Sign Systems Studies 47(1/2), 2019, 126–151

Semiotics of threats: Discourse on the vulnerability of the Estonian identity card

Andreas Ventsel

Department of Semiotics
University of Tartu
Jakobi 2, 51005 Tartu, Estonia
e-mail: andreas.ventsel@ut.ee

Mari-Liis Madisson

Department of Semiotics
University of Tartu
Jakobi 2, 51005 Tartu, Estonia
e-mail: ml.madisson@ut.ee

Abstract. This article analyses various e-threats that were expressed in media texts that focused on e-threat discourses concerning the Estonian identity card's security risk in 2017. The discourse of cyberthreats contains strong and controversial meanings because the peculiarities of cyberspace remain intangible for average readers who do not possess expert knowledge regarding ICT. The wider aim of the paper is to suggest how the topic of e-threats could be given public coverage without fuelling irrational anxiety and unwarranted threat scenarios. Our theoretical basis combines the frameworks of the Copenhagen School of security studies and ideas of cultural semiotics. We explain the semiotic logic of phobophobia (i.e. the abstract concern with the devastating impacts of the collective feeling of fear) and the discourse of fear that is characterized by a significant reliance on analogies, drawing vague demarcation line between reference objects and the dominance of negative emotional tonality. Our study demonstrates that the main actors of threat and the consequences of the identity card's security problems were associated with unknown hackers and the damaging of the reputation of Estonia as an e-state.

Keywords: e-threats; cultural semiotics; phobophobia; securitization; security risk; semiotics of fear

https://doi.org/10.12697/SSS.2019.47.1-2.05

Introduction

The article focusses on the media coverage of the theoretical vulnerability of Estonian identity cards that was discovered in autumn 2017. The coverage painted the hitherto overwhelmingly positive image of the Estonian e-state in much darker colours and envisioned several imminent e-threats. Since the beginning of the 1990s, discourse on smart e-solutions in education, medicine and state government has become commonplace; many researchers have pointed out that the digital success story has become a cornerstone of the brand of Estonia as a nation (Jansen 2008; 2012; Kulcsár, Yum 2012: 198; Madisson 2016; Tammpuu, Masso 2018). In collaboration with marketing agencies, dozens of Estonia's top politicians and experts – or, in other words, spokespersons of e-Estonia – have been systematically spreading and creating messages that promote Estonia's image as a digital state, both for domestic and foreign audiences.[1] This image of Estonia was perhaps one of the main reasons for the emergence of a heated public debate around the unsuccessful communication strategies deployed to inform the public about the identity card vulnerability. A common position taken was that the coverage of the vulnerability had created an irrational panic that, on the one hand, undermined citizens' positive outlook on the e-state and, on the other hand, enabled hostile forces to keep detailed track of the vulnerabilities of Estonia's digital infrastructure – and consequently, to undermine the Estonian state's security and/or positive image. The discourse surrounding the vulnerability of the identity card provides semiotics with fascinating research material, since there is a collision of positive self-descriptions and expressions of several fears related to the digital state.

One purpose of the article is to explicate the discourse of e-threats. An aspect of this discourse is phobophobia – fear of the fear itself, unleashed in society by the identity card vulnerability. Several academic works have pointed out that the object-level complexity and vague boundaries of information and communications technology (ICT) tend to get transferred to meta-level analyses (for example, to expert opinions). The latter, then, consider a general culture of fear accompanying the developments of information technology, without, however, explicating the culture's specific elements and their interrelations (Sandywell 2006; Hansen,

[1] From 2017 onwards, such image design is being coordinated by the communication agency Callisto Group; a detailed description of their main messages and a list of spokespersons can be found in the document "e-Eesti rahvusvahelise maine edendamise ajakohastatud tegevuskava aastateks 2018–2019" ["Plan for the promotion of Estonia's international reputation for the years 2018–2019"]; https://www.ria.ee/sites/default/files/content-editors/ITT/e-eesti_rahvusvahelise_maine_edendamise_tegevuskava_2018-2019.pdf.

Nissenbaum 2009; Jarvis *et al*. 2016). Our article has two main aims. Firstly, it analyses media texts that explicitly refer to phobophobia, or in other words, express concerns over the sense of fear prevalent in society and its potential effects on the decision-making process of individuals. The second purpose is to articulate the semiotic mechanisms underlying the discourses of e-threats and fears.

The first part of the article develops a theoretical framework, using the framework of securitization developed by the Copenhagen School. These scholars of international relations underline the social aspects of security. According to the framework of securitization, constructing an e-threat is a discursive act that constitutes at least one referent object, envisioned as being under threat and thus in need of urgent protection (Hansen, Nissenbaum 2009: 1156; Barnard-Wills, Ashenden 2012: 114). The referent object can be a state or a nation, but it can also belong to the private sector, for example, banking or transport. The second part of the article presents a textual analysis detailing the ways of constructing e-threats in the media coverage of the security vulnerability of the Estonian identity card. The third part explains the semiotic mechanisms of phobophobia and discourse of fear; here, we mainly rely on Mihhail Lotman's ideas on the semiotics of fear and Juri Lotman's framework of discrete and non-discrete logic of signification.

We analysed 40 articles published on Estonian news sites (Postimees.ee, Delfi.ee, err.ee, Geenius.ee) from September 2017 to September 2018. Postimees.ee and Delfi.ee are the most viewed news sites in Estonia; err.ee is the official site of the Estonian National Broadcasting. Geenius.ee was included in the sample because the site largely concentrates on digital and electronic technology; furthermore, the articles published in Geenius.ee are often reported in major Estonian newspapers. All the analysed articles explicitly referred to the vulnerability of the identity card.

1. Phobophobia and the semiotics of fear

Contemporary risks are more and more related to cyberspace and ICTs: data security, hacking, defence of digital infrastructure, personal (smart) technology, biased strategic communication, and troubling phenomena of social media such as the viral dispersion of fake news and information overload. Perception of e-threats and especially of risks related to social media has become solidified after Donald Trump's election victory and the Brexit vote; disinformation campaigns and echo chambers are constant talking points, a sense of anxiety prevails over algorithms' potential negative effect in shaping public opinion. It is feared that people's beliefs and opinions are algorithmically predictable and perhaps even formable by big data analysis programs (Harsin 2015). It is increasingly believed that those with

most power are those able to align their strategic messages with big data analysis – as was done, for example, by Cambridge Analytica.

The atmosphere of fear accompanying a sense of ignorance and distrust is explainable by the concept of phobophobia, which has been studied by Mari-Liis Madisson in the context of sociocultural meanings of contemporary ICTs. According to Madisson, the core of phobophobia – or in other words, a certain meta-level fear – lies in the concern with the dangerous effects of a collective sense of fear and helplessness. Phobophobia is based on the understanding that society has been gripped by a wave of fear that inhibits any capacity for rational analysis and renders people short-sighted and easily manipulable (Madisson 2016: 19). In the context of an atmosphere of fear it is common for people to start searching for scapegoats and act based on instinct rather than reason. The possibility of the emergence of conspiracy theories is one of the fears arising from such a context. The presupposition that it is possible to exploit the chaotic sense of fear and anxiety affecting the masses is a crucial component of meta-level fears. Phobophobia is often supported by the apprehension that powerful positions will be seized by those who have managed to stay out of sight in ordinary democratic deliberation.

Discussing discourses of fear, it is important to differentiate between fright and fear. The former signifies an immediate reaction to events that have already taken place, the latter, however, entails anticipation of future events and presupposes both the expectation of danger as well as interpretation of signs in a foreboding key (M. Lotman 2009a: 209). The temporal distance between experience and interpretation ensures a smooth run for mechanisms of signification (M. Lotman 2009a: 210). As opposed to fright, fear operates as a frame for interpreting everyday events. The American sociologist David Altheide (2002: 59) calls this aspect the 'discourse of fear' or 'non-parallel fear' in which fear has become dominant and been turned into a context influencing the interpretation of singular events and phenomena. The fear of such a fear that has overcome society has been termed phobophobia in this article. From a semiotic perspective, the discourse of fear manifests itself in the contingency and arbitrariness of threats and in their future-oriented nature; concrete threats are seldom expressed. The discourse of fear is characterized by vagueness and indeterminacy of reference. The atmosphere of fear itself is an important context for the risks articulated in phobophobic discourse.

2. Discourse of e-threats and securitization

This article regards cyberthreats first and foremost as discursive phenomena. According to the Copenhagen School, securitization is a discursive act with a specific rhetorical structure and political effect, an act that represents referent objects as existentially threatened; consequently, a successful securitizer can persuade his or her audience to take measures unthinkable outside the emergency situation (Buzan *et al.* 1998: 5). In studying securitization, it is important to analyse when a discourse with a specific semiotic structure attains enough power to persuade the public to break the rules in a way previously considered unacceptable (Buzan *et al.* 1998: 25).

Studying the discursive construction of cyberthreats does not amount to saying that these threats are insignificant or that they do not actually exist. We are interested in those processes through which something becomes publicly perceptible and acceptable as a cyberthreat. A strong reaction to certain threats (for example, strict control of internet use in the case of cyberterrorism) may bring about serious problems in other domains (limitation of free speech and mass surveillance). Risks and the accompanying threat scenarios are largely constructed through meanings that they have in specific contexts for researchers, stakeholders and interest groups (Grint 2010; Head, Alford 2015).

The emergence of an atmosphere of fear plays a significant role in the construction of threat discourses. This atmosphere enables the public to interact emotionally with certain topics and thus to attract more attention in the media. Mediating fear presupposes determining the causes of fear. According to Mihhail Lotman it is important to recognize in the articulation of social fears that the semiosis of fear is oriented towards finding expressive signs suitable for communicating a subjective sense of fear. This is the reason why the significational mechanisms of fear are indeterminate and ambiguous by nature (M. Lotman 2009b: 1239). This is exactly why it is important to analyse how a discourse of fear constructs relations between different referent objects and thus contributes to its coherence.

Securitization occurs when objects under threat are constructed and different domains needing protection are weaved into a whole (Hansen, Nissenbaum 2009: 1163). Hansen and Nissenbaum (2009: 1157) name three modalities of securitization: (1) everyday security practices that draw on everyday experiences and securitize the latter through constructing possible scenarios; (2) technification: the discourse of threat and possible solutions to problems are constituted as necessitating technical expert knowledge; and (3) hyper-securitization, the construction of large-scale instantaneous cascading disaster scenarios that

place a long list of grave threats into an immense chain – while none of those threat scenarios have taken place as yet. Although fear has a role to play in the construction of each modality, hyper-securitization is the most likely trigger of a discourse of fear and of constructing chains of indeterminate connections (Ventsel, Madisson 2018; Ventsel *et al.* 2019).

3. Analysis: Representation of e-threats in the media coverage of Estonian identity card vulnerability

The discussion dealing with the media coverage of the vulnerability of the Estonian identity card will, firstly, map the referent objects represented as being in need of protection. Secondly, we analyse four interrelated categories: representation of the social actors connected to e-threats and their activity–passivity; the articulation of the acuteness of e-threats; the construction of an emotional context for e-threats; and the description of potential counter-measures (to be) taken in order to solve the problems facing the referent objects. These categories are based on the observations of authors (van Leeuwen, Hansen, Nissenbaum, Bednarek, Caple) dealing with discourses of threat; the categories provide us with a systematic perspective on the analysed material. Let us start with a brief overview of the chronology of events.

3.1. Chronology of the case

At the beginning of September 2017, the Estonian public was notified that the almost 760 000 identity cards of the new type (that is, issued from October 2014 until October 2017), produced by Gemalto, have been identified as having a theoretical vulnerability in their software. On 3 November, CERT-EE, an institution operating under the Information System Authority [*Riigi Infosüsteemi Amet*, RIA], issued a warning of potential phishing e-mails. Such e-mails were associated with potential spreading of malware and identity theft.[2] From the evening of 3 November, the Estonian government decided to suspend all certificates of identity cards with the vulnerability. The Police and Border Guard Board [*Politsei- ja Piirivalveamet*, PPA] offices were open, from 3 November to 5 November, outside working hours in order to provide intensive users – those who actively use the PIN1 and PIN2 codes – with the possibility to update their certificates. During these three days, remote updating of certificates was disabled.

[2] Full text of the warning can be found here: https://twitter.com/CERT_EE/status/926475950883328000.

Priority was given to doctors, legal workers and employees of the Vital Statistics Department (Jõevere, Helme 2017). After 5 November, remote updating of certificates was restored until 31 March 31, 2018. It transpired, however, that 18 000 people could not update their certificates remotely (Krjukov 2017). Extensive media coverage of the identity card vulnerability ensured a numerous turnout to the PPA offices of even those people who used identity cards' electronic applications infrequently (Saar 2017). The end of November 2017 witnessed a marked media escalation of the topic. At that time, a dispute broke out between Gemalto and the PPA. Gemalto's representatives claimed that they had notified the PPA of the vulnerability already in the summer and that the latter had simply covered it up until September (Pau 2017a).

3.2. Mapping referent objects

In the analysis of the threat discourses regarding the identity card vulnerability, we were able to delineate three principal domains of referent objects represented as directly threatened. The first domain was related to *national security* – the suspension of identity cards' certificates impeded information exchange between citizens and the state. These threats were not perceived as overly dangerous; it was stressed that any potential hacking and exploitation of personal data would be too time-consuming and expensive: it would require a separate hacking of each individual account.

> In the future, any code is hackable; the question is, however, if and for whom is it is feasible to splash a million Euros in order to access a pensioner's bank account or steal a vote from the Minister of Social Affairs in order to support the Reform Party?[3] [...] [H]acking of one card would cost 80,000 Euros. (Kund, Pau 2017)

The potential manipulation of e-voting was seen as the principal referent object in need of securitization. It was parliamentary politicians and not digital experts, who would argue that Estonian democracy would come under threat because of manipulations to free elections. This is the reason why this particular threat discourse should be viewed in the context of the political struggle accompanying the 2017 local elections which took place in October. A heated debate ensued among politicians over the security of e-voting; cancelling the e-vote was repeatedly put on the table for security reasons. The Conservative People's Party of Estonia (*Eesti Konservatiivne Rahvaerakond*, EKRE) and the Estonian Centre

[3] In 2017, the Reform Party (then in the opposition) was critical of the rise in excise tax put on alcohol, a rise initiated by the Minister of Social Affaris Jevgeni Ossinovski from the Social Democratic Party.

Party (*Eesti Keskerakond*) were the principal opponents of the e-vote; they had been sceptical of electronic voting even earlier. According to Mart Helme, the chairman of the EKRE faction in *Riigikogu* [Parliament], their party had come to the conclusion that the vulnerability of the identity card had created a risk of manipulation of votes and thus influencing election results.

> According to legal practice, it is enough that there exists a possibility of the violation of rights, any actual violation need not take place. In cancelling the e-vote, the probability of exploitation of the vulnerability does not matter, since it cannot be predicted by anyone. (Reisenbuk 2017)

Jaanus Karilaid, Vice Chairman of the Centre Party, pointed to similar threats looming over the e-vote: "Democracy cannot have any vulnerabilities." He then recommended that the election commission should, in coordination with experts, seriously consider whether it is appropriate to go forward with the e-vote in light of the vulnerability. "The Centre Party has always stressed that e-voting should be secure and transparent," said Karilaid (Kund, Pau 2017).

Parties previously favourably disposed towards e-voting – the Estonian Reform Party [*Eesti Reformierakond*] and the Pro Patria and Res Publica Union [*Isamaa ja Res Publica Liit,* IRL][4] – did not change their position and expressed their support for the e-vote even after the disclosure of the vulnerability. "It is low to connect this [vulnerability of Estonian ID-card] to the general debate over the reliability of e-voting, as does Mart Helme, using a spiteful rhetoric in hindsight," said Urmas Reinsalu, the Minister of the Interior from the IRL (Olup 2017). Politicians' statements were largely characterized either by accusing the opponents in escalating fears or by connecting the identity card vulnerability with the other (Centre and Conservative People's) parties' previous condemnatory positions towards e-voting that were legitimized by the current situation.

The second domain of referent objects was the *private sector*. Here, the main theme was the potential disturbance in banking and electronic trade. In a flash interview to Postimees, Tanel Tammet, Professor of the School of Information Technologies at the Tallinn University of Technology, said: "I would personally say that e-commerce and, because of this, internet banking, are the main reasons for the large-scale use of electronic identity in Estonia" (Pau 2017b).

A much more forceful discourse of threat was articulated in relation to the third domain, *damage to the Estonian e-state's international reputation*. Foreign media paid a significant attention to security problems facing the Estonian identity card; renowned publications such as the *Financial Times* and the *Frankfurter Allgemeine*

4 Starting from June 2018, the party has been named *Pro Patria* [*Isamaa*].

painted a rather dark picture of the theoretical security problems. Lauri Hussar, the editor-in-chief of the *Postimees* daily at the time, summarized this as follows: "In principle, we can say that the reputation of the Estonian e-state is put in question and the journalists over-suspicious of the cyber world can now gloatingly state that our success story will become the flight of the Phoenix" (Hussar 2017). The identity card blunder was also covered by the British technology news site *The Register* that had dug up an Estonian expletive for their title: "*Kurat võtku*!" ["Damn it!"] (Piir 2017).

According to the journalists of the *Postimees*, several analysts of the security of information technology found that the sole credible threat emerging from the vulnerability was reputation damage: "If somebody really wanted to take advantage of the vulnerability, resources would most likely be spent on ruining Estonia's reputation" (Kund, Pau 2017).

3.3. Active and passive social actors

Having first delineated the principal referent objects under threat, we can now use them to analyse the distribution of active and passive social roles. According to Theo van Leeuwen (2008: 33), active actors are represented as dominating and shaping a certain domain or action. Those in a passive role are, to the contrary, represented as the recipients and perceivers of a certain event. Regarding e-threats, it is telling how the roles of the threatener and the threatened are expressed. As mentioned above, the complexity of information technologies often makes it difficult to identify the dominating and controlling actors.

The producer of cards, Gemalto, and their customer, the PPA were among the first to articulate risk scenarios regarding the identity card. Both attempted to locate the cause of the crisis in the other's activity. When the vulnerability was picked up by the media, Gemalto almost immediately launched a counter-communications operation that laid the principal blame on the PPA. Andreas Lehmann, representative of Gemalto Eesti and the CEO of Trüb Baltic AS, commented on the social network LinkedIn on a post made by Andres Kütt, the former chief architect of the e-state for the RIA. Lehmann claimed that he had notified Estonian authorities (i.e. PPA and RIA) of the vulnerabilty on 15 June 2017, and that the main reason why Estonia had remained passive and not taken measures to relieve the threats was the summer vacation enjoyed by the authorities (Tamm 2017). The official position of the Estonian state denied Lehmann's statement. "The PPA received information of the identity card chip vulnerability from the RIA on 31 August," stated Martin Luige, spokesperson of

the PPA (Gavronski 2017). Claims made by Lehmann did, in fact, turn out to be unverifiable later; Lehmann was transferred to a different position. The mutual accusations made by Gemalto and the PPA should be viewed in the context of the process of negotiating a solution for the compensation of damages, a process that aimed to identify the main culprit for the crisis (Lõugas 2018a). This is the reason why, based on the speaker's position, the other side was depicted either as the source of the problem or else as a victim suffering because of it.

The second actor represented in the discourse of Estonian identity card vulnerability was *Russia*. Mart Helme pointed at the Russian special services – more precisely, at the Foreign Intelligence Service – and their interest in Estonian elections. "Let us recall that Russia has also been previously accused of interfering with elections in France, Germany, Great Britain, and the USA. Now the time has come for Estonia," Helme said (Kund, Pau 2017). Regarding Helme's comment, it is important to underline that Russia was not understood to have been the cause of the problem, but a possible beneficiary and abuser of the vulnerability; in other words, Russia was represented as an active participant in magnifying e-threats.

This accusation made towards Russia should, again, be interpreted in the context of the 2017 local elections for no one named Russia as an active agent besides politicians – for whom the Russian threat is an important rhetorical tool to be used in scare tactics. Helme was soon countered by the EKRE's principal ideological opponent, the Social Democratic Party [*Sotsiaaldemokraatlik Erakond*, SDE]. Hannes Hanso, the former Minister of Defence for the SDE, claimed that Russian hacking of Estonian e-voting system was highly unlikely (Velsker 2017). The possible experiences of threat for Russia's potential victims were, however, not elaborated on; nor were the potential consequences of Russian manipulation of e-voting specified: whether the interference would have had promotion of a specific political force or damaging the Estonian e-state's reputation more generally as its aim.

The third type of actors represented in the media were *hackers*. "From the moment when the work of the Czechs[5] was disclosed and when it became clear that the deficiency was, in addition, caused by Slovaks, Spaniards, Germans, and the services of Microsoft and Google, international attention grew to a point where *those type of people* emerged whose interest it is to pry open our cards," said the CEO of CERT-EE Klaid Mägi. It was considered theoretically possible for hackers to create a digital clone of an Estonian resident and pose as him/her in the internet – providing that the hackers possessed enough financing, of course. Mark Erlich, technology consultant at the RIA, described this as follows:

[5] The theoretical security risk was discovered by a group of researchers led by the Czech Petr Svenda.

> If someone could clone a digital ID, he could theoretically use the identity card for personal identification and for signing documents digitally without possessing a card him or herself and without knowing the PIN codes.(Kund, Pau 2017)

The discourse on hackers did not determine, however, how the hackers would actively be using the digital clone and what the security threats would be like for groups under specific attacks. Possible threats to banking (for example, stealing people's bank accounts) and disturbances in communication between the e-state and e-citizens were, to be sure, pointed out, but, as said above when mapping out referent objects, these actions were regarded as unlikely because of their expense and technical complexity. The identity of the hackers was left indeterminate; references were made to 'those types' and 'crooks', the opposition of the 'good hackers' ('scientists') and the 'bad hackers' ('cyber criminals') was used – naming strategies common when referring to actors operating in secrecy.

The fourth group of actors were *the public relations specialists* of the Estonian Government. Serious deficiencies were spotted in their work, especially in their actions in informing the public of the identity card vulnerability and the accompanying risks. Many were of the opinion that the public relations department did not so much inform the public than exploit the crisis in the pre-election struggle. Lauri Hussar, for example, said:

> Upon closer inspection, we must, unfortunately, admit that we ourselves have been the greatest threat to the reputation of our e-state. If only the theoretical vulnerability had been addressed differently, not involving *the Prime Minister and the politicians*, coverage of the topic would have been far more moderate. (Hussar 2017)

Hanno Pevkur, former Chairman of the Reform Party, shared the opinion. He pointed at the pre-election struggle as a principal cause of damage done to our reputation: "When we talk of the reliability of e-services and the reputation of the Estonian state, then this is no place to be scoring political points" (Kund, Pau 2017). Also Aivar Pau, a journalist at the *Postimees* pointed to the reprehensible connections between the escalation of e-threats regarding the identity card vulnerability and the upcoming elections: "The PR show served only one purpose: the desire of Jüri Ratas to discredit the e-vote" (Pau 2017c). The journalist also accused the public relations specialists of "sowing panic". Instead of informing the public of potential e-risks, the opposite result was achieved: "This is the first case in Estonia in which a crisis is generated by the crisis communication itself[6]"

[6] Pau is referring to a press conference organized on 5 September 2017, by the government, the PPA and the RIA in order to inform the public about the security risks of the ID-card.

(Pau 2017d; see also Kiin 2017). Pau also brought out the potential target groups for the government's crisis communication: "vulnerability abusers and the people" (Pau 2017d).

Thus, the public relations department of the Prime Minister's office was represented as a primary actor exploiting the topic of identity card vulnerability in order to amplify the media coverage of the Prime Minister and of the politicians sitting in the parliament, and in order to put certain political themes (opposition to e-voting) on the media agenda. The public as a whole was represented as the primary "victim", needlessly and excessively scared.

Both Liisa Oviir (SDE) (Oviir 2017), the former Minister of Entrepreneurship and Information Technology and a Member of the *Riigikogu*, as well as Toomas Hendrik Ilves (Beltadze 2017), the former President of Estonia, opposed the discourse, accusing the Estonian government of sowing fear and hysteria and saying that informing the public of a potential identity card vulnerability was a natural practice in a democratic state. Oviir and Ilves did not regard it as a bad practice that the Prime Minister took on the task of informing the public about potential risks. According to them, it would have been dangerous coming from any other source, as then a potential cover-up by the government would have been added to the list of problems.

Media emerged as another actor. The main critique addressed at journalists was their incompetence in covering the complex topic of information technology. Toomas Hendrik Ilves pointed out that the problems of Estonian e-solutions are technically complex and complicated, which is why talking about them and delving into them "requires both time and technical nous. As the articles in the *Frankfurter Allgemeine* and the *Financial Times* showed, many are not up to the task" (Beltadze 2017). In addition to the complexity of digital technologies, the clickbait logic of media economy, corrupting journalists' work ethic, was pointed out as an amplifier of the threat discourse and a source of incompetence:

> Superficial treatments are always a journalistic risk in the case of complex topics. One does not go deep enough, does not bother to engage properly. In case of this type of stories, I find myself thinking that the press does not always realize the responsibility that comes with writing. It is not an intentional lie, but carelessness and clickbait attraction. (Beltadze 2017)

Journalists were thus represented as the amplifiers of the crisis, and not as the generators of it. The superficiality and inadequacy of media coverage was seen as a result of structural changes in the journalist profession (shorter articles, catchy and often more negative interpretations of topics, the need to gain clicks, etc.).

3.4. Articulation of the urgency of threats

An important aspect in representing e-threats is the expression of their urgency, or, in other words, the way they are depicted as in need of a fast and forceful reaction. This in turn presupposes the outlining of terrifying future scenarios which illustrate the realization of threats (Hansen, Nissenbaum 2009: 1164). Another significant rhetorical device in representing the potential consequences of cyberthreats is the construction of analogies with tragic historical events, for example, to 9/11, Pearl Harbor, or natural disasters (Jarvis *et al*. 2016: 620).

The dominant rhetorical device in representations of the urgency of threats to national security and reputation damage was to imagine terrifying future scenarios. As already noted above, because of the identity card scandal politicians from the EKRE questioned the security of e-voting in general. A leading politician of the party Martin Helme claimed that there was an increase in the gravity of the threat because of its extensive coverage in the media. Justifying the necessity to cancel the e-vote, he noted: "It is a fact that *no one* can guarantee that manipulations won't take place, *especially now* that information regarding the vulnerability and its causes has spread all over the world" (Reisenbuk 2017). Thus Helme essentially stated that IT experts cannot possibly solve the problem, which is why it would be necessary to cancel the e-vote in order to guarantee security. The article addressed the attacks in a rather abstract manner, without specifying either the potential details of their execution or any concrete aggressors. A similar line of thought, namely that extensive media coverage has turned the vulnerability into an attractive target for attacks, was also repeated by other authors. The journalist Aivar Pau (2017d) stated, for example, that "if, by any chance, there previously existed a crook ignorant of the vulnerability, then *now* they would *definitely have at their disposal all* the information necessary for hacking."

The emerging threats related to the identity card were represented as if needing an extremely quick reaction – potential attacks were foreseen as occurring in just a couple of days into the future. Thus, the *Postimees* reported on the position of a civil servants:

> The time allotted to us is coming to an end as our information systems constantly keep crashing. The time for updating will run out *very shortly*. The threat assessment, or the black scenario, goes as follows: an attack directed at the security system of the Estonian identity card chip will occur on Friday or Saturday at the latest. (Pau, Berendson 2017)

This statement clearly expresses both recognition of signs of threat (constantly failing information systems) and the imminent actualization of risks. Underlining

the great probability of attacks taking place, one article stated: "*The target is extremely attractive for attacking*. Furthermore, it is more likely that hackers will attack in the next 48 hours than that they will not" (Pau, Berendson 2017). When speaking of e-threats, journalists reporting the positions of government officials used a hyper-securitizing style – they envisioned extensive and imminently escalating risks with indeterminate reference. The article in question was dramatically entitled: "The ID-scare promises to turn into a catastrophe", characterizing the gravity and future-oriented nature of the threats. The referent objects were represented as diffuse and omnipresent; for example:

> While a couple of months ago, at the time of the publication of the news story coined as the e-scare, the potential target was only the vulnerability of the Estonian identity card chip, *now the risk assessment is already global*. It entails large corporations and other countries using a similar chip technology. (Pau, Berendson 2017)

The claim was related to the information revealed meanwhile, which implicated also the e-services of Microsoft and Google, as well as Slovakia, Spain and Germany that had also collaborated with Gemalto.

Damage to the reputation of the Estonian e-state was also talked about as an extremely extensive problem, and yet one that would only materialize in the future. The closing lines of Lauri Hussar's opinion piece exemplify this kind of attitude: "Damage to Estonia's reputation *has already been done* and the opportunity to remedy the situation even a little will present itself at the end of the month at the European Union summit on digital technology. What is at stake is *nothing more or less* than the reputation of the Estonian e-state" (Hussar 2017). The media often repeated the idea that the identity card vulnerability puts Estonia's image as a leader in digital technology at risk. On the one hand, it was stressed that the trustworthiness of Estonia's e-systems could be set in doubt. On the other hand, it was even argued that the security risk might jeopardize our innovative e-infrastructure which might then be replaced with something primitive or backward-looking. In order to refer to such negative developments, the phrase "from the progress of an e-state, back to the stone age" (Pau, Berendson 2017) was used.

To highlight the gravity of the threat, previous disasters that had shocked Estonia were referenced. In an opinion piece, the technology journalist Hendrik Roonemaa used a figurative comparison: "The storm of the century is raging around the Estonian e-state. [...] During an emergency situation it is wise not to stick your nose out and just accept it instead – unless this is urgently required"

(Roonemaa 2017). The comparison is probably with the January storm that hit Western Estonia in 2005, causing extensive flooding in the seaside towns of Pärnu and Haapsalu.

Some statements also pointed at the disproportionate stress on security threats related to the vulnerability in specific parties' communication strategies. Aivar Pau (2017c), for example, posed an intriguing rhetorical question: "I am definitely not a follower of conspiracy theories, but our e-vote and especially the identity card *experienced the biggest blow to their reputation in history yesterday*. My conspiracy-theory-flavoured question is: which party gains the most?"

3.5. Constitution of the emotional background to the threats

Connecting events and their potential consequences to the speakers' condemning judgments and reactions expressing fear provides the events with a tone of emotion. Charging utterances with negative emotions makes it possible to attract the public's attention and to intensify the sense of fear. This strategy is present, for example, in expressions of concern or in condemnations of certain developments, in the use of value judgments (e.g., 'terrible', 'dreadful', 'dangerous') or of vocabulary with negative connotations (e.g., 'problem', 'conflict', 'damage') (Bednarek, Caple 2017: 79).

More than a half of all the media reports on the identity card vulnerability contained condemning or fearful judgments of the events. "A high-ranking civil servant who has been dealing with the identity card vulnerability for the last couple of days, told the *Postimees* yesterday, 'The situation is terrible'" (Pau, Berendson 2017). When speaking of the vulnerability, a range of negatively charged words were used to refer to the events of autumn 2017: 'crisis', '(security) risk', 'threat'. In articles speaking of the threat to Estonia's digital infrastructure or to e-voting, there occurred a lot of talk of potential 'attacks' and of the 'vulnerability' of systems. References to the clearly negative term 'manipulation' were quite common. Manipulation was most often mentioned regarding both the potential tampering with the e-vote and the disproportionate scaring of the public with threats accompanying e-voting.

Media coverage that dealt with reputation damages to e-Estonia also used the term 'vulnerability scandal' to refer to the event. This term indicates that the vulnerability had been turned into a sensational media event. A similar tone was conveyed by the phrases 'PR show' and 'crisis generated by crisis communication'. The phrase 'damage to reputation' and the verb 'blemish' that refers to malicious infringement were used quite often. To characterize the public's reactions and

the media coverage itself, condemnatory terms or even ones referring to psychopathology were used such as 'panic' and 'hysteria'. Henrik Roonemaa (2017) used the metaphors of 'panic' and 'hysteria' forcefully in his opinion piece: "In the phase of hysteria, the dust from the tumult has not yet settled, so that nothing can be seen clearly. [...] There is no point, in this type of a situation, in waving your hands in the dust and panicing. After some time has passed, everything will become much clearer." The wording expressed the author's critical attitude towards the media's overreaction as well as towards the excessive anxiety displayed by the people.

3.6. Ways of managing threats

A key statement in the discourse of digital securitization is: if certain measures are not taken, grave events will occur in the near future (Hansen, Nissenbaum 2009: 1161). Thus, at least some solutions are suggested in a discourse of threats, even if only implicitly. Because of the technical complexity of e-threats, public discourse tends to associate facing and fighting them with a relatively small group of experts possessing knowledge of the field (Hansen, Nissenbaum 2009: 1167). Informing the public of countermeasures to e-threats is thus a crucial component in a discourse of fear.

In the discourse of Estonian identity card vulnerability, the following aspects were mentioned: (a) *technical countermeasures* taken in order to prevent attacks to identity cards with the vulnerability, and (b) *structural countermeasures* either taken or planned to be developed should similar digital problems occur in the future.

The former, technical category involves, first and foremost, restrictions on the use of identity cards, applied in fear of potential hacking. On 5 September, the day that the media first reported the problem, the PPA suspended the public keys database. The keys enabled encryption and decryption of files – only the owner of the key can decrypt a file sent to him or her. The other significant measure was taken at the beginning of November. All identity cards with the vulnerability were suspended, because issuing new cards did not go according to plan and experts feared a hacking attack (Pau, Berendson 2017). The production of an updated version of the identity card, issued in 2018, also counts as a countermeasure (Lõugas 2018b). Some domains of the private sector were also involved in organized countermeasures. The RIA advised that citizens adopt mobile identity (Velsker 2017) and, after the disclosure of the identity card vulnerability, the Estonian mobile service providers were prepared for an increase in demand (Postimees 2017).

Legitimization of the above-mentioned countermeasures occurred in the context of a threat discourse on hacking and digital cloning. The countermeasures were supposed to diminish the (theoretical) threat even further. Our study did not find a single media report that would have mentioned a successful hacking of identity cards with the vulnerability.

The structural countermeasures regarding management had to do with gaining better control of the whole system and with prevention of potential future security problems. Taimar Peterkopf, the general manager of the RIA, said in an interview:

> If we wish to act as a role model and be among the leaders of digital states also in the future, then the politicians have to dedicate more resources and attention to the field. For this purpose, we could appoint a separate minister. (Lõugas 2018c)

In addition, it was pointed out that there were too few specialists knowledgeable in identity card security in the public sector. Introducing a report on the identity card security crisis, Rain Ottis, the Head of the Centre for Digital Forensics and Cyber Security at the Tallinn University of Technology, said that the crisis was largely survived thanks to the specialists working in the private sector: "Whether it is the private sector, the academic sector or the public sector – it is not possible to bring them all together under the same roof. However, there is nothing bad in having specialists in the private sector, given that they are available to the government during emergencies" (Piir 2018).

Both of these countermeasures – restructuring of the field dealing with cyber security and increasing the number of specialists in digital technology – were justified by the position and reputation of Estonia as a leading e-state. Potential e-threats inevitably accompany the structures of the Estonian e-state. Both the experts [see, e.g., an interview with Anto Veldre (Leivak 2017)] and the spokespersons of e-Estonia (e.g., Toomas Hendrik Ilves) highlighted that the cyber domain is constantly evolving and that this always involves a possibility of certain risks. "The security risks [accompanying the identity card] are inevitable. An actual cyberthreat is preventable" (Beltadze 2017). Andrus Ansip, Vice-President of the European Commission, said that at the moment, when e-state's solutions were facing special scrutiny – since Estonia was holding the presidency of the Council of the European Union – "quick problem solving [could] demonstrate our strength" (Velsker 2017) and help compensate for the damage to our reputation in the international arena.

4. The logic of relations between scenarios of security risks in the context of phobophobia

The following will explain the semiotic mechanism underlying the discourses of fear regarding the identity card vulnerability. We will concentrate on directly phobophobic positions expressing concern over the excessive fear gripping the public, and on explicating the characteristics that amplified the discourse of fear in articulations of threat scenarios.

4.1. Fear of fear

The first important characteristic of a phobophobic discourse is that those articulating this discourse *position themselves outside a discourse of fear*. We are thus dealing with the position of a bystander – one does not rise to the meta-level by reflecting over his or her own fears, but by expressing concerns over a panicking and manipulable *public*.

In the course of the analysis of the discourse of e-threats we were able to determine two instances which clearly expressed concern over the unjustified sowing of fear. The first of those dates back to the beginning of the crisis. It was a piece of criticism directed towards the Prime Minister and his office, accusing them of amplifying the topic and of connecting it to the local elections. Sirje Kiin, literary scholar and communications specialist, noted in an opinion piece (Kiin 2017) that, although informing the public of the identity card vulnerability was entirely justified, it should have been done not by the Prime Minister, but by either the RIA, Estonia's top IT experts, or by the minister of the field in question.

> Did this type of top-level political attention-grabbing not damage the reputation of the Estonian state even more than one (although, granted, large-scale) identity card security threat – that, furthermore, was not caused by an error made in Estonia, but by chips imported from elsewhere. (Kiin 2017)

A similar sentiment was expressed by Aivar Pau, journalist at the *Postimees*: "Sowing of panic up front was not justified in my opinion; it was disproportionate and damaging – to Estonia, to our identity card and to the reliability of our e-voting" (Pau 2017d).

The second wave of concern over the proliferation of fears emerged at the beginning of November. By then, the potential likelihood of hacking had significantly increased according to several cyber security specialists, and the Estonian government decided to suspend the use of identity cards with the

vulnerability in fear of the threat scenarios becoming reality. Analysing the media coverage of the vulnerability in an opinion piece entitled "Everything will soon be alright", the technology journalist Hendrik Roonemaa wrote, "No doubt it is necessary to cover these kind of events critically, but hysteria is not justified, nor is it necessary to anybody" (Roonemaa 2017).

In the following, we will explicate the general meaning-making mechanism prevalent in the representation of e-threats and the discourse of fear.

4.2. The semiotic mechanisms of the discourse of threat

E-threats can be divided in two: (1) concrete (actual or possible – that is, located in the future); (2) abstract or reference-based that are articulated in a relatively ambiguous manner. The latter type is characteristic of the discourse of fear. As shown by their very name, concrete e-threats are relatively clear-cut and can be localized. The articulation of abstract threats, however, entails the constitution of extensive sources of threat (covering several domains of life); the omnipresence and difficulty of identification of these sources is underlined. In the formation of a discourse of fear, it is important to analyse which discursive mechanisms are used to speak of e-threats and how different actors, referent objects and threat scenarios are woven together in a whole.

Semiotics of culture differentiates between two fundamental types of discursive relations: (1) approximate or non-discrete logic of signification based on similarity and analogy; (2) discrete or verbal logic based on the regularized connection of elements, for example, chronologically and according to relations of cause and effect or the part and the whole (J. Lotman 2002: 2646–2649). The discourse of fear is first and foremost characterized by non-discrete signification: relations between the causes and effects of threats, as well as the sense of fear stemming from the risk, are ambiguously articulated.

In the texts analysed, the abstract nature of threats was mainly expressed by the indeterminateness of actors and by future threats that were defined relatively vaguely. The texts described the boundaries of the referent objects of securitization, the relations between them, and the actors behind threat scenarios in a vague manner. Thus, in order to refer to active actors, the texts used the terms 'evil hackers' and 'crooks' whose potential actions (e.g., the possible use of digital clones) and motivations were left unspecified – which is why these actors proved to be almost impossible to identify. A similar construction of relations can be seen in the discourse concerning the interference in e-voting. While a dangerous activity – manipulating the process of e-voting – was concretely named, it was not specified how exactly it is possible to interfere in the voting process, who would

commit the interference, and whose interests the interference would have served in the local election. The Russian card played by the Conservative People's Party of Estonia can be understood as a strategy attempting to influence the constituency with fear of Russia. It is remarkable that such a hypothetical threat with a relatively vague reference was linked to a larger cascade of threats, thus connecting the identity card vulnerability with something so fundamental as the subversion of the Estonian democratic social order.

We also recognized a contrary, non-discrete logic of the discourse of threat, a logic that clearly identified the actor, but did not specify any concrete threat scenarios or domains needing securitization. Prime Minister Ratas and the government's PR team were identified as the generators of e-threats; they were accused of sowing panic among the public and of damaging the international reputation of the e-state. The specific meaning of 'reputation damage' was, however, left unspecified. The word 'reputation' is rather ambiguous; any specific descriptions of what damage to reputation would entail and whose reputation it was that was damaged – or, what the concrete referent object was – never became clear. Characteristics of hyper-securitization were present in the media coverage of reputation damage; the latter was constituted as an umbrella that gathered together different threatened referent objects. Reputation damage and unsuccessful communication became the meta-level generators of causality, i.e those operating outside specific discourses of threat. The extensive and intensive coverage of the event was pointed to as a factor increasing the probability of attack, since the coverage supposedly resulted in drawing the attention of both the hackers and forces hostile to Estonia to the identity card and Estonian digital infrastructure. At the same time, unsuccessful communication was represented as a factor undermining trust in Estonian digital infrastructure and Estonia's image as an e-frontrunner both at the national and the international level. The latter was perceived as especially problematic, since this image is a cornerstone of Estonia's positive and future-oriented national identity.

One characteristic of the abstract threat discourse was the articulation of scenarios of e-threats based on analogy. The purpose here was to envision and exemplify both the high probability and the terrible consequences of potential attacks. Analogies were drawn with events from recent history (Russian interference in French, German, British and American general elections; "the storm of the century"). Hypothetical future scenarios that drew parallels between the tense present situation (shortcomings in updates to information systems) and threats soon to be actualized (large-scale attacks on citizens' e-identity or on the Estonian digital infrastructure).

Since an analogy describes one object via a metaphorical substitution with another, the addressee of the message is often tasked with creating his or her own

image of the relations between the elements referring to the referent object. The relations are often defined by a mere reference to analogy or by an act of naming – a clear example of non-discrete construction of relations, according to Juri Lotman (J. Lotman 1999: 51; Ventsel, Madisson 2017, see also Ventsel 2014, 2016; Selg, Ventsel 2010).

Besides analogy, the characteristic discursive ambiguity of phobophobia was expressed in the description of countermeasures to be taken in order to defend the securitized referent objects. This description was often characterized by a sense of urgency concerning the problem. 'Crisis', '(security) risk' and 'panic' were constituted, in public discourse, as labels for the event – all referring to an urgent need to remedy the situation and to find quick solutions. In order to manage e-threats, however, relatively abstract and future-oriented instructions were presented. Taimar Peterkopf, the general manager of the RIA, was rather indeterminate in his description of the professional tasks of a proposed ID-minister: the minister would "set an ambition and create a political demand for fast progress" (Lõugas 2018b). It is not clear what could be done better or differently in case of a possibly emerging crisis. But of course some very concrete measures were also taken to manage the identity card security risks (see Section 3.6. "Ways of managing threats").

5. Conclusion

The article discussed the formation of a discourse of fear that emerged in connection with the identity card vulnerability disclosed in September 2017. In order to delineate this discourse we mapped the main referent objects, the actors, the urgency of threat references, and the proposed solutions to deal with the threats. According to the analysis, the principal threats presented in media discourse were the potential manipulation of the results of e-voting, hacking into the state's information systems, and the extensive reputation damage to the e-state. The latter was constituted as a centre bringing together different discourses of threat, since the probability of hacking was understood to be increasing because of the extensive coverage of the event. The excessive and disproportionate communication of risks stemming from the vulnerability was seen as a direct cause of the reputation damage. In the discourse, this communication was related to pre-election political struggle, but also to not easily graspable nature of information technology. The discourse speaking of unsuccessful communication was largely conceptualized in terms of phobophobia – the expression of fear concerning the potential consequences of the proliferation of the threat discourse. At this point it

is important to note that reputation damage was the topic everybody was speaking about: IT experts, politicians, communications experts and journalists. Reputation damage was thus constituted as a hyper-securitized referent object. E-voting was the object of mainly political rhetoric, while potential threats of hacking were mostly addressed by specialists in the field.

We explicated the semiotic logic underlying the formation of a discourse of fear. This logic is based on non-discrete signification. In summary, the latter is expressed by the indeterminate manner of defining the relations between the causes and effects of threats and by the ambiguous sketching of the sense of fear accompanying the risks. In the coverage of the identity card vulnerability, the non-discrete formation of connections by the discourse of fear was manifested, in some texts, in the representation of actors that were rather vaguely articulated, and in other texts, in the indeterminateness of threat scenarios and domains in need of securitization.[7]

Appendix 1. Analysed material

Beltadze, Georgi 2017. Toomas Hendrik Ilves: e-riigina tegutseb Eesti maailmaliigas, kriitikaks tuleb valmis olla [Toomas Hendrik Ilves: As an e-state, Estonian belongs to the top league; we must be ready for criticism]. *Postimees* 12.09.2017 =https://arvamus.postimees.ee/4240381/toomas-hendrik-ilves-e-riigina-tegutseb-eesti-maailmaliigas-kriitikaks-tuleb-valmis-olla.

e-Eesti rahvusvahelise maine edendamise ajakohastatud tegevuskava aastateks 2018–2019 [Plan for the promotion of Estonia's international reputation for the years 2018–2019]. Information System Authority. https://www.ria.ee/sites/default/files/content-editors/ITT/e-eesti_rahvusvahelise_maine_edendamise_tegevuskava_2018-2019.pdf.

Hussar, Lauri 2017. Tallinn, meil on probleem [Tallinn, we have a problem]. *Postimees* 07.09.2017. https://arvamus.postimees.ee/4236439/lauri-hussar-tallinn-meil-on-probleem.

Jõevere, Kristjan; Helme, Kristi 2017. Turvariskiga ID-kaartide sertifikaadid peatatakse alates homme õhtust [Identity cards with the security risk will be suspended starting from tomorrow evening]. *Delfi* 02.11.2017, http://www.delfi.ee/news/paevauudised/eesti/blogi-ja-fotod-turvariskiga-id-kaartide-sertifikaadid-peatatakse-alates-homme-ohtust?id=80046784.

Gavronski, Anna 2017. ID-kaardi tootja Gemalto palus PPA-lt vabandust [Gemalto, the producer of identity cards, apologised to PPA]. *ERR* 29.11.2017. https://www.err.ee/645667/id-kaardi-tootja-gemalto-palus-ppa-lt-vabandust.

Kiin, Sirje 2017. ID-torm veeklaasis [ID storm in a teacup]. *Postimees* 19.09.2017. https://arvamus.postimees.ee/4248337/sirje-kiin-id-torm-veeklaasis.

[7] **Acknowledgements.** This work was supported by the research grants PUTJD804, SHVFI19127 "Strategic Narrative as a Model for Reshaping the Security Dilemma", O-014 and PRG314.

Krjukov, Aleksander 2017. 18 000 inimest ei saa ID-kaarti kauguuendada [18 000 people unable to update their identity cards remotely]. *ERR* 01.11.2017- https://www.err.ee/639921/18-000-inimest-ei-saa-id-kaarti-kauguuendada.

Kund, Oliver; Pau, Aivar 2017 a. Häkkerid võinuks luua eestlastest digikloonid [Hackers could have made digital clones of Estonians]. *Postimees* 05.09.2017. https://tehnika.postimees.ee/4234045/hakkerid-voinuks-luua-eestlastest-digikloonid.

Leivak, Verni 2017. E-riigi reliktid [Relics of the e-state]. *Postimees* 15.09.2017. https://www.postimees.ee/4238749/e-riigi-reliktid.

Lõugas, Hans 2018a. Kuidas meile ID-kaardi kriisi kohta dokumendid lekitati ja miks me neid ei usu [How the documents of the identity card crisis were leaked to us and why we don't believe them]. *Geenius* 06.09.2018.

– 2018b. Aasta lõpus tuleb välja kontaktivaba ID-kaart [At the end of the year, contactless identity card will be released]. *Geenius* 29.06.2018. https://geenius.ee/uudis/aasta-lopus-tuleb-valja-kontaktivaba-id-kaart/.
– 2018c. RIA peadirektor läheb pikale puhkusele: ID-kaardi kriisi kordudes teeksime ühe asja teistmoodi [RIA's general managers takes a long vacation: in case of the identity card crisis repeating, we'd do one thing differently]. *Geenius* 03.09.2018. https://geenius.ee/uudis/ria-peadirektor-laheb-pikale-puhkusele-id-kaardi-kriisi-kordudes-teeksime-uhe-asja-teistmoodi/.

Olup, Nele-Mai 2017. Reinsalu turvariskist: alatu on seda siduda poliitilise debatiga e-valimiste usaldusväärsusest [Reinsalu on the security risk: It is low to tie this into the political debate over the reliability of e-voting]. *Postimees* 05.09.2017. https://www.postimees.ee/4234057/reinsalu-turvariskist-alatu-on-seda-siduda-poliitilise-debatiga-e-valimiste-usaldusvaarsusest.

Oviir, Liisa 2017. Vastus Aivar Paule: ID-kaardi kriisikommunikatsiooniga tegelesid ässad [A reply to Aivar Pau: The identity card crisis communication was handled by aces]. *Postimees* 14.09.2017. https://arvamus.postimees.ee/4244293/vastus-aivar-paule-id-kaardi-kriisikommunikatsiooniga-tegelesid-assad.

Pau, Aivar 2017a. Kes vassib: kõik, mida teame ID-kaardi riski teavitamisest [Who's muddling: All that we know of communicating the identity card vulnerability]. Postimees 27.11.2017, https://tehnika.postimees.ee/4324531/kes-vassib-koik-mida-teame-id-kaardi-riski-teavitamisest?_ga=2.33923233.1046869938.1548582760-1960120442.1516030406.

– 2017b. Professor: miks Eesti inimene ei kasuta ID-kaarti? [Professor: Why doesn't the Estonian use the identity card]. *Postimees* 13.09.2017. https://tehnika.postimees.ee/4242309/professor-miks-eesti-inimene-ei-kasuta-id-kaarti.
– 2017c. Repliik: Ratas andis ID-kaardi jamaga turmtuld e-valimistele [Ratas attacked e-voting equipped with the identity card blunder]. *Postimees* 06.09.2017. https://tehnika.postimees.ee/4234361/repliik-ratas-andis-id-kaardi-jamaga-turmtuld-e-valimistele.
– 2017d. Repliik: Kriis, mis tekitas kriisi [The crisis that generated the crisis]. *Postimees* 14.09.2017. https://tehnika.postimees.ee/4243691/repliik-kriisikommunikatsioon-mis-tekitas-kriisi.

Pau, Aivar; Berendson, Risto 2017. ID-ehmatusest tõotab saada häving [The identity card scare threatens to turn into a disaster]. *Postimees* 01.11.2017. https://tehnika.postimees.ee/4296205/id-ehmatusest-tootab-saada-having.

Piir, Rait 2017. Välismeedia nimetab Eesti ID-kaardi juhtumit piinlikuks [Foreign media calls Estonian identity card case embarassing]. *Postimees* 06.09.2017. https://tehnika.postimees.ee/4234511/valismeedia-nimetab-eesti-id-kaardi-juhtumit-piinlikuks.

– 2018. TTÜ raport ID-kaardi kriisist: riigiasutustes on ohtlikult vähe krüptograafia spetsialiste [Tallinn University of Technology's report on the identity card crisis: State institutions employ dangerously few cryptography experts]. *Postimees* 19.04.2018. https://tehnika.postimees.ee/4475152/ttu-raport-id-kaardi-kriisist-riigiasutustes-on-ohtlikult-vahe-kruptograafia-spetsialiste.

Postimees 2017. Mobiilioperaatorid on valmis suurenenud huviks mobiil-ID vastu [Mobile service provides are prepared for increased demand for mobile identity]. *Postimees* 05.09.2017. https://www.postimees.ee/4233689/mobiilioperaatorid-on-valmis-suurenenud-huviks-mobiil-id-vastu.

Reisenbuk, Karel 2017. EKRE vaidlustas e-valimiste korraldamise [EKRE challenged the organization of e-voting]. *Postimees* 11.09.2017. https://www.postimees.ee/4239139/ekre-vaidlustas-e-valimiste-korraldamise.

Roonemaa, Hendrik 2017. Kõik saab varsti korda [Everything will soon be alright]. *Postimees* 02.11.2017 https://arvamus.postimees.ee/4297675/henrik-roonemaa-koik-saab-varsti-korda.

Tamm, Mihkel 2017. ID-kaardi tootja Gemalto Eesti esindaja: teavitasin turvariskist juba 15. juunil [Estonian representative of Gemalto, the identity card producer: I made a notification of the risk already on 15 June]. *Delfi* 22.11.2017. http://www.delfi.ee/news/paevauudised/eesti/id-kaardi-tootja-gemalto-eesti-esindaja-teavitasin-turvariskist-juba-15-juunil?id=80250642.

Velsker, Liis 2017. ID-kaardi kiibis avastati teoreetiline turvarisk [Theoretical vulnerability discovered in the identity card chip]. *Postimees* 05.09.2017. https://tehnika.postimees.ee/4233255/id-kaardi-kiibis-avastati-teoreetiline-turvarisk.

References

Altheide L. David 2002. *Creating Fear: News and the Construction of Crisis*. New York: Aldine de Gruyter.

Barnard-Wills, David; Ashenden, Debi 2012. Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture* 15(2): 110–123.

Bednarek, Monika; Caple, Helen 2017. *The Discourse of News Values: How News Organizations Create Newsworthiness*. New York: Oxford University Press.

Buzan, Barry; Wæver, Ole; Wilde, Jaap de 1998. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.

Grint, Keith 2010. Wicked problems and clumsy solutions: The role of leadership. In: Brookes, Stephen; Grint, Keith (eds.), *The New Public Leadership Challenge*. Basingstoke: Palgrave Macmillan, 169–186.

Hansen, Lene; Nissenbaum, Helen 2009. Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly* 53(4): 1155–1175.

Harsin, Jayson 2015. Regimes of posttruth, postpolitics, and attention economies. *Communication, Culture & Critique* 8(2): 327–333.

Head, Brian W.; Alford, John 2015. Wicked problems: Implications for public policy and management. *Administration & Society* 47(6): 711–739.

Jansen, Sue Curry 2008. Designer nations: Neo-liberal nation branding – brand Estonia. *Social Identities* 14(1): 121–142.

– 2012. Redesigning a nation: Welcome to Estonia, 2001–2018. In: Kaneva, Nadia (ed), *Branding Post-Communist Nations: Marketizing National Identities in the "New" Europe*. New York: Routledge, 79–98.

Jarvis, Lee; Macdonald, Stuart; Whiting; Andrew 2016. Analogy and authority in cyberterrorism discourse: An analysis of global news media coverage. *Global Society* 30(4): 605–623.

Kalmus, Veronika; Talves, Kairi; Pruulmann-Vengerfeldt, Pille 2013. Behind the slogan of "e-state": Digital stratification in Estonia. In: Ragnedda, Massimo; Muschert, Glenn (eds.), *The Digital Divide: The Internet and Social Inequality in International Perspective*. London: Routledge, 193–206.

Kulcsár, László; Yum, Young-ok 2012. One nation, one brand? Nation branding and identity reconstruction in post-communist Hungary. In: Kaneva, Nadia (ed.), *Branding Post-Communist Nations: Marketizing National Identities in the "New" Europe*. New York: Routledge, 193–212.

Leeuwen, Theo van 2008. *Discourse and Practice: New Tools for Critical Discourse Analysis*. New York: Oxford University Press.

Lotman, Juri 1999. Kultuur kui subjekt ja iseenese objekt. In: Lotman, Juri, *Semiosfäärist*. (Pruul, Kajar; Lias, Pärt, trans.) Tallinn: Vagabund, 37–52.

– 2002. Kultuuri fenomen. (Salupere, Silvi, trans.) *Akadeemia* 12: 2644–2662.

Lotman, Mihhail 2009a. Hirmusemiootika ja vene kultuuri tüpoloogia I: Kultuurisemiootika ja hirmu fenomenoloogia. (Pruul, Kajar, trans.) *Akadeemia* 1: 191–215.

– 2009b. Hirmusemiootika ja vene kultuuri tüpoloogia V: Kokkuvõtte asemel. *Akadeemia* 6: 1217–1248.

Madisson, Mari-Liis 2016. Snowdeni skandaali kujutamine eesti meedias: Hirmu ja ohtude konstrueerimine. *Acta Semiotica Estica* 13: 10–36.

Madisson, Mari-Liis; Ventsel, Andreas 2016. 'Freedom of Speech' in the self-descriptions of the Estonian extreme right groupuscules. *National Identities* 18(2): 89–104.

Sandywell, Barry 2006. Monsters in cyberspace: Cyberphobia and cultural panic in the information age. *Information, Communication & Society* 9(1): 39–61.

Selg, Peeter; Ventsel, Andreas 2010. An outline for a semiotic theory of hegemony. *Semiotica* 182: 443–474.

Tammpuu, Piia; Masso, Anu 2018. "Welcome to the Virtual State": The Estonian e-residency and digitalised state as a commodity. *European Journal of Cultural Studies* 21(5): 543–560.

Ventsel, Andreas 2014. Hegemonic signification from perspective of visual rhetoric. *Semiotica* 199: 175–192.

– 2016. Rhetorical transformation in Estonian political discourse during World War II. *Semiotica* 208: 103–132.

Ventsel, Andreas; Madisson, Mari-Liis 2017. Tõejärgne diskursus ja semiootika. *Acta Semiotica Estica* 14: 93–116.

– 2018. Fobofoobia: Küberohtude ja infosõja diskursused Zapad 2017 õppuste meediakajastuse kontekstis. *Sõjateadlane* (*Estonian Journal of Military Studies*) 8: 181–199.

Ventsel, Andreas; Hansson, Sten; Madisson, Mari-Liis; Sazonov, Vladimir 2019. Discourse of fear in strategic narratives: The case of Russia's Zapad war games. *Media, War & Conflict,* 1–19.

Семиотика угроз: дискурсы уязвимости эстонского удостоверения личности

Статья анализирует отражение в эстонских СМИ различных дискуссий, вспыхнувших после обнаружения угрозы риска злоупотребления эстонским удостоверением личности в 2017 году. Дискурс о киберугрозах не очень понятен обычному читателю, не обладающему экспертными знаниями относительно функционирования и архитектоники электронных услуг. Поэтому тексты, где рассматриваются киберугрозы, вызывают иррациональное беспокойство и создают необоснованные сценарии угроз. Наша теоретическая основа объединяет понятийный аппарат Копенгагенской школы исследований в области безопасности с идеями семиотики культуры. Мы объясняем семиотическую логику фобофобии (то есть абстрактную озабоченность разрушительными последствиями коллективного чувства страха) и семиотические механизмы дискурса страха. Этот дискурс страха характеризуется использованием аналогий, нечеткими гранями между разными объектами-референтами и преобладанием отрицательной эмоциональной тональности. Наше исследование показывает, что главными актантами в дискурсе об электронной безопасности удостоверения личности были представлены неизвестные хакеры и подрыв репутации Эстонии как электронного государства.

Ohusemiootika: Eesti ID-kaardi haavatuvuse diskursused

Artiklis analüüsitakse 2017. aasta sügisel avastatud Eesti ID-kaardi turvariskiga seotud e-ohtude meediakajastusi. Küberohud on ilma IKT-alaste eriteadmisteta üldsuse jaoks raskesti mõistetavad ja seetõttu sisaldavad nendest rääkivad tekstid rohkelt vastuolusid, oletuslikkust ning tugevat emotsionaalset laengut. Analüüsis lähtutakse Kopenhaageni koolkonna *julgeolekustamise* raamistikust, mille kohaselt on e-ohu konstrueerimine diskursiivne akt, mis kehtestab vähemalt ühe referentobjekti, mida kujutatakse ohustatuna ning kiiret kaitset vajavana. Uurimuse laiemaks eesmärgiks on selgitada, kuidas rääkida e-ohtudest viisil, mis ei tekitaks auditooriumis liigseid ohustsenaariume, ärevust või hirmu. Selgitame fobofoobia loogikat, mis väljendub abstraktses mures kollektiivse hirmutunde ohtlike mõjude pärast, ning hirmudiskursuse semiootilisi mehhanisme. Viimast iseloomustab tugev toetumine analoogiatele, referentobjektide vaheliste piiride ähmasus ning negatiivne emotsionaalne tonaalsus. Meie uurimus näitab, et ID-kaardi turvariskiga seotud ohudiskursus kujutas peamiste toimijatena tundmatuid häkkereid ning nägi ohustatuima ning tulevikus kõige enam probleeme tekitava referentobjektina Eesti kui e-riigi maine kahjustamist.