

## Semiotics of Estonian E-Threats. An Interview with Mari-Liis Madisson

**Theresa Procházková; Marie Zetová**

*Charles University*

*Mari-Liis Madisson conducts research on semiotics of risk and e-threats within the Estonian political context at the Department of Semiotics at the University of Tartu, where she also chairs the Media and Communication Department. She teaches courses about media semiotics and online culture. Her research interests, however, cover also other topics in cultural semiotics, political semiotics, identity studies, media studies and strategic communication with respect to surveillance and communication in cybersphere. She is the author of *The Semiotic Construction of Identities in Hypermedia Environments: The Analysis of Online Communication of the Estonian Extreme Right* (Tartu University Press, 2016). The interview was conducted in August 2017 during the Summer School of Semiotics in Tartu, where she, along with her colleague Andreas Ventsel, delivered a presentation on their current research. We also spoke about her view of media literacy and perception of cyber threats among the general public.*

**Your contribution to the Summer School was devoted to the semiotics of risk and Estonian e-threats. In the presentation, you were talking about the fear of e-threats and you used semiotics to describe the discourse people use to talk about it and the way e-threats are represented in the mass media. What are you going to use this research for?**

We are in the phase of deciding what our case study will be about and probably we will conduct a study that is analysing a period of one year in Estonian major media outlets; how the threats are constructed. And probably we will concentrate on visual discourse – how the media are using images for pairing it with a story and making those threats more plausible and more tangible. And it is funny, I have noticed. When we were doing our preliminary study for the presentation, just a simple data-gathering, what caught our eyes was that they are often re-using the same images. For example, a green hand that is coming out of a computer screen was used quite often, and also some other pictures – like one image in which a computer mouse was depicted as a tank.

**In your presentation, you also mentioned how we tend to compare the possibilities of e-threats to some events that are more tangible, for example to natural disasters or terrorism. Do you think that these parallels are accurate or rather misleading?**

Well, I think it is not a talk of “good” and “bad”. They definitely are activating some associations that are relevant in the sense of articulating the e-threats. The domain of

cyber-sphere is really vague and people don't have habitual patterns of imagining it, because it is relatively new and quickly developing. When the media draw parallels with terrorism, they are, in a way, on point and justified, because the attackers are hidden and can potentially harm a huge number of people. But in some other ways it can be tricky, it may raise too much fear.

**In the research you have conducted, did you, along with the military or terror threats, also find any reflection of how social networks collect data about their users in order to “personalise” advertising, thus potentially manipulate consumers’ choices? Is collecting personal data also represented in the pictures and do people see it as a threat?**

That is a really good question which probably has many layers. If we take the perspective of the user, then yes. I think the images of Big Brother are used quite often, but it is very abstract. And it may mean that people are aware that using a free platform means that their own data and personal choices and preferences are the price that they pay for it. I think that in Estonia, but also in some other countries, people gradually acknowledge that. But the image of Big Brother is so abstract that it may refer to surveillance which comes from the state structures and private companies. But there is also another layer of this industry, which is industrial espionage.

**What kinds of e-threats prevail in public discussion: business or terrorism-related ones?**

I think they are much varied, depending on what is happening in big media picture. The last big wave of this talk about cyber-threats was related to the WannaCry virus [worldwide ransomware attack that took place in May 2017, affecting hundreds of thousands of computers with Microsoft Windows and manipulating users into paying in Bitcoins for data recovery] and the main image that was used to illustrate it was a picture of a hacker who looked almost like a burglar, with a black hat and his face covered except for the eyes (usually they appeared to be male). Computers or hackers are typically depicted as active and the users as the victims. Regarding the debate about how Russia possibly hacked the elections in the USA, one could also see pictures of army with keyboards and computer mice.

**In Russia, there are whole “factories” for manufacturing hoaxes and fake news in order to spread fear. What if you were to compare it to the illustrations in mainstream media, how these come into existence?**

The cartoonists who work for the newspapers quite often draw the pictures. They want to intrigue, they want to catch the clicks and they are making the images as dramatic as possible. Another thing that is interesting about this visual discourse is that newspapers are using the pictures that are publicly available and that are not under copyright protection and that is the reason why Estonian newspapers and for example the BBC are also using the same images. These things play a very significant role in the visual discourse. Sometimes it is difficult to find out who makes the most violent and intriguing images; these are often not very professional.

**What is the role of fake news in all of this in your opinion? How are they created and transmitted further?**

That is also a really interesting aspect. I would say that we have not detected any strictly orchestrated fake news in our study; rather we have noticed that people – journalists – sometimes just do not know the facts. So I believe that journalists can spread ambiguous details and fuel fear unwillingly. It happened in the case of WannaCry. The first news was vague and it was not backed up with the facts, only opinions or pieces of information that were not put together logically. But I would not call it a deliberate information attack.

**It is not deliberate, but it is still happening for some reason.**

Yes, that is why I think it is good to distinguish between misinformation and disinformation. Disinformation is strictly orchestrated, and it is possible to detect it. But if people share it on their social media profiles, at least their purposes are not strictly manipulative. Another thing – and I think this aspect is important – is that there is quite huge media coverage (in mainstream media, but also in alternative media or in social media) of the fear of fake news and of the fear of the fact that information can be deliberately manipulated – and that is also an aspect of cyber-fears. In the past we had gate-keepers, we had some sources we could trust, but now the mainstream media is also oriented towards the clicks and it also tries to get huge coverage in social media.

**Do you think the news is getting more ambiguous?**

Yes, definitely.

**And does this also happen with well-established newspapers in Estonia – that a hoax, for example, makes it to the front page?**

I would not say it is a common thing. But what I can see is that, for example, opinion stories have gotten more colourised. Especially the titles are very intriguing – something like this wasn't possible ten years ago. But they really want to get clicks. They need to get money, they need to be shared.

**And what is the role of semiotics in all of this? Do you think that semioticians should “step in” and warn or educate people more on these topics?**

Yes, definitely! I think semiotics as a discipline, especially media semiotics or cultural semiotics, has a role in developing media literacy. Of course, critical, contextual reading is one thing that we can teach with our theories and methods. But another thing is that we can analyse the level of representation and see what kind of socio-cultural functions particular tendencies of representation have in society. For example, are memory and community feeling oriented towards dialogue? And yes, as a semiotician I think addressing those questions is our mission.

**What kind of theoretical framework do you find applicable? And how can it be put into practice?**

Since I come from Tartu, I feel that some of Lotman's tools are very applicable. For

example, his framework of five socio-communicative functions of text can be really used in research. Also his ideas about auto-communication and dialogic communication. Trans-media theories, multi-modal translation and the concept of repetition can be useful as well. If some information is repeated in various sign systems, it probably has a very strong attention-grabbing effect. Additionally, the concept of anchoring also seems relevant because it explains how headlines and illustrations activate certain patterns of interpretation and how they can start to frame our reading paths. It helps to understand how pictures may guide a possible interpreter to a certain direction, what activates your previously existing associations. I think such problems can be examined very well using semiotics.

**Is there some research that applies Lotman's theory to problems like social media and social networks?**

Yes, we are doing those things in Tartu, I am personally. We also have a research group that is especially concentrating on social media. There are colleagues who study trans-media community. At the moment, they are dealing with artistic texts and films and actively collaborate with writers and film directors, expanding their focus also on social media.

**Can you tell us more about some particular steps by which you have put semiotics into practice in the past, in terms of both using it in empirical research and holding an interaction between semiotic community and the public?**

My co-author Andreas Ventsel hosted a "hackathon" on post-truth society. It was a working meeting of several groups of people who, together, tried to come up with some solutions of phenomena related to the post-truth era. There were many programmers who tried to come up with apps for detecting fake news. One team wanted to create environment that allows you to step inside a filter bubble that does not fit your own pre-existing views, the opposite group. I think that this hackathon raised public attention.

**Are there any plans for more projects of this kind in the future?**

Yes, definitely. We are applying for a grant, which is dedicated to the construction of cyber risks and threats. If we get it, then we will start a systematic analysis. We are planning to organise some workshops that are dedicated to high school teachers of social sciences like social education, history and media. Later, we would like to include also some students.

**So you will be spreading this kind of discussion in schools.**

Yes, that is one of our goals. We also plan to collaborate with our students for finding good strategies of reaching younger audiences. I don't feel like an old person, but I already see that students are digital natives and are more skilled than I am. The conversation with them can be very educating. They bring exciting examples from different forums to our discussions. I don't have much time to be on Reddit or 9GAG but my students bring the examples, I get interested and I go there to check them out.

**In your presentation, you mentioned that IT knowledge is a bit esoteric or opaque. Do you think it is so even for young people who were born into the digital era?**

I think, sadly, it is so. They may feel confident in the field of social media content creation but when it comes to practical programming tasks, their courage seems to vanish. Math comes in and they feel like there are experts doing it for us and that it is hard to participate in it. There are groups of students who are programming, writing the codes, and not just analysing the codes, but there are not so many.