KU_A4_FARVE

KØBENHAVNS UNIVERSITET

The Great Ukrainian Information War

* A case study of the conflict between Russia and Ukraine in cyberspace

KU_A4_FARVE

Student ID: htw606

Exam Number: XXX

Tegn (inkl. mellemrum): XXX

Tegn i fodnonter (inkl. mellemrum): XXX

Indhold

[1.0 Introduction 3](#_Toc438561299)

[1.1 The approach 4](#_Toc438561300)

[1.2 The structure 4](#_Toc438561301)

[2.0 This is information war 5](#_Toc438561302)

[2.1 Russian military perspective on Information war 5](#_Toc438561303)

[2.2 What does Russian information war look like? 6](#_Toc438561304)

[3.0 What is cyberspace? 8](#_Toc438561305)

[3.1 A brief history 8](#_Toc438561306)

[3.2 Internet as a centerless network 9](#_Toc438561307)

[4.0 Information as a cyber threat 9](#_Toc438561308)

[4.1The theory 9](#_Toc438561309)

[4.2 Fighting against Mordor 10](#_Toc438561310)

[4.3 The nation is at stake 11](#_Toc438561311)

[4.4 Take care of your self 13](#_Toc438561312)

[4.5 Enter the resistance 13](#_Toc438561313)

[4.6 Fight the Kremlin bot 15](#_Toc438561314)

[5.0 A threat with no boundaries, a threat with no end 16](#_Toc438561315)

[5.1 Whom to protect? 16](#_Toc438561316)

[5.2 Are you a real patriot? 17](#_Toc438561317)

[5.3 To secure against whom? 17](#_Toc438561318)

[5.4 For how long? 17](#_Toc438561319)

[5.5 Securitized who? 18](#_Toc438561320)

[6.0 Conclusion 19](#_Toc438561321)

# 1.0 Introduction

The Russian annexation of Crimea in March 2014 has put the entire world in shock. The military move was unexpected by both policy makers and experts in NATO countries and Ukraine (Ozcelik 2015:1). For many, the surprising element was not just Russia’s military intervention. It was the type of warfare itself. Ukraine lost 1/3 of its coastline within just three weeks after Russia mobilized its troops in Crimea. A large part of the population was in favor of the Russian troops, who were on several occasions surrounded by “shields” of supportive civilians. The military takeover of local government building culminated in a highly disputed referendum, in which 97% allegedly voted for a unification with Russia. During this entire operation, there was only one fatal military casualty (Jackson 2014). The success of this offensive was accredited to the use of so called “information warfare”. In this case, mass media was used to portray the Crimean people as being threatened by the fascist takeover in Kiev, the capital of Ukraine (Thornton 2015:40).

General Philip Breedlove, The Supreme Allied Commander in Europe, described Russia’s operation as ‘…the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare’ (Thornton 2015:40). Although a large part of communication in Ukraine and Russia takes place in “old media” like television and radio, an enormous focus has been on cyberspace as well (Van Niekerk 2015: 307).

In Ukraine, politicians, the media and the numerous activists groups are taking the importance of the concept seriously. These volunteer collectives, largely unknown in the west, include *Information Resistance group, InformNapalm*, *Dokaz*, [*Bellingcat's vehicle tracking project*](https://www.bellingcat.com/resources/2015/02/03/ukraine-conflict-vehicle-tracking-launch/) and *Stop Terror*. They have declared themselves as active partakers in the “information struggle” against Russian trolls, propaganda and manipulation in cyberspace. In 2015, Ukrainian *Ministry of Information Policy* initiated a collaboration between activists and authorities by forming the *Ukrainian Information Army* while simultaneously putting a focus on “information war with Russia” in cyberspace (UIA 2015; MIP 2015a).

Despite the enormous public and political attention, there is relatively little academic research about wars in cyberspace and even less about information warfare. The recent conflict between Ukraine and Russia has spurred new interest in the topic, particularly in international, academic journals about democracy and military studies. These publications have focused on the effectiveness, danger and novelty of Russia’s strategies (Pomerantsev 2015; Thornton 2015; Thomas 2014; Cimbala 2014). Ukraine has been portrayed as a passive recipient of Russian aggression at best or neglected entirely.

However, understanding a conflict between opponents requires an investigation of more than one side. I will argue that we can gain new insights about the conflict by focusing on a majorly overlooked aspect of the conflict: Ukraine’s own response to the informational threat. With this goal in mind, the paper will be centered on the following question:

*What practical challenges do Ukrainian authorities face in their attempt to fight an “information war” in cyberspace?*

## 1.1 The approach

The analysis is inspired by Securitization theory, which examines how political and non-political issues are transformed into matters of national security (Wæver et al. 1993; Wæver 1995; Buzan et al. 1998). The purpose of this paper is therefore not to discuss whether information warfare poses a “real” threat or whether malicious information itself should be seen as an act of war. An extensive discussion of this matter can be found in Thomas Rid’s book, *Cyber War will not take place* (Rid 2013)[[1]](#footnote-1).

As I will show in chapter 2 and 5, Both Ukrainian and Russian authorities see information war as an inevitable aspect of warfare today and in the future. Because of this, powerful political and military agents are mobilizing material and symbolic resources to fight the “war”. In this sense, the political and practical consequences of “war” in cyberspace are present, regardless of whether dissemination of information constitutes a threat or and act war “in reality” or not[[2]](#footnote-2).

The main object of the analysis will be the publically available policy of Ukraine’s Ministry of Information Policy as it is stated in official documents, political statements made by the ministry’s officials and the *Ukrainian Information Army*. Will focus entirely on the aspects that are related to cybersecurity.

Cybersecurity deals with threats to internet infrastructure, and threats unfold themselves through the internet. Cybersecurity is a changing phenomenon, where the definitions of threats and the threatened are under constant contestation (Cavlety 2013:105,118). This paper will examine how the scope of Ukrainian cybersecurity broadens. Today it does not only encompass threats likes computer virus and spying tools, but also information warfare: “untruthful” information about Ukraine, Russia and the rest of the world.

Understanding how specific information is framed as a cybersecurity threat is therefore important in order to understand practical challenges the authorities must face in their pursuit of the changing cybersecurity (Cavelty 2013: 105,118; Cavelty & Mauer 2008: 159-160; Cavelty 2007:21).

## 1.2 The structure

This paper will engage with the issues in the following order. Chapter 2 will examine the concept of “information warfare”. Chapter 3 will give a brief review of cyberspace and internet infrastructure. Chapter 4 will analyze how Ukraine’s Ministry of Information Policy transforms “information warfare” into a “cybersecurity” issue through speech acts (Hansen & Nissenbaum 2009:1156). In the final chapter, I will put the transformation in a broader perspective by discussing the ambiguity of “cyberspace”, “information warfare” and the challenge of defining security policy.

# 2.0 This is information war

“Information warfare” can be generally defined as use of information for military purposes. The term has been used as early as 1970’s to describe the spread of propaganda through “old media” long before the proliferation of internet (Minor 1970). Cyber threats and “information warfare” are therefore distinct phenomena that overlap. This paper focuses on this very overlap: Information warfare that takes place in cyberspace.

The specific meaning of the words differ heavily depending on the context (Brazzoli 2007)[[3]](#footnote-3) . For the purpose of this paper, I will examine the concept as it has been understood by Ukrainian authorities and scholars in the context of conflict between Russia and Ukraine. Information warfare consists of psychological operations that attempt to manipulate the mind of people in order to achieve a political or military goal (Boyd-Barrett 2015; Pomerantsev 2015; Thornton 2015; Aliaksandrau 2014; MIP 2015a). Because the Ukrainian authorities see it as their task to protect its population against Russian Information warfare, I will examine the concept as it appears in the Russian military doctrine in the section below.

## 2.1 Russian military perspective on Information war

Rod Thornton gives a very recent account of the way prominent Russian military thinkers and officials perceive information warfare. The dominant view amongst them is that information today plays a primary role in military operations, whereas conventional military forces have a supportive role (Thornton 2015:42; Aliaksandrau 2014:56-57)[[4]](#footnote-4). As the Latvian analyst, Janis Berzins, puts it, we are witnessing a shift from a “…war in the physical environment to a war in the human consciousness and in cyberspace.” (Berzins in Pomerantsev 2015:46). The mind is simultaneously the target and the battlefield. The purpose of this warfare from the perspective of the Russian military is to:

*(…) reduce the necessity for deploying hard military power to the minimum necessary, making the opponent’s military and civil population support the attacker to the detriment of their own government and country.* (Berzins in Thornton 2015:43)

Information is a vehicle of manipulation. It is used to create representations of reality that suit particular political and military purposes (Thornton 2015:42). These “information operations” are to be disseminated not only by the radio and TV, but also through social media (Ibid.:43) by strategically manipulated citizens themselves.

When authorities combine “information operations” with military, political and economic tools, information warfare becomes an element of the so-called “Hybrid war”[[5]](#footnote-5). The main purpose of information warfare here is to “blur” the situation and make the population question 1) who the enemy is and 2) whether they are in a state of war at all (Thornton 2015:41)[[6]](#footnote-6).

## 2.2 What does Russian information war look like?

The purpose of this paper is not to make an essentialist judgement of what is propaganda, “the truth” or whether the narratives correspond to “reality” (Ponamarentsev 2015: 41). However, in order to understand Ukrainian “informational struggle” against “Russian aggression”, it is important to understand the discourses that are commonly labeled in Ukraine as acts of information war. For this purpose, I will use example of “warfare” that have now become common pop culture references in Ukraine.

Shortly before the Russian annexation of Crimea in March 2014, one could find Youtube videos, Facebook posts, tweets and other messages suggesting that neo-Nazis and fascists seized the Ukrainian parliament (Hughes 2014)[[7]](#footnote-7). According to the narrative, the groups were going to Crimea to wreak havoc and punish separatists (Lenta.ru 2014; Ukrainskaya Pravda 2014).

Shortly after the annexation of Crimea, the conflict spread to South Eastern Ukraine, the “Donbass” region. Armed, self-declared separatists began to seize government buildings in April 2014. In the beginning of this military takeover, new reports flourished on social media. A reporter from “Rossiya-24” wrote a story on Facebook about how Ukrainian authorities stopped every single man in trains and busses in order to conscript them into the Ukrainian National Guard (Depo 2014). Bewildered citizens who could not observe such an innovative recruitment practice began their own informational campaign through “memes” by making fun of the absurdity of the message (See picture below).



*Translation: Get of the train, you are now in the National Guard*

This was followed by an interview with an alleged civilian from eastern Ukraine claiming that Ukrainian troops were fighting the war because they were promised two personal slaves as a reward (Web 1)[[8]](#footnote-8). Later, the internet flourished with videos of allegedly Russian actors staging interviews about the atrocities caused by fascist, Ukrainian government. One example is a single woman who allegedly pretended to be 5 different people - simultaneously as a resident in Kyiv, Kharkiv and Odessa - all of whom have witnessed the horror of the Ukrainain fascist government (Crossley 2014).

Another example is an interview with an alleged eyewitness, who described how Ukrainian soldiers tortured and crucified a three-year-old boy to a wooden board before his mother’s eyes, whereafter they tied the mother to a tank and dragged her around a public square. Since no other evidence was found, the Russian journalists behind the interview were accused by Russian and Western journalists for fabricating the story as part of information warfare (Nemtsova 2014; Pomarentsev 2015: 41).

Those civilians who disseminate the “harmful absurdities” are themselves perceived as an important of the enemy’s military machinery. As Myriam Dunn Cavelty and Victor Mauer point out, the information operations “…blur the boundaries civilian and military objectives and systems” (Cavelty & Mauer 2008: 153). Indeed, as mentioned earlier, the very purpose of information warfare is to blur these boundaries.

# 3.0 What is cyberspace?

In order to further understand information war in cyberspace, one must understand “cyberspace” itself.

## 3.1 A brief history

Ever since the words origin in 1982, cyberspace has been conceptualized either as something radically different and independent from the offline world, or as chaotic and unruly space where freedom can unfold (Barlow 1996)[[9]](#footnote-9). As the use of internet proliferated, prominent authors began to emphasize that cyberspace is not a realm that is completely detached from “the real word” (Meyer 2015; Rid 2013: 10,31). Firstly, the internet has penetrated many aspects of our “offline” life. An example that is obvious today, but perhaps not as politicized 1996, is the consequences of cyber identity theft. An intrusion into a person’s bank account through imitation of his credentials will have as real “offline” consequences as an “analogue” money theft. This has led author’s liked David Meyer (2015) to conclude that the term “cyberspace” misleads us to see offline and online lives as separate from each other[[10]](#footnote-10).

The way we conceptualize cyberspace is important for the way we approach cyberspace politically, which is why the discussion is important (Hwang & Levy 2015; Cavelty 2013: 118-119). Although this paper does not seek to discuss which conceptualization of cyberspace is “best”, the differing views highlight the ambiguity and vagueness of “cyberspace”. Because the concept itself is ambiguous, political attempts to identify threats in this “space” become difficult.

However, before one can examine representations of cyber *threats*, it is important to clarify the internet’s technical infrastructure.

## 3.2 Internet as a centerless network

The internet is the result of lead designers, Vint Cerf and Robert Kahn’s, search for a flexible system that 1) can connect different networks together 2) while being able to adapt to extreme circumstances (Naughton 2010). The internet is therefore based on two axioms. Firstly, there is no one to decide who is to use the internet and for what purpose. Secondly, the network itself should not be optimized for specific applications. Until this day it primarily built to do one thing: delivering packets of data from one end to another – indifferent to the origin of the content, or whether it consists of Russian propaganda, pictures of cats or both simultaneously (Ibid.)

The existing literature in cybersecurity highlights that the origin of cyberattacks remain unknown in many cases (REFERENCE). The proliferation of free encryption tools and privacy setting in social media gives anyone the opportunity to either hide ones identity from other users or simply “put on” whichever fictional identity. As I will show in Chapter 4 and 5, the internet’s decentralized nature has significant consequences for information warfare itself.

# 4.0 Information as a cyber threat

In this chapter, I will analyze the practical challenges Ukrainian political authorities face in their attempt to draw information into the realm of national cybersecurity. To do so, I will draw on concepts from Securitization Theory from Copenhagen School of security (Wæver 1995; Buzan et al. 1998).

## 4.1The theory

Securitization Theory examines how politicized or none politicized issues enter the domain of national security. This process is referred to as securitization (Cavelty 2007: 22). Whereas traditional security theory focuses on national states as threats, Copenhagen School has broadened the scope of analysis by examining HIV/AIDS, trafficking and ethnic conflict (Hansen & Nissenbaum 2009: 1158).

Securitization is a process that consists of a series of socially constructed speech acts. This means that there nothing out there that inherently remains a threat at all times independently from those who perceive it. To become a threat an issue has to be successfully presented as such by politically established key actors (Cavelty 2013: 106). By uttering something as a threat to national security, the speaker claims a special right to use any means possible to counter this threat. This way agents can enact security practices through the speech itself (Cavelty 2007: 22; Wæver 1995).

To put in securitization terms, the theory examines how those who securitize (the agents) enact an issue or a group as a threat (the securitized) in order to protect the referent object (the population, the nation, etc.) (Cavelty 2007: 22-23). Throughout the analysis, I will describe securitizing acts by referring to framing. I understand framing as a selection of certain aspects of an issue in order to provoke specific reaction or an understanding of the threat among the audience.

The securitization-inspired approach has been applied to cybersecurity in several studies (Hansen & Nissenbaum 2009, Cavelty 2013; Cavelty 2007). As Myriam Dunn Cavelty argues, there is no inherent link between national security and cyberspace. Elements of cyberspace are actively enacted as threats and become a part of cyber (in)security (Cavelty 2007: 105).

We should therefore see cybersecurity itself as a series of discursive practices that can take different shapes – depending on how cyberspace and the threat is perceived. In the case of this study, discoursive practices refer to use of speech, text, pictures and others vehicles of meaning that represent the threat in a particular way.

As mentioned earlier, what is to be considered as part of cybersecurity is under constant contestation. Different forms of cybersecurity are enabled through different discoursive practices. In their own securitization analysis of cyber space, Lene Hansen and Helen Nissenbaum present three distinct modalities - or so called “grammars” - that specify cybersecurity (Hansen & Nissenbaum 2009:1157).

The first one is *hypersecuritization*, which identifies sudden large-scale (cyber) disaster scenarios such as the total shut down of the power grid due to a hacker attack. Hence the “urgent need” for cybersecurity that can cope with such a disaster (Ibid.:1164).

The second one consists of *everyday security practices* that securitizes citizen’s everyday life experiences. The threat is represented as something ordinary citizens can experience in their own everyday - virus in emails, risk of identity theft and so on. The citizens are therefore called to enact cybersecurity by following particular security precautions (Ibid.:1165).

The third and the last modality consists *of technifications* that portrays an issue as a solely technical matter that depends on expert knowledge and is therefore politically neutral (Ibid.:1166-1168). The way one must handle computer virus, for example, is presented as a matter of following the instructions of computer experts and not something, that should be decided through political debate. In the paragraphs below, I will use these concepts heuristically in order to show how information is transformed into a cyber threat.

## 4.2 Fighting against Mordor

The concept of “information warfare” has not been a high priority on Ukrainian security agenda prior to the conflict in 2014. However, when facing Russia annexation of Crimea in March 2014, political-, military-, national media critics and even the authority figures generally agreed upon a simple yet bleak statement: the country is losing an information war to Russia (Kovac 2015; MIP 2015b).

The Ukrainian government responded to these concerns by establishing the Ministry of Information Policy in 2014 (hereafter abbreviated as MIP). One of MIP’s main, official tasks is to counteract Russian “informational aggression”. One should therefore note, that there are many agents involved in the formation of the “information war” discourse[[11]](#footnote-11). However, it is important to note the ministries role as a securitizer, precisely because the institution itself is born out of the discourse. It is bestowed with government authority (and budget) to ensure the continuation of the information warfare discourse in society at large (MIP 2015b).

As mentioned earlier, the ministry pursues this goal by establishing the “Ukraine information Army”. The picture below is taken from the group’s actual Facebook page and serves as an illustration of its purpose and mobilization of population through dramatic and ironic imagery (UIA 2015b). The goal of the ministry is to mobilize the forces of the internet against mindless orcs from Mordor – recent Ukrainian slang for Kremlin that originates from J.R. Tolkien’s “Lord of the Rings”. The enemy hordes assemble under the banners of propagandist Russian media: Life News, 24 Rossiya and Russia Today. The members of the army are then asked to create fake profiles on Facebook and other social media sites in order to locate false information and fight it by disseminating what they literarily call the “truth” (Lyushnevskaya 2015) As the website states: “Each of your social media messages is a strike to support Ukraine!” (UIA 2015a)



## 4.3 The nation is at stake

How does the ministry then enact representations of a cyber threat so serious that the mobilization of an entire population is called for?

Hansen and Nissenbaum describe how digital threats are hypersecuritized through stories of digital apocalypse. The narratives remind how an entire nation can witness total disruption and even fatal casualties through attacks against critical infrastructure. When talking about this first grammar of securitization, they highlight that such a drastic securitization demands large effort. Since such an attack has never taken place according to them, the hypersecuritization relies on hypothetical what-if scenarios and reminders of a disaster that “inevitably will come” (Hansen & Nissenbaum 2009:1161).

The MIP, however, does not need to rely such a hypothetical threat scenarios. According their own narrative, Ukraine has already witnessed such an attack. Kremlin’s “informational aggression” has caused loss of the Crimean peninsula and the separatist uprising in Donbass region. Entire state sovereignty is now at stake.

The Deputy of MIP, Tatyana Popova’s message to the public through journalist interviews illustrates this point. She states that although “(…) Russian aggression against Ukraine is hybrid, the casualties are real”. In another interview, she emphasizes that: “(…)Even our Western partners see this as the first war that came out of TV” (MIP 2015c). According to her, the internet played an essential role especially after Ukraine banned Russian Television as a counter measure to the “informational aggression” (Ibid.:)[[12]](#footnote-12).

MIP mobilizes the material realities of Ukraine to sustain the discourse[[13]](#footnote-13). The real physical destruction of a virtual threat is portrayed through dramatic imagery in MIP’s poster bellow (MIP 2015d). The headline reads the following in Russian: “Separatism brings instability and destruction”. To the left is the beautiful city of Mariupol in Eastern Ukraine that has been recaptured by Ukrainian Forces in the early phase of the “Antiterrorist Campaign”. To the right is the city of Donetsk, which is still under control of the separatists. The text in the bottom left says: “Protect Mariupol against separatism”. The referent object of this hypersecuritization is not just the state, the Ukrainian army but also innocent civilians – indeed, the very nation itself.



## 4.4 Take care of your self

According to Hansen and Nissenbaum, actors mobilize the lived experiences in order to secure compliance in protecting security and “… to make hypersecuritization scenarios more plausible by linking elements of the disaster scenario to experiences familiar from everyday life” (Hansen & Nissenbaum 2009: 1165). This is refered to as “everyday security practices.”. Seen in this light, MIP’s focus on dangers in social media enacts the general population’s everyday security practices. In its most recent “Information Security project” document, the ministry states that “communicational threats” consist of amongst other elements (MIP 2015a):

*(…) external, negative informational influence on human consciousness and society through means of mass communication, herein the internet, which attempt to damage the government and seek to: alter the psychological and emotional states of a person’s mind*

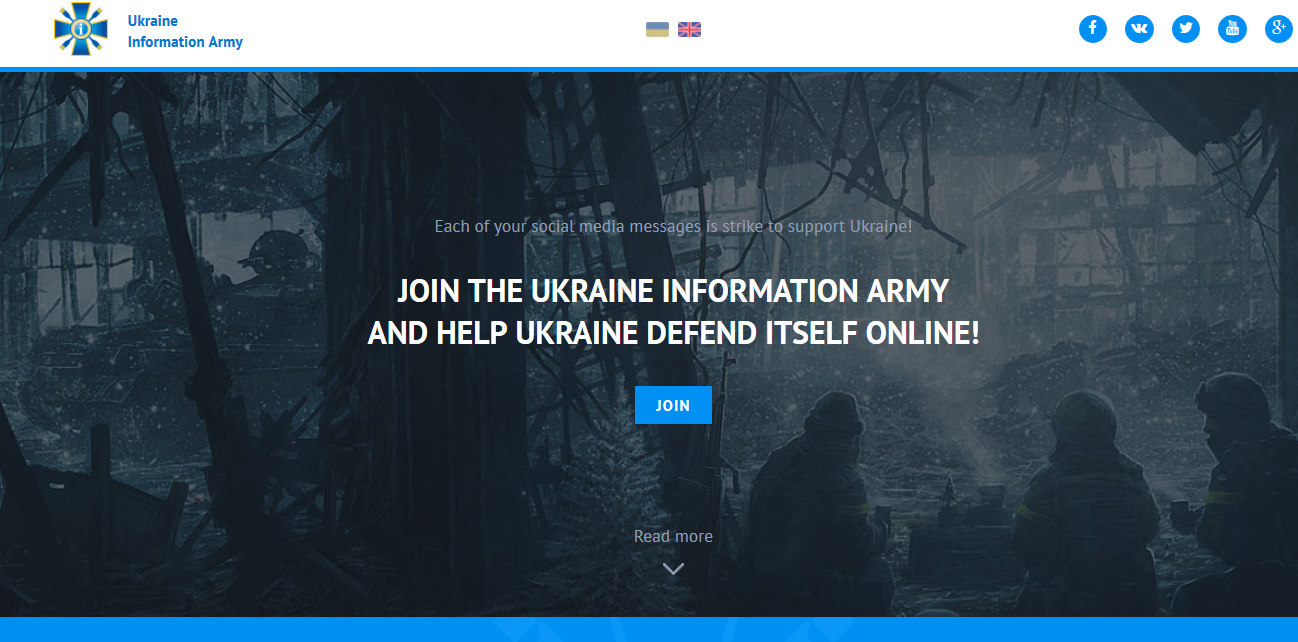
In line with the Russian discourse about information warfare, the Ukrainian authorities portray the mind as the battlefield of modern warfare. Each individual is therefore called to literarily protect his own “self”. The dangers of losing one self to the enemies informational machinery is to be found in videos and comments on Youtube, messages, images, likes and news feed on Facebook. In this sense, the “threat” penetrates a large part of everyday life experience. Those who are in danger are not just the soldiers at the frontline – it is potentially anyone online.

## 4.5 Enter the resistance

As mentioned in section 4.1, the cybersecurity practices described in 2009 followed not only the grammar of *hypersecuritization* and *everyday security practices*, but also *technification* (Hansen & Nissenbaum 2009: 1165). I will argue, that this is true only to some extent in the examined case from 2014-2015.

MIP’s uses some elements of technification by framing information - that has previously been perceived as pro-Kremlin political views - as instrumental acts of military craft. These opinions are not presented as legitimate calls for political action – instead they are framed as a part of a highly calculated military strategy. However, the process of technification constitutes only one of several aspects of the general discourse.

As Hansen and Nissenbaum point out, the grammar of *every day security practices* bestows the individual with responsibility (Ibid.: 1167-1668) In section 4.3 we have seen that every individual is called to take care of the besieged self in times of information war. On the first page of Information Army’s website, as shown in the screenshot below, we are informed that: “…Every Ukrainian with Internet access can make his or her contribution in the information struggle” (UIA 2015a). ” Entering it requires nothing more than typing your email address and any desired name (UIA 2015a)[[14]](#footnote-14).



Indeed, some of the tasks do not require any technical skills other than the ability to manage several accounts on social media. Although there are alleged experts in information war in both Ukraine and abroad, cyberwarfare practice itself has not been presented as something that relies on any particular expertise.

According to MIF’s security project document, the subjects of informational security *should* first of all be: “Citizens of Ukraine, civil associations, civil organizations and other institutions of the civil society” (MIP 2015a). In this sense, MIP does not simply depoliticize cybersecurity by moving it in the domain of “neutral” technical experts. On the contrary, it calls for a massive collective action that encompasses everyone! The struggle against Russian “informational aggression” is perceived as legitimate, political action, whereas dissemination and production of Russia propaganda is presented as military craft, that cannot be approach through mutual dialog. This brings us to the question: what exactly is the securitized cyber threat?

## 4.6 Fight the Kremlin bot

The securitized other may appear as a clearly defined entity at first glance: The Kremlin authorities. I will show that due to ambiguous nature of cyberspace itself, the securitized threat takes multiple forms.

For this purpose, it is relevant to drawn on the notion of “data doubles”. The concept is inspired by the works of Deleuze,and Guattari (1987) and have been revitalized in the context of surveillance studies by Haggerty and Ericson (2000). The term can be useful in this examination because it captures the ambiguity and complexity of online human representations.

Each time we interact online, data is stored about us in governmental and commercial databases. These chunks of information constitute data doubles of ourselves (Haggerty & Ericson 2000: 613)[[15]](#footnote-15). They capture a part of our behavior or preferences – represented in an analyzable format – without capturing our persona in its entirety. As Poster puts it, the new “body” is “…*a double which involves ‘the multiplication of the individual, the constitution of an additional self’* (Poster 1990: 97).

In the case of MIP, the threat is presented as a network of individuals and machines that manipulate people. In a phenomenological sense, these anonymous “persona” appear not as real *individuals* of flesh and blood, but as data doubles in the shape of profile pictures, videos, texts and sounds. Because we do not see these *people* in front us, we cannot be sure of their identity or physical location. The person posting “unpatriotic” images about Ukrainian fascists on Facebook as an “eyewitness” can be an actual person’s experiences. But it could also be a message from an intelligence officer in Saint Petersburg or another manifestation of information warfare. This uncertainty manifests itself in two discoursive concepts that have entered both Ukrainian and Western mainstream culture in general.

The first is the Russian troll. A troll is internet jargon for someone who takes numerous identities in order to provoke a strong reaction from the audience for his own pleasure. One of the goals is to ruin the reputation of the target individual or organization (Coleman 2014: 4,19) Investigative journalists and CNN suggested that Russian government hires people full time in so called “Troll farms” in order to spread pro-Kremlin views. According to this widespread discourse, these Russian trolls pretend to be several different people by posting things like “Ukrainians are fascists” as comments to Youtube videos, new articles etc. Data-doubles themselves are allegedly doubled by the “Troll Farms” in an infinitely expanding number in order to fill each corner of the internet with “lies” – multiplying the threat to Ukrainian sovereignty (Pomerantsev 2015:45).

The second discoursive representation of the threat is the Kremlin bot (Pomerantsev 2015:45). The word “bot” refers to a program that does automated tasks on the internet. Kremlin bots are alleged automated accounts on social media, such as twitter that spread pro Kremlin information. They pretend to by using Russian, Ukrainian or even American names, retweeting and befriending each other on Facebook in order to appear more human (Alexander 2015). As data-doubles, Kremlin bots are not just constantly multiplying the representations of each other. They are literarily nothing more than chunks of computer code with no real human behind – other than the operator of the expanding bot network. A kremlin bot is a mask with no face behind[[16]](#footnote-16).

# 5.0 A threat with no boundaries, a threat with no end

When Hansen and Nissenbaum described hypersecuritization in 2009, they had focused on “classical” cyber threats against computer infrastructure through malicious code: virus, worms or spying tools. The Ukrainian case shows us that the range of perceived threats in cyberspace is becoming more diverse and wide-ranging. The referent object is no longer threatened by hacking tools and computer code but now also Kremlin bots, Russian trolls, general sympathies towards Kremlin, alleged (mis)information about the Ukrainian state, war events and eventually calls for separatism itself.

## 5.1 Whom to protect?

Because internet’s decentralized nature (Naughton 2010; Barlow 1996) does not allow an easy verification of whether someone is a Kremlin bot or a Russian Troll, anyone with “unpatriotic views” online can be deemed a manipulating troll or a bot. As a representation of the Kremlin cyber threat, a Russian troll or a Kremlin bot is potentially anyone online who you do not know. This makes any efforts to delimitate the referent object – those “in need of protection” - very difficult.

Because of this lack of boundaries, the referent object category becomes unstable. Since the threat takes place in the ambiguous, borderless cyberspace, the battlefield is not just limited to Ukraine, but social sites and webpages where Kremlin bots and Russian trolls may appear[[17]](#footnote-17). Those to be “defended” are not just victims of information war, who perceive the Ukrainian government as fascist. The goal is also to police the “sane patriots” and “adequate” foreign audiences whose minds can potentially be targeted by the omnipresent phantom enemy. MIP’s policies target *all of us*.

## 5.2 Are you a real patriot?

Even when the identity of the person, the same sense of cyber insecurity towards “antipatriotic” flux of information can be applied offline. Indeed, that the very idea of “we” or “patriots” itself is not a stable category. It is the object of constant political contestation.

In war time Ukraine it is not uncommon that self proclaimed patriots - journalists politicians, and even Ukrainian war veterans – are labeled as intentional or unintentional accomplices of Kremlin (Sprotiv 2015). Accusing other “patriots” of corruption or inefficiency involves the risk of being portrayed as someone who drives a wedge between patriots in times of crisis. This is the label which, for instance, the Ukrainian MP, “Semyon Semyonchenko” used to describe journalistic investigations that suggests his lack of efficiency as a political and military leader. What previously might be seen as political critique can now be framed as “information warfare”.

Following the ambiguous logic of information war, MIP’s failed attempts to win on the information war can be potentially framed as an unpatriotic attempt to sabotage the national war effort. Indeed, the government’s inefficiency in fighting the war is often described as “zrada”, treason.

## 5.3 To secure against whom?

It is important, that defining the referent object is not the only challenge the authorities face. Not only does MIP frame the entire – undefined – population as being threatened, it is also calls *everyone* to police the cyberspace against the threat. I will argue that the lack of boundaries is itself a component of the grammar of information warfare. Because the battlespace is the mind online, the problem of (cyber)security cannot be “solved” by single authority alone. It has to involve the minds of the populace. Yet if “everyone” is to police the cyberspace, it becomes unclear, who exactly is to target in campaigns that promote direct citizen action. Every civilian is supposed to be part of the war efforts, yet simultaneously no one particular. This lack of delimitation brings us to the next question.

## 5.4 For how long?

Because there is no clear boundary between civilians and military in the discoursive space of information war, the boundary between war and peace itself cease to exist (Cavelty & Mauer 2008: 153). If MIP frames the minds of the citizens as being under constant threat, then there can be no final informational victory. This leaves MIP with few substantial means of evaluating the effectiveness of its “war efforts”. Empirical examination of MIP’s strategy documents suggests that this is indeed so. Here, one does not find any criteria for an informational victory. As Mauer and Cavelty put it, the informational operations themselves become permanent (Ibid.)

## 5.5 Securitized who?

Although the line of thinking in this paper is inspired by the securitization theory, the concluding remarks point towards a different direction. In most of the existing securitization studies we see a relatively well defined securitized other: be it the State, HIV or Al Qaeda (Hansen & Nissenbaum: 1158). The paper points out that making a clear definition of the securitized is extremely difficult in the context of information war. The Securitization theory in its original form does not encompass this ambiguity due to its a priori assumption about the relatively delimited nature of the securitized. By putting this assumption on hold, one can encompass challenges of war that might otherwise be left unnoticed.

By doing so, we see that MIP is facing the challenge of fighting a war everywhere in cyberspace at all times by mobilizing everyone against potentially anyone. As mentioned in chapter 2, the very purpose of information war is to blur boundaries between war, peace, civilians and none civilians. This is both the alleged strength of the warfare, yet also its Achilles’ heel. No one is definitely safe from being securitized as a Kremlin threat, not even the securitizers themselves.

Due to practical challenges of delimitation, it becomes difficult to make concrete policy with objectives that target a clearly defined segment of the population.

# 6.0 Conclusion

In this paper, I have shown that the Ukrainian state is transforming information about the recent war events, the Ukrainian nation and the west into a cybersecurity issue. By seeing cybersecurity as a series of discoursive practices through the lenses of Securitization theory, particular challenges of policing cyberspace appear.

The Ukrainian Ministry of Information policy has framed the loss of Crimea as the result of Russian informational aggression. An attack that can potentially threaten the entire state sovereignty. Because the ministry relates this threat to the general population’s everyday security practices, it faces the practical challenge of delimiting the range of the threat. In the context of the decentralized cyberspace, the risk of being manipulated is presented as something omnipresent. It lurks in any part of cyberspace where Ukraine is discussed or (mis)represented.

Since the battlespace of the information war is presented as the mind itself, anyone is potentially in danger of being manipulated by Kremlin. The authorities face a colossal challenge of delimiting the referent object. The question “who is to protect?” remains without a clear answer.

Because of these factors, defining the securitized threat itself becomes increasingly difficult. Despite the fact that the Russian government is portrayed unambiguously as the aggressor behind the informational war, the cyber-attacks manifest themselves in an omnipresent, phantom-like manner. Anyone online could be intentionally or unintentionally a part of the enemy’s war machinery, even the Ukrainian authorities that are supposed to fight the threat. The authorities not only facing the challenges of defining policy – who is to fight what, where and how – but are also facing the danger of themselves becoming “threats” in unstable discourse of “information war”.

1. Rid concludes that information is neither a “weapon” nor can it be a real act of war (Rid 2013:37). [↑](#footnote-ref-1)
2. The main assumption behind this paper is that different ways of conceptualizing and talking about a threat matters. Different understandings of security can lead do different answers to the question of what is the threat and what are the legitimate ways of fighting it. These answers can themselves lead to different cybersecurity practices and therefore challenges. [↑](#footnote-ref-2)
3. Information warfare can been as something that 1) targets computer networks 2) resides within the electromagnetic spectrum and includes jamming and intercepting signals or consists of 3) psychological operations that target the minds of the target audience (Brazzoli 2007). [↑](#footnote-ref-3)
4. For example, the military can cause panic in the population by holding military exercises close to the border or by taking over public administration buildings in the middle of civilian protests in the same place. [↑](#footnote-ref-4)
5. Both the notion of Hybrid war and Information war as an element in the “hybrid” mix has proliferated heavily in the last few years in both Ukraine and Russia. [↑](#footnote-ref-5)
6. From the perspective of the Russian government and military thinkers, the recent antigovernment protests, or the so called “color revolutions” in the “near abroad” Ukraine, Georgia, Kyrgyzstan and Belarus, are example of USA’s use of information warfare against Russia. They are not caused by the population’s agency or democratic choice. Rather, they are the result of USA’s ideological pressure on the people’s mind. The alleged goal of this information war is to weaken Russia’s position in the region and eventually create a regime change in Russia itself that is favorable to the interest of USA’s military. [↑](#footnote-ref-6)
7. *“Neo-nazi mainly refers to what was then a paramilitary group, “Right Sector”.* [↑](#footnote-ref-7)
8. This became an instant internet meme amongst Ukrainian civilians and soldiers who were “disappointed” by their lack of reward. [↑](#footnote-ref-8)
9. The first of the word in the Anglophone world appeared in sci-fi author, William Gibson’s short story, Burning Chrome in 1982. Later it appeared in his novel, *Neuromancer* (Gibson 1984:67). Cyberspace is portrayed as something global, fascinating, mysterious and yet difficult to grasp. [↑](#footnote-ref-9)
10. . Because of this unclarity, the term cyberspace should be abandoned altogether (Ibid.). [↑](#footnote-ref-10)
11. An example of different agents behind the discourse are the following: Ukraine’s ministry of defense, journalists, non-governmental think tanks, western university institutions, NATO’s reports, Russian military experts and many more. [↑](#footnote-ref-11)
12. According to an advisor to MIP, Sergey Konstinskiy, the conflict shows that “words kill” (<http://mip.gov.ua/ru/news/433.html>). [↑](#footnote-ref-12)
13. . According to the highly cited UN reports, the war has caused nearly 8,000 death and 18,000 injured. 1.5 million civilians have fled the warzone and remain internally displaced in Ukraine until this day [↑](#footnote-ref-13)
14. The initiative should been seen in the context of numerous informal volunteer collectives “resisting Russia” which have been active prior to any government legislation in this matter. [↑](#footnote-ref-14)
15. Often without our knowledge of their existence. [↑](#footnote-ref-15)
16. Although propaganda in itself is not new, information warfare in cyberspace means that the threat can be disseminated on social media almost instantly through an enormously complex global network of human and none humans nodes. In this sense, information warfare with bots and trolls in cyberspace is distinct from mere propaganda on TV, radio or newspapers. [↑](#footnote-ref-16)
17. Psychological mobilization against Ukraine can take place on comment boards on The Guardian’s website, in the English speaking online channel, Russia Today, or even Chinese forums. [↑](#footnote-ref-17)