity of the threats of Russia's information warfare (Ibid.).

The second element in the Russia-West confrontation frame were Russia's narratives about the West, which were seen to be used to influence the opinions of both domestic and international audiences. Russia was considered particularly successful in shaping the perceptions about the EU at the domestic level, as three quarters of Russians were said to have a negative opinion about the union according to a poll. The keywords used to describe the union were "hypocritical", "multicultural", and "decadent", which followed the government's narrative. (Smyth, 2017b) In order to introduce how Russia's narratives portrayed the West, the frame utilised a quote by a Latvian translator and editor who also countered internet trolling:

> *"Russian trolls here say that NATO and the EU are weak and divided; the Baltic countries are failed states, where everything is bad and everyone leaves to find work; that we have lost our sovereignty to the decadent West and there are no gains from EU membership; and that NATO is provoking Russia and making us a target."* (McLaughlin, 2017c)

Using a source with expertise in countering internet trolling could have carried the purpose of presenting the information about Russia's narratives more reliable. Although the given quote was rather specific to the Baltic states, the frame also described Russia's claims that addressed the West more broadly. For example, according to Russian's narratives, the EU was collapsing under the migration crisis, conducting information warfare against Russia, struggling with the rise of fascism and nazism, denying any moral principles, etc. (Smyth, 2017b) In defence of the West, the frame condemned and partly ridiculed the allegations, while avoiding overly emotional tones. (Ibid.)

Finally, the frame included the element of confrontation between Russia and the West in the cultural dimension. The news relevant to this element were potentially attractive to wider audiences, as the topics were not as specific to the field of politics and international relations. First, the frame addressed Russia's doping scandal that was caused by the World Anti-Doping Agency's report, which claimed that the Russian government assisted with hiding the use of doping by its athletes. (McLaughlin, 2015) Although several Russian sources were utilised to describe their position on the matter, the frame expressed skepticism towards the views, as the Russian sources argued that the report was part of the Western information campaign. Both Russian politicians and sports figures labelled the report as a tool of information warfare. (Ibid.) The second example touched upon the 2016 Eurovision song contest and the victory of Ukraine with a political song, which indirectly addressed the 2014 Russia's annexation of Crimea. Russia contended that Ukraine's victory was politically motivated and once again part of the Western information warfare against Russia. (Martin, 2016) The key phrases on Russia's behalf were "general demonstration" and "politics that beat art". (Ibid.) The frame took a neutral tone on the topic and did not make moral judgements on the allegations, apart from skepticism of the Western information warfare, which could have been to avoid unnecessary conflicts with the other parties.

Technology and extremism frame

The final frame in the Irish media coverage on information warfare was the technology and extremism frame. The frame was constructed through describing the use of technology by extremists and means to counter the threats. The main keywords and phrases were "radicalise", "recruit", "social media", and "cyber attack". There were three major elements in the frame: tools and platforms employed by extremists, large-scale cyber attacks by extremists, and means to counter extremism in the cyberspace. As reflects from the title of the frame, the discussion was rather technical and focused on cyber issues with a direct effect on the societies. Extremism in the frame was principally related to Daesh and North Korea (O'Dwyer, 2017a), providing examples of both non-state and state actors engaging in information warfare. The technology and extremism frame was clearly directed at the society and aimed to educate, which was visible in the tone and style of writing, particularly in the articles addressing the tools and platforms used by extremists as well as means to counter extremism. Therefore, instead of merely reflecting on certain events or phenomena, the frame also included and activated the audience with the purpose of preventing and countering extremism.

The first category in the frame introduced the information warfare tools and platforms employed by extremists. The discussion focused primarily on the success and practices of Daesh. It was described how al-Qaeda's recruitment and spreading of information was based on the tactics of information operations and electronic warfare, while adding that Daesh has moved forward to take full advantage of the social media platforms:

> *"Isis expanded that* [al-Qaeda's] *approach, developing sophisticated tools to amplify its propaganda material across social media, from Twitter accounts to YouTube videos, going so far as to develop an app called the Dawn of Glad Tidings to retweet its messages from the accounts of its followers."* (O'Dwyer, 2017a)

In addition to data mining, the frame referred to big data analysis of social media as a frequent practice of Daesh, which ensures the efficient distribution of information.

Spreading “fake news” on Facebook with shocking headlines to attract more clicks was provided as a traditional example of Daesh’s practices, which was considered particularly worrisome in combination with Facebook’s algorithms (Ibid; Smyth, 2016). The frame also stressed the important role of encrypted communication apps, such as WhatsApp and Telegram, which enable secret conversations out of the reach of intelligence agencies. (O’Dwyer, 2017a) Finally, the frame utilised a chief architect and product director for an IT security company as a source to shed light on the future cyber security challenges, not only deriving from Daesh but also other actors. According to the source, cyber wars will evolve to affect connected household devices through the Internet of Things, which will be the next step from computer terminals. (Slattery, 2017)

The technology and extremism frame also involved articles on large-scale cyber attacks by extremists, which provided examples of the realised risks of information warfare. The most extensively covered case were the WannaCry attacks in 2017, which affected hundreds of thousands computers in over 100 states. The main characteristics of WannaCry were explained in the frame as follows:

> *“WannaCry is a form of ransomware, a malware worm that encrypts the contents of a hard drive and holds the data hostage, and is demanding payment of between $300 and $600 to a Bitcoin account to unlock the encryption.”* (O’Dwyer, 2017b)

While the attacks were unanimously condemned, there were also serious moral concerns about the fact that the tools used for WannaCry attacks had been stolen from the US National Security Agency (NSA) (Ibid.). The US accused North Korea of the WannaCry hacks, likewise the 2014 destructive attack on Sony Pictures Entertainment (Rosen, Kelley, 2014). Although Ireland was not reportedly harmed by the WannaCry attacks, the state’s minister of communication could only consider the state and organisations “lucky” (Power, 2017). The judgement presented an appropriate acknowledgement of the state’s vulnerability in cyberspace and reinforced the need to develop the respective defence capabilities. In the same way, the frame discussed attacks on healthcare data and big data, which were recognised as “the greatest security

threats in the coming years" (Edwards, 2017b). Moreover, the prospective shift to "non-traditional avenues of attack" was seen to involve more actors in information warfare and damage organisations and individuals who have not invested in cyber security due to the lack of previous of exposure (Ibid.).

The final element of the technology and extremism frame was countering extremism in the cyberspace. There were two major normative judgements on countering the threats from extremists that led the discussion: first, technology companies have to get more involved, and second, democratic states need to intensify cooperation. In regard to the latter, the frame utilised a quote by the British prime minister as a call for action:

> *"We need to work with allied democratic governments to reach international agreements that regulate cyberspace to prevent the spread of extremism and terrorism planning."* (O'Dwyer, 2017a)

For the same purpose, further cooperation was insisted between the technology industry and governments. There was a common recognition that cyberspace has become the new battlefield, which needs better regulation and to this end, a "digital Geneva Convention" was proposed (Edwards, 2017c). The frame emphasised that technology alone could not counter extremism, as extremists are highly adaptable to new technological solutions, exemplified by the evolution from using social media to also include cryptocurrencies, etc (Ullah, 2017). Therefore, it was maintained that countering extremism in cyberspace requires a comprehensive and analytical approach to data. For example, in the field of terrorist recruitment, it was considered essential to focus on separating relevant social media data from the "ineffective layers", as it is not possible nor necessary to counter all extremist communication (Holden, 2015). In addition, the frame drew attention to the importance of combining data analysis with research on cultural contexts, as the way extremism forms was described to be related to the cultural context (Ibid.). Therefore, coming to understand the root causes to one turning to extremism would also be key to countering it.

Comparative analysis

The previous chapters have analysed the framing of information warfare in Estonian and Irish online news media between 2014-2017. The author identified three frames in the media coverage of both states: Russia-West confrontation frame, national security frame, and truth frame for Estonia, and national security frame, Russia-West confrontation frame, and technology and extremism frame for Ireland. This chapter aims to provide a comparative analysis of the Estonian and Irish media coverage to elaborate on the differences and similarities to gain more comprehensive knowledge of the framing of information warfare (see *Qualitative framing analysis*, p. 26). Therefore, the author seeks to answer the following research question:

> Research question 2: *What are the main differences and similarities in the framing of information warfare in Estonian and Irish online news media in 2014-2017?*

In order to provide a comprehensive answer to the research question, this chapter will compare the following elements relevant to information warfare in Estonian and Irish media: coverage and priority given to information warfare, framing of the confrontation between Russia and the West, framing of Russia's interventions in the internal affairs of other states, framing of threats to national security, truth versus technology and extremism, and the use of rhetorical and technical devices in the media frames.

Estonian and Irish media gave considerable coverage and priority to information warfare, as there were 142 articles published in Estonian media and 74 articles in Irish media in the given time frame. Although the number of articles is not central to the qualitative analysis, the fact that there were nearly twice as many articles published in Estonian media compared to Irish media refers to few salient differences between the two states. The main reason for the variation is related to the states' different geopolitical positions and historical backgrounds, which also translated into the content of the frames. More specifically, due to the historical background, Estonia is still

influenced by Russia's foreign policy and information warfare as part of it despite accessing the EU, NATO, and other Western organisations. Given that Estonia is greatly exposed and directly affected by Russia's information warfare (see Case selection, p 22), the state cannot afford to refrain from discussions on the respective risks and defence matters, both in terms of internal affairs and in the context of international defence cooperation. For this reason, countering information warfare is one of the priorities on Estonia's national security agenda and it receives a lot of coverage also in media. On the other hand, Ireland as a militarily non-aligned state with a fortunate geopolitical position has had limited exposure to information warfare and although the state and media acknowledge the respective threats, it is understandable that information warfare is not given equal priority in Irish media to that of Estonian media.

The geopolitical and historical differences described above can be connected with the framing of the confrontation between Russia and the West in Estonian and Irish media. Although comparing the number of articles included in the frame carries again an illustrative purpose, there was a significant difference between Estonia and Ireland in this case: in Estonian media, the Russia-West confrontation frame involved 64 articles, while for Ireland the respective number was 16. The difference is not only remarkable in absolute quantities, but also considering the proportional representation of the frame in Estonian and Irish media coverage. Therefore, in order to give meaning to the priority of the Russia-West confrontation frame in Estonian media and the moderate to small representation in Irish media, it pays to revisit the geopolitical and historical differences, which appear to have an influence also on the content of the frames. The general tone of the Russia-West confrontation frame in Estonian media was inciting, both in terms of reinforcing the opposition as well as calling for unity against Russia. The frame emphasised the conflicting principles of the democratic West and the authoritarian Russia and insisted on deepened cooperation between the democratic states. The characteristics and elements of Russia's information warfare were also thoroughly investigated and condemned as to claim moral superiority over Russia. The Irish media coverage took a similar attitude, as it discussed the hostile aims and

narratives of Russia's information warfare, while acknowledging the need for advanced cooperation between the Western democracies. However, the Irish media frame did not cover the characteristics of Russia's information warfare in such extent and detail as Estonian media, as the topic is less relevant for Ireland. In addition, the Irish media frame involved the cultural dimension of the confrontation, which reflects a more versatile approach to the topic than that of Estonia, which had the narrow political focus on reinforcing the unity of the West.

Estonian and Irish media coverage also involved the aspect of interventions in the internal affairs of other states with a primary focus on elections as part of Russia's information warfare. In Estonian media, Russia's interventions in elections were depicted as an element of the principal confrontation between Russia and the West, which were utilised to reinforce the opposition and Russia's hostility. The interventions in the elections of the US, France, Germany, and the Netherlands were included in a set of examples, which was then used to illustrate the broader confrontation. As described above, Irish media was less concerned with the opposition between Russia and the West, which also reflected from the coverage on the interventions. In Irish media, the interventions were discussed from the perspective of national security and were thus included in the national security frame. The key reason for the variation was the Irish media's approach to the interventions as separate cases rather than a set of elements part of the broader opposition as in Estonian media. The Irish media coverage involved more extensive descriptions of the interventions and discussed Russia's information warfare case by case without explicitly emphasising the connections between the interventions. The variation in the approaches relates back to the geopolitical and historical differences, which also inform the states' national interests. In this case, Estonia's national interest is to reinforce the unity of the West at all levels for defence purposes, whereas the issue is not as acute for Ireland and thus the less politically motivated approach.

The national security of Estonia and Ireland were inseparable elements of the national security frames. In Estonian media, the discussion focused on the areas of media and psychological security. The threats of information warfare to media were related to the information space of the Russian minority, available information channels, and integration issues in the Estonian society, while psychological security was discussed in connection to psychological defence at the state level, "information hygiene" in the society, and information warfare within the society. The frame also utilised instances of information warfare from other states as an aligning device or a warning to draw attention to the national security issues. In Irish media, the threats of information warfare were principally seen as a risk to the state's democratic process. Legislative measures were introduced to counter the threats and deepened defence cooperation at the EU level was encouraged to protect the Irish national security. Due to Ireland's limited exposure to information warfare so far, much of the discussion was directed to the future and focused on preventive measures to defend Ireland against the attacks as experienced by the US, Estonia, and other democratic states. Therefore, the depth of discussion in Irish media differed remarkably from that of Estonia, whose extensive exposure and experience with information warfare reflect from the debates in media. The variations derive again from the states' different geopolitical positions and historical backgrounds, which have a direct effect on the national security challenges.

One of the most visible differences in the framing of information warfare in Estonian and Irish media was the variation in the third frame, which was the truth frame for Estonia and the technology and extremism frame for Ireland. In Estonian media, the truth frame was primarily concerned with the moral and ethical considerations, which were discussed in relation to the opportunities of the democratic states to defend themselves against information warfare, the responsibility of media to provide reliable information, and information validity in the context of information warfare. In Irish media, the technology and extremism frame touched upon the tools and platforms employed by extremists, large-scale cyber attacks by extremists, and countering extremism in the cyberspace. Although the frames are seemingly different, there were

noticeable similarities in the moral judgements represented in Estonian and Irish media, which emphasised the importance of the democratic values and the comprehensive security of the societies. Both of the frames were also concerned about information validity and the impact of the spreading of hostile information on the societies. However, the key difference reflected from the discussion on extremism, which was neglected in Estonian media in the way it was represented in Irish media, namely through the focus on Daesh. The reason could be the perceived distance from the direct threats of Daesh in Estonia and the more narrow focus on Russia. Ireland, on the other hand, does not have such distance, as the UK has been severely affected by Daesh. Therefore, the technical and societal aspects of extremism stand much closer to Ireland than to Estonia, which was also visible in the media coverage.

The final aspect focuses on the rhetorical and technical devices in the Estonian and Irish media frames. First, the observed rhetorical devices were keywords, word choice, and exemplars. The keywords in the Estonian media were principally related to offences, e.g., “war”, “division”, “manipulation”, values, e.g., “ethical”, “freedom of speech”, “trust”, and aims, e.g., “integration”, “psychological defence”, “information hygiene”. In Irish media, the keywords touched upon offences, e.g., “destabilise”, “intervene”, “cyber attack”, information sabotage, e.g., “propaganda”, “fake news”, “manipulation”, and extremism, e.g., “radicalise”, “recruit”, “social media”. The parallel category of offences reflects the similar understanding of the nature of information warfare, while the differences in the other categories refer to more country-specific discussion topics, such as extremism in Irish media. In regard to word choice, there was a tendency in the frames to use the word “propaganda” as synonym to “information warfare”, which applied to the media frames of both countries. Third, as for exemplars, Estonian and Irish media emphasised the supremacy of the values and practices of the Western states over the offenders conducting information warfare against them. Second, the observed technical devices were sources and quotes. It was a common practice in the frames to utilise high-level and expert sources to claim validity and reliability, as information warfare is a sensitive matter in both regards. The position and expertise of the sources

were emphasised before the quote to create an authoritative association. On the other hand, quoting the social deviant was more visible in Irish media, particularly in describing the cultural dimension of the confrontation between Russia and the West. The similar use of the rhetorical and technical devices captures once more the common underlying values of Estonia and Ireland that have been reaffirmed in this chapter despite the influences of different geopolitical positions and historical backgrounds.

Limitations

As a final part of the framing analysis, the author would discuss three main limitations of the study. First, the research is unable to explain in which way the media frames affect public opinion. Due to the limited scope of the thesis, the study was focused on media frames, which enable to analyse how certain issues are presented to the audience and presume the potential effect, but the concrete impact cannot be automatically assumed (see *Media framing*, p. 19). Therefore, further research on the topic could involve the area of individual frames to explain the effects of the media frames the on the audience's perception. Second, the research was limited in terms of search phrases. While the search phrases were the equivalents of information warfare, the research could be extended by including other relevant search phrases, for example, the subareas of "psychological warfare" and "cyber warfare". In this case, the scope would again exceed the limits of the thesis, but it could provide interesting insight into the topic. The third and final limitation to be discussed is related to the number of cases included in the research. While the given thesis was a comparative study of two cases, then future research could increase the number of cases. For example, an extensive study could involve all EU member states to gain knowledge about the perspectives on information warfare and thus facilitate mutual understanding and more informed communication both at the political and societal levels. However, a large-N study of this kind would either require a group of researchers or predefined frames.

Conclusion

In recent years, the threats of information warfare have become an inseparable part of discussions on security and defence. While states and other actors have employed the means of information warfare throughout the history, the threats to states and societies have become much more significant in information age. The primary concerns in regard to information warfare are related to the threats to people's minds, described by psychological warfare, and threats to the technology and information technology infrastructure, which involves physical and virtual infrastructure. The trends are worrying in both categories, as the widespread use of computers entails the greater exposure to information warfare and people can be affected by various means, may it be hacks, fake news, or others of the kind. In regard to hacks, the past few years have demonstrated that the attacks can be as serious as to take over hundreds of thousands of computers around the world or threaten the democratic processes in some of the most influential countries. Similarly, the psychological operations threaten the societies, as truth is being blended with half-truths and lies, which makes it difficult to distinguish valid and reliable information from the so-called alternative truths. This process is further spurred by social media, which is skilfully employed by trolls and terrorist groups. These developments illustrate how powerful information can be, if combined with refined tactics and devices, which also explains the priority of countering information warfare on the international security agenda.

The thesis has provided an insight into the described developments through analysing the framing of information warfare in Estonian and Irish online news media in the past four years since 2014 to 2017. The aim of the research was to identify the main media frames in the respective countries, elaborate on the elements and framing devices that constitute the frames, and produce a comparative analysis of the two cases with the purpose to give meaning to the differences and similarities in the perspectives on information warfare. In order to conduct the framing analysis, the author collected the

articles from the three most visited online media of Estonia and Ireland. Following the selection criteria (see, the author found 142 articles from Estonian media in 2014-2017 that employed the term “infosõda” (i.e., the Estonian equivalent for information warfare and information war): 83 articles from Postimees.ee, 17 articles from Delfi.ee, and 42 articles from Err.ee. In Irish media, the author found in total 74 articles from 2014-2017 that employed the phrases “information warfare” and “information war”. First, 18 articles were found that included the phrase “information warfare”: 3 articles from Independent.ie, 12 articles from Irishtimes.com, and 3 articles from Thejournal.ie. Second, 56 articles were found that included the phrase “information war”: 7 articles from Independent.ie, 42 articles from Irishtimes.com, and 7 articles from Thejournal.ie. Following the criteria for identifying the frames, the author identified three frames in the Estonian media coverage on information warfare: Russia-West confrontation frame, national security frame, and truth frame. In Irish media, there were also three frames identified: national security frame, Russia-West confrontation frame, and technology and extremism frame.

In the Estonian media coverage on information warfare, the most commonly utilised frame was the Russia-West confrontation frame. The frame was constructed through describing the authoritarian Russia’s information warfare against the democratic West, while emphasising and prioritising the moral superiority of the democracies. Most characteristic keywords were “war” and “division”, which were used to reinforce the hostile character of Russia’s actions and the aim to amplify any divisions in and between the Western states. One of the key examples of the frame was presenting Russia’s interventions in the elections of the US, France, Germany, and the Netherlands as a set of examples, which portrayed Russia as the offender and reaffirmed the unity of the West under the attacks. The second frame was the national security frame. The frame discussed information warfare as a threat to national security and inspected the challenges at the state level exclusively from the defence perspective. It was constructed through three subcategories: threats of information warfare to Estonia’s media, Estonia’s psychological security, and the threats of information warfare to the national security of

other states. The main keywords were “psychological defence”, and “information hygiene”. The primary issue of was the information space of the Russian population in Estonia and the frame echoed the opinion that communicating with the Kremlin-controlled television channel PBK was not justified to reach wider Russian language audiences. There was also an interesting example of a call for “information hygiene”, which was aimed to warn against engaging in information warfare by sharing uncontrolled material on social media. The final frame in the Estonian media coverage was the truth frame. The central concerns of the frame were truth and valid information, or the lack thereof, in the context of information warfare. Main keywords included “ethical” and “freedom of speech”. The frame discussed the ethical challenges of democratic states in protecting the social freedoms as well as their sovereignty from hostile foreign influence. As the frame endorsed the normative approach to democratic freedoms, it provided an example of an organisation that was providing information from the outside world to people in North Korea to liberate the population’s awareness.

In Irish online news media, the most represented frame was the national security frame. The frame was constructed through describing information warfare as a threat to the US national security, Ireland’s national security, and to the national security of other states. The main keywords were “elections” and “intervene”. Above all, the frame was concerned with the US presidential elections of 2016. While in other cases, the frame identified the external sources of threat, then in the context of the US elections, Russia was described as the external threat and Trump’s presidential campaign as the internal threat. The second frame was the Russia-West confrontation frame. This frame discussed the aims of Russia’s information warfare, Russia’s narratives about the West, and the cultural dimension of the Russia-West confrontation. Most characteristic keywords were “propaganda” and “destabilise”. Russia was found to successfully manipulate with the opinion of domestic audience in claiming that the West was “hypocritical”, “multicultural”, and “decadent”. The final frame in Irish media was the technology and extremism frame. The frame discussed the use of technology by extremists and means to counter the threats, as it described the tools and platforms

employed by extremists, large-scale cyber attacks by extremists, and means to counter extremism in the cyberspace. The principal keywords used in the frame were "radicalise" and "cyber attack". The two main examples of extremism involved first, the success and practices of Daesh with a focus on social media, and second, the large-scale cyber attacks in 2017, known as the WannaCry attacks. The frame acknowledged the severe threats posed by the skilful use of technology by extremists and called the democratic states to cooperate on countering the threats of extremists.

The comparative analysis of the Estonian and Irish media coverage focused on the following range of elements: coverage and priority given to information warfare, framing of the confrontation between Russia and the West, framing of Russia's interventions in the internal affairs of other states, framing of threats to national security, truth versus technology and extremism, and the use of rhetorical and technical devices in the media frames. The author found that the varying coverage of information warfare in terms of the number of articles published and the content of the frames reflects the different historical and geopolitical background of the states. This aspect was also present in other elements of comparison. For example, in Estonian media, the Russia-West confrontation frame reinforced the conflict between the democratic West and the authoritarian Russia and called the Western states for deepened cooperation, as the threats from Russia are perceived more sharply. In Irish media, the Russia-West confrontation frame acknowledged the opposition, but the coverage was more diverse in terms of content, as it also included a dimension of cultural confrontation. Interestingly, Russia's interventions in the internal affairs of other states were included in different frames in Estonian and Irish media: while Estonian media used the interventions as a set of examples to reinforce the Russia-West confrontation, then Irish media approached the instances from the perspective of national security, as it was politically less motivated. In terms of the states' own national security, Estonian media engaged in heavy present-day discussions on the information space of the Russian minority and the psychological security of the society, whereas in Irish media, the discussion was more directed to preventing the damage of information warfare and legislative measures. In regard to the

variation in the third frame, truth versus technology and extremism, the author found that the seemingly different frames were connected through emphasising the democratic values and the comprehensive security of the societies. As Estonian media prioritised discussions on moral considerations and information validity in the context of information warfare, it left aside the threats of Daesh, which were well covered in Irish media. The author connected this variation with the perceived distance of the threat for Estonia, as Ireland is much closer to the threat through the damage Daesh has caused to the UK. Finally, the rhetorical and technical devices in the Estonian and Irish media frames were compared. The keywords were compared as categories, which in Estonian media were described as relating to offences ("manipulation"), values ("freedom of speech"), and aims ("integration"), whereas in Irish media, the keywords touched upon offences ("intervene"), information sabotage ("propaganda"), and extremism ("radicalise"). Further, both Estonian and Irish media often used "propaganda" as a synonym to "information warfare" in terms of word choice and viewed Western democracies as exemplars as opposed to undemocratic regimes. High-level and expert sources were utilised in both countries to claim validity and reliability, while Irish media was more likely to also quote the social deviant. In conclusion, the author found that despite certain variety in the states' frames and positions, which derives from the different geopolitical and historical background, the comparative analysis has reaffirmed the common underlying values and views in regard to information warfare.

Above all, the framing analysis has highlighted the different nuances in the media frames of Estonia and Ireland. While some of the variations can be assumed based on the historical background, such as the more politically motivated character of the Russia-West confrontation frame in Estonian media compared to Irish media, the study was able to reflect upon and compare the main themes in the media coverage of Estonia and Ireland. Therefore, the analysis has interpreted what is prioritised in both countries in relation to information warfare and further facilitated mutual understanding through comparing the differences and similarities. As this kind of analyses support more informed communication between states and societies, it would also be beneficial to

extend the study to involve more states, for example, all EU member states, as interpreting the media frames could point out issues that interstate debates would otherwise miss. Given the importance of mutual understanding in terms of the comprehensive defence of the EU, the research on media frames deserves further investigation.

List of sources

Aasaru, H. (2015). EL-is hakkab tööle Venemaa propagandale vastutegevust arendav üksus. *Err.ee*, 26 August. Available at: https://www.err.ee/544427/el-is-hakkab-toole-venemaa-propagandale-vastutegevust-arendav-uksus [accessed 1 May 2018].

Alexa (2018a). Available at: https://www.alexa.com/about [accessed 25 April 2018].

Alexa (2018b). Available at: https://www.alexa.com/topsites/countries/EE [accessed 25 April 2018].

Alexa (2018c). Available at: https://www.alexa.com/topsites/countries/IE [accessed 25 April 2018].

Allik, S. (2014). Eesti on tegelikult hübriidsõjaks valmistunud. *Postimees.ee*, 25 December. Available at: https://riigikaitse.postimees.ee/3034459/eesti-on-tegelikult-hubriidsojaks-valmistunud [accessed 4 May 2018].

Applebaum, A. (2014). Russia's Information Warriors Are on the March – We Must Respond. *The Telegraph*, 7 March. Available at: https://www.telegraph.co.uk/news/worldnews/europe/russia/10683298/Russias-information-warriors-are-on-the-march-we-must-respond.html [accessed 26 April 2018].

Buchanan, R. A. (2018). The 20th Century. In: *Encyclopædia Britannica*. Available at: https://www.britannica.com/technology/history-of-technology/The-20th-century [accessed 13 April 2018].

Central Statistics Office (2017). Available at: http://www.cso.ie/px/pxeirestat/Statire/SelectVarVal/saveselections.asp [accessed 24 April 2018].

Cluskey, P. (2017). Why hackers may turn their attention to Angela Merkel. *Irishtimes.com*, 22 May. Available at: https://www.irishtimes.com/news/world/europe/why-hackers-may-turn-their-attention-to-angela-merkel-1.3091108 [accessed 8 May 2018].

Connolly-Ahern, C., Broadway, S. C. (2008). "To Booze or Not to Booze?" Newspaper Coverage of Fetal Alcohol Spectrum Disorders. *Science Communication*, Volume 29 (3), pp. 362-385. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1000.7334&rep=rep1&type=pdf [accessed 27 April 2018].

Cooper, C. (2017). What the EU27 wants from Brexit. *Politico.* Available at: https://www.politico.eu/article/what-the-eu27-wants-from-brexit/ [accessed 24 April 2018].

Cottey, A. (2018). *The European Neutrals and NATO: Non-alignment, Partnership, Membership?* London: Palgrave Macmillan.

Davis, J. (2007). Hackers Take Down the Most Wired Country in Europe. *Wired.* Available at: https://www.wired.com/2007/08/ff-estonia/ [accessed 18 May 2018].

De Vreese, C. (2005). News Framing: Theory and Typology. *Information Design Journal*, Volume 13(1), pp. 51-62. Available at: https://www.researchgate.net/publication/250888488_News_Framing_Theory_and_Typology [accessed 23 April 2018].

Department of Foreign Affairs and Trade (2018). Available at: https://www.dfa.ie/our-role-policies/international-priorities/peace-and-security/neutrality/ [accessed 24 April 2018].

Derrig, R. T. (2016). Trump used sophisticated propaganda to win US election. *Irishtimes.com*, 26 December. Available at: https://www.irishtimes.com/opinion/trump-used-sophisticated-propaganda-to-win-us-election-1.2916964 [accessed 6 May 2018].

Dickson, J. (2017). *The Case for Synthesizing Electronic Warfare and Cyber.* Available at: https://www.thecipherbrief.com/the-case-for-synthesizing-electronic-warfare-and-cyber [accessed 8 May 2018].

Donohoe, P. (2018). Ireland must work with other small, open, liberal EU states post Brexit. *The Irish Times*, 8 March. Available at: https://www.irishtimes.com/opinion/ireland-must-work-with-other-small-open-liberal-eu-states-post-brexit-1.3419507 [accessed 24 April 2018].

Doyle, K. (2017). Five years in jail for spreading 'fake news' under FF proposal. *Independent.ie*, 4 December. Available at: https://www.independent.ie/irish-news/politics/five-years-in-jail-for-spreading-fake-news-under-ff-proposal-36375745.html [accessed 6 May 2018].

Edwards, E. (2017a). 'No doubt' Russians tried to undermine US election. *Irishtimes.com*, 14 February. Available at: https://www.irishtimes.com/business/technology/no-doubt-russians-tried-to-undermine-us-election-1.2975897 [accessed 6 May 2018].

Edwards, E. (2017b). Raids on sensitive health data among looming threats, say experts. *Irishtimes.com*, 7 March. Available at: https://www.irishtimes.com/business/technology/raids-on-sensitive-health-data-among-looming-threats-say-experts-1.3001527 [accessed 10 May 2018].

Edwards, E. (2017c). Cyber security experts warned of a hacked world. *Irishtimes.com*, 15 February. Available at: https://www.irishtimes.com/business/technology/cyber-security-experts-warned-of-a-hacked-world-1.2976432 [accessed 10 May 2018].

Ehand, E. (2017). ERR Brüsselis: Venemaa on infosõjas sihikule võtnud ELi väidetava allakäigu. *Err.ee*, 4 December. Available at: https://www.err.ee/646681/err-brusselis-venemaa-on-infosojas-sihikule-votnud-eli-vaidetava-allakaigu [accessed 1 May 2018].

Einmann, A. (2015). Andres Einmann: mure. *Postimees.ee*, 24 March. Available at: https://arvamus.postimees.ee/3133789/andres-einmann-mure [accessed 2 May 2018].

Emmott, R. (2017). Spanish ministers claim Russia interfered in Catalonia separatist vote in a bid to destabilise Spain. *Independent.ie*, 13 November. Available at: https://www.independent.ie/world-news/europe/spanish-ministers-claim-russia-interfered-in-catalonia-separatist-vote-in-a-bid-to-destabilise-spain-36315599.html [accessed 6 May 2018].

Entman, R. M. (1993). Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication,* Volume 43(4), pp. 51-58. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1460-2466.1993.tb01304.x [accessed 20 April 2018].

Entman, R. M., Matthes, J., Pellicano, L. (2009). Nature, Sources and Effects of News Framing. In: K.Wahl-Jorgensen, T. Hanitzsch, eds., *The Handbook of Journalism Studies*, 1st ed. New York: Routledge, pp. 175-191. Available at: https://www.researchgate.net/publication/281755007_Nature_sources_and_effects_of_news_framing [accessed 23 April 2018].

European Commission (2017). Available at: http://europa.eu/rapid/press-release_IP-17-2064_en.htm [accessed 20 May 2018].

European Council (2017). Available at: http://www.consilium.europa.eu/en/press/press-releases/2017/12/11/defence-cooperation-pesco-25-member-states-participating/ [accessed 24 April 2018].

European Union (2018a). Available at: https://europa.eu/european-union/about-eu/countries_en [accessed 24 April 2018].

European Union (2018b). Available at: https://europa.eu/european-union/about-eu/countries/member-countries/ireland_en [accessed 24 April 2018].

European Union (2018c). Available at: https://europa.eu/european-union/about-eu/countries/member-countries/estonia_en [accessed 24 April 2018].

European Union External Action (2017). Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/33119/eu-and-nato-inaugurate-european-centre-excellence-countering-hybrid-threats_en [accessed 19 May 2018].

Eurostat (2018). Available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_access_and_use_statistics_-_households_and_individuals [accessed 19 May 2018].

Evron, G. (2017). Estonia 10 Years Later: Lessons learned from the World's First Internet War. *The Security Ledger.* Available at: https://securityledger.com/2017/04/estonia-10-years-later-lessons-learned-from-the-worlds-first-internet-war/ [accessed 18 May 2018].

Finn, C. (2018). Irish troops to participate in EU Battle Group. *Thejournal.ie*, 6 February. Available at: http://www.thejournal.ie/irish-troops-eu-battle-group-3837647-Feb2018/ [accessed 24 April 2018].

Gamson, W. A., Croteau, D., Hoynes, W., Sasson, T. (1992). Media Images and the Social Construction of Reality. *Annual Review of Sociology*, Volume 18, pp. 373-393. Available at: https://www.jstor.org/stable/pdf/2083459.pdf?refreqid=excelsior%3A4949410ed1ca101ee9fc249008fe07e1 [accessed 22 April 2018].

Gambhir, H. (2016). *The Virtual Caliphate: ISIS's Information Warfare*. Available at: http://www.understandingwar.org/sites/default/files/ISW%20The%20Virtual%20Caliphate%20Gambhir%202016.pdf [accessed 26 April 2018].

Gamzejev, E. (2014). Erik Gamzejev: Eesti võimalused infosõjas. *Err.ee*, 12 March. Available at: https://www.err.ee/509234/erik-gamzejev-eesti-voimalused-infosojas [accessed 2 May 2018].

Ganor, B. (2004). Terrorism as a Strategy of Psychological Warfare. *Journal of Aggression, Maltreatment & Trauma*, Volume 9, pp. 33-43. Available at: https://www.tandfonline.com/doi/abs/10.1300/J146v09n01_03 [accessed 9 May 2018].

Giles, K. (2016). *The Next Phase of Russian Information Warfare*. Available at: https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles [accessed 25 April 2018].

Helme, K. (2014). Andres Jõesaar eestikeelsest propagandakanalist: Kremli infosõda on läinud väga jõuliseks. *Delfi.ee*, 11 November 2014. Available at: http://www.delfi.ee/news/paevauudised/eesti/andres-joesaar-eestikeelsest-propagandakanalist-kremli-infosoda-on-lainud-vaga-jouliseks?id=70129105 [accessed 2 May 2018].

Holden, J. (2015). The war online: how the West is playing catch-up with Islamic State. *Irishtimes.com*, 10 September. Available at: https://www.irishtimes.com/business/technology/the-war-online-how-the-west-is-playing-catch-up-with-islamic-state-1.2345631 [accessed 10 May 2018].

Hutchinson, W. (2006). Information Warfare and Deception. *Informing Science,* Volume 9, pp. 213-223. Available at: http://www.inform.nu/Articles/Vol9/v9p213-223Hutchinson64.pdf [accessed 11 April 2018].

Hõbemägi, P. (2014). Priit Hõbemägi: Kas riik võib valetada? *Delfi.ee*, 8 March. Available at: http://www.delfi.ee/archive/priit-hobemagi-kas-riik-voib-valetada?id=68197047 [accessed 4 May 2018].

Iasiello, E. J. (2017). Russia's Improved Information Operations: From Georgia to Crimea. *Parameters*, Volume 47(2), pp. 51-63. Available at: https://ssi.armywarcollege.edu/pubs/parameters/Issues/Summer_2017/8_Iasiello_RussiasImprovedInformationOperations.pdf [accessed 16 April 2018].

Independent.ie (2015). 'IS group' hacks French TV network. 9 April. Available at: https://www.independent.ie/world-news/is-group-hacks-french-tv-network-31128889.html [accessed 6 May 2018].

Ingram, H. J. (2014). Three Traits of the Islamic State's Information Warfare. *The Rusi Journal*, Volume 159(6), pp. 4-11. Available at: https://www.tandfonline.com/doi/abs/10.1080/03071847.2014.990810 [accessed 17 May 2018].

Irishtimes.com (2017). Obama aides left 'trail of intelligence' on Russian interference. 2 March. Available at: https://www.irishtimes.com/news/world/us/obama-aides-left-trail-of-intelligence-on-russian-interference-1.2995153 [accessed 6 May 2018].

Jaitner, M. (2015). Russian Information Warfare: Lessons from Ukraine. In: K. Geers, ed., *Cyber War in Perspective: Russian Aggression Against Ukraine*, 1st ed. Tallinn: NATO Cyber Defence Centre of Excellence, pp. 87-94. Available at: https://s3.amazonaws.com/academia.edu.documents/45169573/CyberWarinPerspective_Jaitner_10.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1526591595&Signature=dMOt33H2TyV5nvfXzYQoFzNubFs%3D&response-content-disposition=inline%3B%20filename%3DRussian_Information_Warfare_Lessons_from.pdf [accessed 17 May 2018].

Johnson-Cartee, K. S. (2005). *News Narratives and News Framing: Constructing Political Reality.* Lanham: Rowman & Littlefield Publishers, Inc.

Kannel, A. (2015). Ukraina blogipidaja "Välisilmale": Donbassi okupeerimine algas tegelikult juba palju aastaid varem. *Err.ee*, 25 May. Available at: https://www.err.ee/535696/ukraina-blogipidaja-valisilmale-donbassi-okupeerimine-algas-tegelikult-juba-palju-aastaid-varem [accessed 2 May 2018].

Keating, J. (2010). Who was behind the Estonia cyber attacks? *Foreign Policy.* Available at: http://foreignpolicy.com/2010/12/07/who-was-behind-the-estonia-cyber-attacks/ [accessed 18 May 2018].

Kiin, S. (2015). Sirje Kiin: mida teha, kui "tõde ei ole ja kõik on võimalik"? *Postimees.ee*, 7 May. Available at: https://arvamus.postimees.ee/3182245/sirje-kiin-mida-teha-kui-tode-ei-ole-ja-koik-on-voimalik [accessed 4 May 2018].

Kiin, S. (2017). Sirje Kiin: Venemaa infosõda Ameerikas ei lõppenud sugugi presidendivalimistega. *Postimees.ee*, 21 October. Available at: https://arvamus.postimees.ee/4282895/sirje-kiin-venemaa-infosoda-ameerikas-ei-loppenud-sugugi-presidendivalimistega [accessed 1 May 2018].

Knudsen, E. (2014). Media Effects as a Two-Sided Field: Comparing Theories and Research of Framing and Agenda Setting. In: L. Kramp, N. Carpentier, A. Hepp, I. Tomanić Trivundža, H. Nieminen, R. Kunelius, T. Olsson, E. Sundin, R. Kilborn, eds., *Media Practice and Everyday Agency in Europe*, 1st ed. Bremen: Edition Lumière, pp. 207-216. Available at: http://www.researchingcommunication.eu/SUSObook201314.pdf [accessed 23 April 2018].

Kofman, M., Rojansky, M. (2015). A Closer Look at Russia's Hybrid War. *Kennan Cable*, Volume 7. Available at: https://www.files.ethz.ch/isn/190090/5-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf [accessed 18 May 2018].

Kook, U. (2017a). Kaljulaid: ERR-i puhul pole olulised vaatajanumbrid, vaid usaldusväärsus. *Err.ee*, 22 December. Available at: https://www.err.ee/650268/kaljulaid-err-i-puhul-pole-olulised-vaatajanumbrid-vaid-usaldusvaarsus [accessed 2 May 2018].

Kook, U. (2017b). Ratas ja Ossinovski toetavad koostööd PBK-ga. *Err.ee*, 21 December. Available at: https://www.err.ee/650115/ratas-ja-ossinovski-toetavad-koostood-pbk-ga [accessed 2 May 2018].

Kooli, R. (2014). Kolumnist: Venemaa infosõdalaste ükskõiksus tõe suhtes on Lääne pahviks löönud. *Err.ee*, 11 September. Available at: https://www.err.ee/519908/kolumnist-venemaa-infosodalaste-ukskoiksus-toe-suhtes-on-laane-pahviks-loonud [accessed 1 May 2018].

Koort, E. (2014). Erkki Koort: kuidas tõde paistab. *Err.ee*, 28 June. Available at: https://www.err.ee/515451/erkki-koort-kuidas-tode-paistab [accessed 4 May 2018].

Kozloski, R. (2018). *Modern Information Warfare Requires a New Intelligence Discipline*. Available at: https://www.realcleardefense.com/articles/2018/02/20/modern_information_warfare_requires_new_intelligence_discipline_113081.html [accessed 8 May 2018].

Kross, E.-N. (2017). Eerik-Niiles Kross: väide, et PBKsse ostetavate saadete sisu pole Eestile ohtlik, on vale. *Postimees.ee*, 17 December. Available at: https://arvamus.postimees.ee/4347105/eerik-niiles-kross-vaide-et-pbksse-ostetavate-saadete-sisu-pole-eestile-ohtlik-on-vale [accessed 2 May 2018].

Kumar, D. (2006). Media, War, and Propaganda: Strategies of Information Management During the 2003 Iraq War. *Communication and Critical/Cultural Studies,* Volume 3(1), pp. 48-69. Available at: https://www.tandfonline.com/doi/pdf/10.1080/14791420500505650 [accessed 13 April 2018].

Laaneots, A. (2015). Ants Laaneots: Venemaa 2014. aasta uue sõjalise doktriini ülevaade: info- ja psühholoogilistel operatsioonidel on otsustav roll. *Delfi.ee*, 18 January. Available at: http://www.delfi.ee/archive/ants-laaneots-venemaa-2014-aasta-uue-sojalise-doktriini-ulevaade-info-ja-psuhholoogilistel-operatsioonidel-on-otsustav-roll?id=70589551 [accessed 1 May 2018].

Laugen, L. (2015). Soome valitsuses loodi Venemaa infosõja vastane löögigrupp. *Delfi.ee*, 26 April. Available at: http://www.delfi.ee/news/paevauudised/valismaa/soome-valitsuses-loodi-venemaa-infosoja-vastane-loogigrupp?id=71331549 [accessed 2 May 2018].

Laugen, L. (2016). Lätikeelne Sputnik kolis pärast sulgemist uuele aadressile. *Delfi.ee*, 30 March. Available at: http://www.delfi.ee/news/paevauudised/valismaa/latikeelne-sputnik-kolis-parast-sulgemist-uuele-aadressile?id=74091613 [accessed 2 May 2018].

Linström, M., Marais, W. (2012). Qualitative News Frame Analysis: A Methodology. *Communitas*, Volume 17, pp. 21-38. Available at: http://scholar.ufs.ac.za:8080/xmlui/bitstream/handle/11660/3650/comm_v17_n1_a9.pdf?sequence=3&isAllowed=y [accessed 23 April 2018].

Lipton, E., Sanger, D., Shane, S. (2016). How Russian hackers hijacked the US election. *Irishtimes.com*, 14 December. Available at: https://www.irishtimes.com/news/world/us/how-russian-hackers-hijacked-the-us-election-1.2905839 [accessed 6 May 2018].

Longley, R. (2017). *An Introduction to Psychological Warfare*. Available at: https://www.thoughtco.com/psychological-warfare-definition-4151867 [accessed 9 May 2018].

Mackey, R. R. (2017). *Information Warfare.* Available at: http://www.oxfordbibliographies.com/view/document/obo-9780199791279/obo-9780199791279-0024.xml [accessed 11 April 2018].

Martin, A. (2016). Outraged Russia hints at Eurovision boycott over Ukraine's win. *Independent.ie*, 16 May. Available at: https://www.independent.ie/entertainment/music/outraged-russia-hints-at-eurovision-boycott-over-ukraines-win-34717697.html [accessed 8 May 2018].

Masso, I. A. (2015). Iivi Anna Masso: Infosõjast, naabrite sõprusest ja sellest, mida on meil Soomelt õppida. *Delfi.ee*, 6 February. Available at: http://www.delfi.ee/archive/iivi-anna-masso-infosojast-naabrite-soprusest-ja-sellest-mida-on-meil-soomelt-oppida?id=70736909 [accessed 4 May 2018].

Matthes, J., Kohring, M. (2008). The Content Analysis of Media Frames: Toward Improving Reliability and Validity. *Journal of Communication*, Volume 58, pp. 258-278. Available at: https://www.deepdyve.com/lp/wiley/the-content-analysis-of-media-frames-toward-improving-reliability-and-20Zza1hpJK?shortRental=true [accessed 23 April 2018].

McLaughlin, D. (2015). Disbelief in Russia as doping allegations revealed. *Irishtimes.com*, 10 November. Available at: https://www.irishtimes.com/sport/other-sports/disbelief-in-russia-as-doping-allegations-revealed-1.2424194 [accessed 8 May 2018].

McLaughlin, D. (2016). Estonia is in the vanguard of Europe's cyber battlefield. *Irishtimes.com*, 12 July. Available at: https://www.irishtimes.com/news/world/europe/estonia-is-in-the-vanguard-of-europe-s-cyber-battlefield-1.2718351 [accessed 6 May 2018].

McLaughlin, D. (2017a). Ukraine under fire for banning Russian social media. *Irishtimes.com*, 17 May. Available at: https://www.irishtimes.com/news/world/europe/ukraine-under-fire-for-banning-russian-social-media-1.3086397 [accessed 6 May 2018].

McLaughlin, D. (2017b). EU finally waking up to 'hybrid' threat from resurgent Russia. *Irishtimes.com*, 6 July. Available at: https://www.irishtimes.com/news/world/europe/eu-finally-waking-up-to-hybrid-threat-from-resurgent-russia-1.3144376 [accessed 6 May 2018].

McLaughlin, D. (2017c). Baltic Elves confront Russian trolls in growing East-West information war. *Irishtimes.com*, 6 July. Available at: https://www.irishtimes.com/news/world/europe/baltic-elves-confront-russian-trolls-in-growing-east-west-information-war-1.3148634 [accessed 8 May 2018].

Mihkelson, H. (2014). Vallo Toomet: Venemaa töötab infosõjas üldiselt väga efektiivselt. *Postimees.ee*, 11 September. Available at: https://www.postimees.ee/2917273/vallo-toomet-venemaa-tootab-infosojas-uldiselt-vaga-efektiivselt [accessed 4 May 2018].

Mills, C. (2018). *ISIS/Daesh: What Now for the Military Campaign in Iraq and Syria?* Available at: https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-8248 [accessed 16 April 2018].

Ministry of Foreign Affairs (2017a). Available at: http://vm.ee/en/estonia-and-nato [accessed 24 April 2018].

Ministry of Foreign Affairs (2017b). Available at: http://vm.ee/en/newsletter/estonia-supports-actual-use-eu-battle-groups [accessed 24 April 2018].

Minnik, T. (2016). Taavi Minnik: aa-aa-aa-demagoogia*. *Postimees.ee*, 30 May. Available at: https://arvamus.postimees.ee/3710649/taavi-minnik-aa-aa-aa-demagoogia [accessed 2 May 2018].

Misra, A. (2015). What does ISIL/ Daesh actually want? *Informed Comment.* Available at: https://www.juancole.com/2015/11/daesh-actually-want.html [accessed 18 May 2018].

Nael, M. (2014). Mihkelson: Venemaa on üha suurendanud pehme jõu rakendamist. *Err.ee*, 23 September. Available at: https://www.err.ee/520730/mihkelson-venemaa-on-uha-suurendanud-pehme-jou-rakendamist [accessed 2 May 2018].

Nael, M. (2017). Ilves: Venemaa peab asümmeetrilist sõda. *Err.ee*, 31 March. Available at: https://www.err.ee/587393/ilves-venemaa-peab-asummeetrilist-soda [accessed 1 May 2018].

NATO (2018). Available at: https://www.nato.int/cps/ua/natohq/topics_51979.htm# [accessed 24 April 2018].

O'Dwyer, D. (2017a). Extremists are using the internet to proselytise and organise. *Irishtimes.com*, 8 June. Available at: https://www.irishtimes.com/business/technology/extremists-are-using-the-internet-to-proselytise-and-organise-1.3110877 [accessed 10 May 2018].

O'Dwyer, D. (2017b). Audacious ransomware attack signals escalation in cyber-warfare. *Irishtimes.com*, 14 May. Available at: https://www.irishtimes.com/business/technology/audacious-ransomware-attack-signals-escalation-in-cyber-warfare-1.3082743 [accessed 10 May 2018].

OECD (2018). Available at: http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm [accessed 24 April 2018].

OSCE (2018). Available at: https://www.osce.org/participating-states [accessed 24 April 2018].

Pan, Z., Kosicki, G. M. (1993). Framing Analysis: An Approach to News Discourse. *Political Communication*, Volume 10, pp. 55-75. Available at: https://www.scribd.com/document/347860041/PAN-KOSICKI-Framing-Analysis-An-Approach-to-News-Discourse [accessed 22 April 2018].

Postimees.ee (2014a). President: Leedut ohustavaid meediaettevõtteid tuleb karistada. 12 December. Available at: https://maailm.postimees.ee/3024089/president-leedut-ohustavaid-meediaettevotteid-tuleb-karistada [accessed 2 May 2018].

Postimees.ee (2014b). Soome ajakirjanik: Vene infosõdadeks tuleb olla hästi ettevalmistunud. 16 June. Available at: https://maailm.postimees.ee/2829007/soome-ajakirjanik-vene-infosodadeks-tuleb-olla-hasti-ettevalmistunud [accessed 2 May 2018].

Postimees.ee (2015a). Peterburi trollivabrik töötab laohoones ja täpse kella järgi. 17 March. Available at: https://maailm.postimees.ee/3125189/peterburi-trollivabrik-tootab-laohoones-ja-tapse-kella-jargi [accessed 1 May 2018].

Postimees.ee (2015b). Siseminister: ELi eesistumine on suurendanud Läti järele nuhkimist. 26 February. Available at: https://maailm.postimees.ee/3104955/siseminister-eli-eesistumine-on-suurendanud-lati-jarele-nuhkimist [accessed 2 May 2018].

Postimees.ee (2015c). Ajakirjandusvabadus on vähenenud kogu maailmas. 12 February. Available at: https://maailm.postimees.ee/3088821/ajakirjandusvabadus-on-vahenenud-kogu-maailmas [accessed 4 May 2018].

Postimees.ee (2017a). Vene kaitseminister tunnistas esmakordselt teabeväe olemasolu. 22 February. Available at: https://maailm.postimees.ee/4024149/vene-kaitseminister-tunnistas-esmakordselt-teabevae-olemasolu [accessed 1 May 2018].

Postimees.ee (2017b). Inimõiguslased lennutavad põhjakorealastele õhupallide abil informatsiooni. 24 December. Available at:https://maailm.postimees.ee/4354869/inimoiguslased-lennutavad-pohjakorealastele-ohupallide-abil-informatsiooni [accessed 4 May 2018].

Power, J. (2017). State agencies are being ‘proactive’ against cyberattack, says Minister. *Irishtimes.com*, 13 May. Available at: https://www.irishtimes.com/news/world/state-agencies-are-being-proactive-against-cyberattack-says-minister-1.3082398 [accessed 10 May 2018].

Rebane, R. (2016). Raul Rebane: me vajame uut valgust. *Err.ee*, 1 March. Available at: https://kultuur.err.ee/310856/raul-rebane-me-vajame-uut-valgust [accessed 4 May 2018].

Rose, J. W. (2000). *Making Pictures in Our Heads: Government Advertising in Canada.* Westport: Praeger Publishers.

Rosen, A., Kelley, M. B. (2017). If North Korea did hack Sony, it's a watershed moment in cyber-warfare. *Thejournal.ie*, 6 December. Available at: http://www.thejournal.ie/north-korea-sony-hack-cyber-warfare-1816893-Dec2014/ [accessed 10 May 2018].

Ruiz, M. M. (2017). Impacts of Russian Information Operations: Technical and Psychological Aims. *Diplomaatia*, Volume 170. Available at: https://www.diplomaatia.ee/en/article/impacts-of-russian-information-operations-technical-and-psychological-aims/ [accessed 18 May 2018].

Salu, M. (2014). Kuidas käituda infosõjas? *Postimees.ee*, 5 February. Available at: https://leht.postimees.ee/2685922/kuidas-kaituda-infosojas [accessed 2 May 2018].

Scally, D. (2017). Hacking and fake news cast shadows over German election. *Irishtimes.com*, 8 September. Available at: https://www.irishtimes.com/news/world/europe/hacking-and-fake-news-cast-shadows-over-german-election-1.3213276 [accessed 6 May 2018].

Scheufele, D. A. (1999). Framing as a Theory of Media Effects. *Journal of Communication*, Volume 49 (1), pp. 103-122. Available at: http://www.phil-fak.uni-duesseldorf.de/fileadmin/Redaktion/Institute/Sozialwissenschaften/Kommunikations-_und_Medienwissenschaft/Vowe/Forschergruppe/Scheufele_Framing_theory_media_effects.pdf [accessed 22 April 2018].

Schmidt, M., Mazzetti, M., Apuzzo, M. (2017). Trump campaign 'in regular contact' with Russian intelligence. *Irishtimes.com*, 15 February. Available at: https://www.irishtimes.com/news/world/us/trump-campaign-in-regular-contact-with-russian-intelligence-1.2976394 [accessed 6 May 2018].

Shane, S. (2017). Russian intervention in US election was no one off. *Irishtimes.com*, 7 January. Available at: https://www.irishtimes.com/news/world/us/russian-intervention-in-us-election-was-no-one-off-1.2929094 [accessed 6 May 2018].

Shear, M. D. (2017). How Donald Trump lost his love for leaks. *Irishtimes.com*, 16 February. Available at: https://www.irishtimes.com/news/world/us/how-donald-trump-lost-his-love-for-leaks-1.2978266 [accessed 6 May 2018].

Shekhovtsov, A. (2015). The Challenge of Russia's Anti-Western Information Warfare. *Diplomaatia*, Special edition. Available at: https://www.diplomaatia.ee/en/article/the-challenge-of-russias-anti-western-information-warfare/ [accessed 26 April 2018].

Slattery, L. (2017). Why everyone should be worried about cyberattacks. *Irishtimes.com*, 19 May. Available at: https://www.irishtimes.com/business/technology/why-everyone-should-be-worried-about-cyberattacks-1.3088065 [accessed 10 May 2018].

Smith, B. L. (2017). Propaganda. In: *Encyclopædia Britannica*. Available at: https://www.britannica.com/topic/propaganda/The-components-of-propaganda [accessed 11 April 2018].

Smyth, P. (2016). Fake news in US election becomes bad press for Facebook. *Irishtimes.com*, 19 November. Available at: https://www.irishtimes.com/opinion/fake-news-in-us-election-becomes-bad-press-for-facebook-1.2870727 [accessed 10 May 2018].

Smyth, P. (2017a). State's brand of neutrality has become obsolete. *Irishtimes.com*, 8 April. Available at: https://www.irishtimes.com/opinion/state-s-brand-of-neutrality-has-become-obsolete-1.3037655 [accessed 24 April 2018].

Smyth, P. (2017b). EU website takes on Russia's fake news industry. *Irishtimes.com*, 14 September. Available at: https://www.irishtimes.com/news/world/europe/eu-website-takes-on-russia-s-fake-news-industry-1.3219824 [accessed 8 May 2018].

Slaughter, A.-M. (2011). War and law in the 21st century: Adapting to the changing face of conflict. Europe's World, Volume 19. Available at: https://www.princeton.edu/~slaughtr/Articles/Slaughter%20FINAL.pdf [accessed 20 May 2018].

Snegovaya, M. (2015). *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*. Available at: http://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare [accessed 16 April 2018].

Statistics Estonia (2017). Available at: https://www.stat.ee/34278 [accessed 24 April 2018].

Stauber, J. C. (1995). *Toxic Sludge is Good for You: Lies, Damn Lies, and the Public Relations Industry*. Available at: https://www.prwatch.org/books/tsigfy10.html [accessed 11 April 2018].

Szostek, J., Randlo, T. (2015). Joanna Szostek: Putini propagandaga võitlemine võib tuua Lääneriikidele vastupidise tulemuse. *Postimees.ee*, 11 June. Available at: https://

arvamus.postimees.ee/3222157/joanna-szostek-putini-propagandaga-voitlemine-voib-tuua-laaneriikidele-vastupidise-tulemuse [accessed 1 May 2018].

Tagel, L. (2016a). Van Herpen: Moskva ehitab uut impeeriumi. *Postimees.ee*, 23 April. Available at: https://riigikaitse.postimees.ee/3665553/van-herpen-moskva-ehitab-uut-impeeriumi [accessed 1 May 2018].

Tagel, L. (2016b). Marcel H. Van Herpen: Kremli propagandale meeldivad valimised, lääne valimised. *Postimees.ee*, 5 December. Available at: https://arvamus.postimees.ee/3935171/marcel-h-van-herpen-kremli-propagandale-meeldivad-valimised-laane-valimised [accessed 1 May 2018].

Tagel, L. (2016c). Urve Eslas: Kremli valede vulkaani nõlval tuleb propagandale vastu astuda. *Postimees.ee*, 29 June. Available at: https://arvamus.postimees.ee/3747067/urve-eslas-kremli-valede-vulkaani-nolval-tuleb-propagandale-vastu-astuda [accessed 1 May 2018].

Tamkin, E. (2017). 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? *Foreign Policy.* Available at: http://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/ [accessed 18 May 2018].

Thejournal.ie (2014). Germany expels top US spy from Berlin over espionage claims. 10 July. Available at: http://www.thejournal.ie/germany-us-spying-1565069-Jul2014/ [accessed 6 May 2018].

Tonra, B. (2017). Greater military co-operation under Pesco presents range of costs. *Irishtimes.com*, 14 November. Available at: https://www.irishtimes.com/news/ireland/irish-news/greater-military-co-operation-under-pesco-presents-range-of-costs-1.3291783 [accessed 6 May 2018].

Touri, M., Koteyko, N. (2014). Using corpus linguistic software in the extraction of news frames: towards a dynamic process of frame analysis in journalistic texts. *International Journal of Social Research Methodology*, Volume 18(6), pp. 601-616. Available at: https://lra.le.ac.uk/bitstream/2381/31715/3/Touri%26Koteyko_Using%20corpus%20linguistic%20software%20in%20the%20extraction%20of%20news%20frames.pdf [accessed 27 April 2018].

Treufeldt, I. (2014). Maria Aljohhina: Venemaa võimudele mõjuvad ainult karmid majandussanktsioonid. *Err.ee*, 27 March. Available at: https://www.err.ee/510175/tais-mahus-maria-aljohhina-venemaa-voimudele-mojuvad-ainult-karmid-majandussanktsioonid [accessed 2 May 2018].

Tüür, K. (2017). Karmo Tüür: tahtmatu infosõdalane. *Postimees.ee*, 20 November. Available at: https://arvamus.postimees.ee/4316481/karmo-tuur-tahtmatu-infosodalane [accessed 2 May 2018].

Ullah, H. K. (2017). 10 myths about Isis and violent extremists that should keep you up at night. *Irishtimes.com*, 28 November. Available at: https://www.irishtimes.com/culture/books/10-myths-about-isis-and-violent-extremists-that-should-keep-you-up-at-night-1.3307227 [accessed 10 May 2018].

United Nations (2018). Available at: http://www.un.org/en/member-states/ [accessed 24 April 2018].

Van Gorp, B. (2007). The Constructionist Approach to Framing: Bringing Culture Back In. *Journal of Communication*, Volume 57, pp. 60-78. Available at: https://www.unc.edu/~fbaum/teaching/articles/J-Communication-2007-4.pdf [accessed 20 April 2018].

Van Vuuren, R. (2015). *A Futures Model to Address Information Warfare as an Upcoming Wicked Problem*. Available at: https://futuresconference2015.files.wordpress.com/2015/06/rianne-van-vuuren.pdf [accessed 17 April 2018].

Velsker, L. (2017). Ratas kaitseb Vene telekanalit: loomulikult ma annan PBK-le intervjuu. *Postimees.ee*, 20 December. Available at: https://www.postimees.ee/4351059/ratas-kaitseb-vene-telekanalit-loomulikult-ma-annan-pbk-le-intervjuu [accessed 2 May 2018].

Vendil Pallin, C., Westerlund, F. (2009). Russia's War in Georgia: Lessons and Consequences. *Small Wars & Insurgencies*, Volume 20(2), pp. 400-424. Available at: https://www.tandfonline.com/doi/pdf/10.1080/09592310902975539 [accessed 18 May 2018].

Ventre, D. (2016). *Information Warfare.* ISTE Ltd and John Wiley & Sons, Inc.

Weber, M. (2017). Manfred Weber: Eesti rahvas ei ole üksi. *Postimees.ee*, 5 September. Available at: https://arvamus.postimees.ee/4233621/manfred-weber-eesti-rahvas-ei-ole-uksi [accessed 1 May 2018].

White, S. (2018). *Understanding Cyber Warfare: Lessons from the Russia-Georgia War.* Available at: https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf [accessed 16 April 2018].

Wilson, C. (2006). *Information Operations and Cyberwar: Capabilities and Related Policy Issues.* Available at: https://fas.org/irp/crs/RL31787.pdf [accessed 8 May 2018].

Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections: The Quarterly Journal*, Volume 15(2), pp. 73-87. Available at: https://search.proquest.com/openview/4602e5748a89ee4cf9f831f0d03718df/1?pq-origsite=gscholar&cbl=136111 [accessed 17 May 2018].

Zgryziewicz, M. R. (2015). *Daesh Information Campaign and Its Influence.* Available at: https://www.stratcomcoe.org/daesh-information-campaign-and-its-influence [accessed 16 April 2018].

Non-exclusive licence for reproduction of thesis and providing access of thesis to the public

I,
_____
_

(*author's name*)

(personal code _____),

herewith grant the University of Tartu a free permit (non-exclusive licence) to:

_____
_____
_____
_____,

(*title of thesis*)

supervised by _____,

(*supervisor's name)*

1. To reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright.
2. To make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright.
3. I am aware that the rights stated in point 1 also remain with the author.
4. I confirm that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu/Tallinn/Narva/Pärnu/Viljandi, _____ (*date*)

_____ (*signature*)