



# Changes in the user practices: the case of extreme nationalist users of SNS Rate

#### Dr. Andra Siibak

University of Tartu, Institute of Journalism and Communication Lossi 36, Tartu 50154 Estonia

Andra.Siibak@ut.ee

#### CHANGES IN THE USER PRACTICES

The role of social networking sites (SNS) to Estonian national security were first detected during the Bronze Night in April 2007 when various communities (e.g. Estonian Skinheads, Keep the homeland clean, etc) in the national-language based SNS rate.ee were used for spreading xenophobic messages, propagating hate speech and violence against the Russian minority. Content analysis of the user profiles (N=174), carried out some weeks after the Bronze Night indicated that many of the SNS users expressed extreme nationalistic views on the profiles by making use of nazi symbols, white supremacy acronyms and contravention of Russians (Pruul 2007).

Although there still are users on Rate who hold and exhibit extreme right wing views, it is presently much harder to detect their existence. The coding scheme used for carrying out the content analysis in 2007 was useless in spring 2011. Due to the changes made by the service provider after the Bronze Night events, many of the users with extremist views appear to be practicing a privacy tactic labelled social steganography i.e. "creating a message that can be read in one way by those who aren't in the know and read differently by those who are" (boyd 2010). The variety of these messages coming in the form of acronyms, symbols, videos, photos, abbreviations, etc has extended remarkably compared to the ones in use in 2007 and thus are often meaningful only to the members of the "audience evoked" (Ede & Lunsford 1984), not for the "imagined community" of SNS users at large (Marwick & boyd 2010). Hence, when targeting your opinions to the users with "specific cultural awareness" (boyd 2010) needed for interpreting the messages, the extreme right users of Rate are constructing an "ideal audience, who is often the mirror image of the user" (Marwick & boyd 2010: 7). The latter, however, could evoke possible problems and lead to unwanted consequences in terms of the security and stability of the state.

#### INTRODUCTION

In the context of the recent events of the Arab spring and the riots in London the role of social media in enabling the general public to spread information, organise events, recruit like-minded individuals, etc. has not gone unnoticed. Hence, numerous scholars have already explored the role social media and social networking sites played as broadcasting and logistical tools in the events which led to the Arab Spring [1,2,3] or the English riots [4, 5, 6, 7] and the Occupy movement. Furthermore, federal governments in several countries, e.g. in the UK and the United States, have released strategies which emphasise the potential role of social media in sharing extremist propaganda and promoting radicalization [8].

In the recent years international security forces have invested a lot of time, effort and finances in order to be able to monitor the traffic on social media. For instance, in 2009 CIA invested in Visible Technologies a software firm which enable them to monitor millions of posts on social networking sites [9]. Similar actions have also been taken by the UK Home Office who has been monitoring all the conversations on social networking sites and instant messenger since 2010 [10], and the agents of U.S. Department of Homeland Security who are allowed to create their own accounts on social media to monitor the traffic on these



platforms [11]. Although the main aim of the above-mentioned actions and strategies has been the fight against international terrorist organisations, the fact that social media is also actively used by various domestic extremist groups that promote radicalization has also been recognized in these documents [8].

Nevertheless, even though a variety of technologies and metrics are available in order to support such surveillance ambitions, analysing all the materials gathered still needs to be carried out by individual experts so as to "increase the 'so what?' value"[12]. Although such expert teams are always made up of specialists who possess both the critical thinking skills and "the insight and context" [12] for interpreting the data; their knowledge and methodologies are continuously tested. In fact, researchers suggest that due to the "context collapse" [13] on social media, the young users of such environments are particularly eager to engage in the practices of social steganography i.e. "creating a message that can be read in one way by those who aren't in the know and read differently by those who are" [14]. In other words, rather than targeting ones messages to the "imagined community" [13] of social media users at large, messages sent by the means of social steganography can only be meaningful to the members of the "audience evoked" [15] who has the "specific cultural awareness" [14] needed for interpreting the content. When used by the group of extremists, however, such a tactic could evoke possible problems and lead to unwanted consequences in terms of the security and stability of the state.

The aim of this paper is to refer to the changes of user practices which have occurred in the course of the last five years in the self-presentation strategies of extreme nationalist users on the Estonian SNS Rate who were very active in voicing their views and ideas at the time of the April Unrest in 2007.

In the first part of the paper I shall give a short overview referring to the importance of social media and social networking site Rate in particular, in the events which have come to be known as the April Unrest or the Bronze Night. In the second part of the paper, one case-study from April 2007 and the other from June 2011 about self-presentation of the extreme nationalist users on SNS Rate will be used as an example to illustrate the changes which have occurred in the social networking site Rate usage practices of such profile owners who hold extreme right-wing or nationalist ideas.

#### The role of SNS Rate in the events of April Unrest

Various authors [16, 17, 18, 19, 20] have explored and analysed the attack on the national information infrastructure in Estonia which has come to be known as the first Internet-war in history [17]. Although the authors of those reports have often given quite a detailed chronology of the events that acted as a trigger for the cyber-war, such articles have been mainly concentrated on portraying the timeline of the cyber-attack and the counter-defence issues surrounding it. However, to the knowledge of the author, none of the authors have tried to investigate the role social media played in triggering the course of events known as the Bronze Night or the April Unrest, i.e. the events which occurred on the streets of Tallinn after Estonian government's decision to re-locate the "Bronze Soldier", a Soviet era memorial to a WWII unknown Russian soldier. Hence, it its has been almost unacknowledged that during the events of April Unrest which were accompanied by a widespread vandalism and riots in the centre of Tallinn and left one dead, 57 injured and more than 300 individuals arrested [21], SNS Rate (<a href="www.rate.ee">www.rate.ee</a>) was actively used both by the ethnic Estonians and Russian-speaking individuals in producing and spreading the narratives of hatred and violence.

The communication spread in the forums and communities of Rate had an important role to play during the events of the April Unrest. Both the ethnic Estonians and the Russian minority made use of forums and communities to spread information about the events occurring on the streets of Tallinn but also for calling up

14 - 2 RTO-MP-HFM-201

people to take action. Furthermore, my unofficial discussions with Estonian government officials have revealed that the site was also used for finding people who would be willing to give financial support to the rioters. In fact, government officials had a right to consider the posts on the site as a case of terrorism financing.

The possible role of the communication apparent on site in facilitating the April Unrest was also recognised by the service provider. At the time of the unrest, the service provider of Rate launched on its main page a call which was targeted to its young users and tried to assure the youth to keep calm and not to succumb to provocations [22]. Although the representative of the service provider also declared that no technical filters or human moderators can be able to monitor and detect all the xenophobic and hate-provoking information spread by its users [22], they did take steps in trying to establish order on the site. For instance, at the time of the unrest, more than 200 moderators working on the site aimed to delete the accounts of users whose posts and comments contained hateful and violence-provoking messages [22]. Soon after the riots the service provider also deleted forums postings and closed down a number of communities where extreme nationalist views were spread. For example, three communities - Estonian Skinheads, Eesti Eest! (Eng. For Estonia!), and Hoia kodumaa puhtana! (Eng. Keep the Homeland Clean!) - which members had been most active in leading the discussions at the time of the unrest, were closed down completely [23]. In other words, despite the multitude of data available on the site, the service provider was quite successful in finding out and closing down unwanted accounts.

In the following section I use the findings of a content analysis of the profiles of extreme nationalist users on Rate, carried out two weeks after the April Unrest, to suggest some of the reasons why the deterrence work of the service provider was quite successful.

#### Usage practices of the extreme nationalist users of SNS Rate

In the year 2007 SNS Rate was by far the most popular social media platform in Estonia with more than 300 000 active users [23]. The site was most actively used by young people. According to the results of the survey "Youth and the Internet" which was carried out in 2007, 70 per cent of 11-18 year old students were users of Rate [24]. Young users of Rate were also most active in voicing their extreme nationalist world-views as the majority of the users who exhibited extreme nationalist views on their profiles were either teens or young adults [23].

Self-presentation strategies among extreme nationalist users

The overall profile features and applications offered on SNS Rate were similar to the ones on Facebook or Orkut. The users were free to choose the content and the exact wording for describing their interests and hobbies, as well as to include all the other personal information they saw fitting.

The content analysis of the profiles of extreme nationalist users on Rate (N=174) indicates that such users often named aspects related to extreme nationalism, xenophobia, hatred, violence, etc. in their Interests section of the profile. For instance, the analysis shows that 16-20 year old supporters of extreme nationalism had included on average 5.3 interests that could be connected to this ideology. Most popular theme represented in the Interest section was that of racism (N=290), followed by interest in oi! music (N=209) and xenophobia (N=135) [23]. On fewer occasions the users also referred to different ideological messages (n=63), historical events (N=36) and, - figures (N=21) as well as violence (N=43) as their interests [23]. In the majority of cases (N=448) the users mainly made use of concrete words, phrases and slogans (e.g. Heil Hitler!, White power worldwide, etc.) connected to their ideology to exhibit those particular interests. However, acronyms (e.g. WP, oi!, SS) and numbers (e.g. 14/88, 85) were also often included in the Interests section - 217 and 132 cases respectively.



Many of the users had also included different slogans, song lyrics and poems that propagated radical world views under the Additional Information section on their profiles [23]. In fact, the analysis of the content of the profiles from 2007 suggests that the extreme nationalist users on Rate mainly relied on text when constructing their messages. Although acronyms and secret number combinations could also be found from some of the profiles, these symbols used represented only a very tiny variety from the list possibilities. In fact, the analysis detected only seven different acronyms and six different number combinations to be used on the profiles [23]. Hence, in comparison to the secret "coded" messages, straight-forward hatred and violence provoking slogans, song lyrics of old war-songs or extracts from Mein Kampf could be found. The latter however, can be much more easily interpreted by the people without any specialists training, compared to the various acronyms and secret number combinations which do require specialist knowledge about the symbols of skinheads, neo-Nazis and other radical groups.

Much of the popularity of Rate at the time was also connected to the fact that the site offered its users a variety of opportunities for content creation, e.g. the users could upload photos or keep a blog, as well as to communicate with other users in different forums and communities. The combination of such features not only created an opportunity to communicate with new people and thus to find new friends, but also to get acquainted with people who would share one's interests and hobbies. Both of the aspects were also named as one of the main reasons why the youth had joined the site altogether - respectively by 55 per cent and 32 per cent of the young [25]. In order to find new acquaintances and meet with like-minded people many of the young also took part of forum discussions and joined various communities. In this context it is also important to note, that young people perceived one's membership in a community to be a form of self-expression [25]. In fact, the majority of the young (43 per cent) tended to believe that the step of becoming a member in a community should be considered as an opportunity to "show myself the way I am" [25]. At the same time communities were also viewed as resources for starting discussions on interesting topics (39 per cent), or for getting advice (25 per cent); but also as a means for networking activity – being together with existing friends, organizing events, etc. (22 per cent) and for sense of belonging (20 per cent) [25].

Considering the above, it is important to note, that in 2007 there were 119 communities on Rate that were connected to spreading xenophobic, racist and radical world-views, and 78 communities that were nationalist in their perspective [23]. The biggest number of users from our sample (N=34 in each) had joined a community called *Eestlane olen ja eestlaseks jään* (Eng. *I am an Estonian and will stay an Estonian*) and *Suht OI!* (Eng. *Quite OI!*). In fact, communities like the latter one, which were built around the common taste in music, were actually quite popular among the extreme nationalist users: 24 of them had joined a community named *Rock against Communism* and nine users also belonged to a community which consisted of fans of the first Estonian skinhead music group P.W.A. (Preserve White Aryans). Interest in white power skinhead bands and music is understandable as 25 of the users from our sample had also identified as members of a community *Estonian Skinheads*.

On the whole the analysis of profiles from 2007 reveals that the majority of the extreme nationalist users of SNS Rate had not yet totally grasped the idea that one's interactions on online platforms tend to be public-by-default and private-through-effort [26]. I suggest there might be two possible explanations to their rather care-free and open communication on the site. On the one hand, the young extreme nationalist users of Rate may seem to have fallen victim to the general illusion of anonymity young people tend to share on SNS, i.e. the young probably just did not expect strangers, and especially "nightmare readers" [13] like the police and government officials, to have any interest in their posts and profiles [27]. In other words, they failed to acknowledge the phenomenon of the internet omnopticon [28] where many watch many through various friendship ties or links. On the other hand, however, radicals and neo-Nazi groups in particular, have been noted to be very well aware of the potential of recruiting new members and spreading their ideological

14 - 4 RTO-MP-HFM-201

messages [29]. By being open and proud about one's beliefs and ideology could have also help to serve some of these causes especially at the time of the events of April Unrest.

#### Targeting one's ideal audience: secret codes from 2011

In the context where various governments and security forces have taken steps so as to "continue to closely monitor important role the internet and social networking sites play in advancing violent extremist narratives" [8], the radicals using these sites are also continuously improving their strategies. For instance, extremists and terrorists have been noted to adapt to new ways and to new technologies with incredible speed [29]. Extremist content is both shared on "darknets" - private encrypted networks - that are difficult to detect and to disrupt [30], but can also be spread on public social media platforms by the means of secret codes.

In order to operate on social media, i.e. in the environment of "context collapse" where a variety of different people are brought together, young people have been known to be skilled users of a privacy tactic named social steganography [14]. Although social steganographic messages are communicated to different audiences simultaneously they are meaningless to the audience at large as unlocking the meaning of that multi-layered message or post requires both recognizing multiple referents [26] and specific cultural awareness to provide the right interpretive lens [14]. When compiling such posts, young people have been found [31] to make use of song lyrics and quotes so as to target their messages to particular users who possess the interpretive lens needed to decode the message. Furthermore, "while some teens choose to hide in plain sight, others post encoded messages intended as visible displays of in-jokes or obscure referents" [26]. In either way, however, such practice can be characterized as being "privately public" [32], making connections to many people while being relatively private with regard to sharing personal details.

However, monitoring the profiles of extreme-nationalist users on Rate in June 2011 gives me a reason to suggest that the practices of social steganography have also been actively practiced by skinheads, neo-Nazis and other individuals with radical views. In fact, my analysis indicates that in five years time, SNS usage practices and self-presentation techniques of the users had changed so remarkably that the coding scheme used for the content analysis in 2007 had become totally useless in 2011. The biggest changes in this realm had to do with the enlarged variety of techniques and genres combined so as to indicate one's extreme nationalist views on the profiles.

Although many of the users continued to make use of written text to express their world-views, the text was sometimes used in unconventional manner. For instance, I could detect practices which could be regarded as an illustration of the padonki counter-culture, i.e. a sub-culture mostly among the Russian-speaking internet community that is characterised by erratic spelling and gratuitous use of profanity and obscene subjects (<a href="http://en.wikipedia.org/wiki/Padonki">http://en.wikipedia.org/wiki/Padonki</a>); and Leet-speak (also known as elect or 1337) which is a specialised form of symbolic writing where combinations of ASCII characters are used to replace Latinate letters (<a href="http://en.wikipedia.org/wiki/Leet">http://en.wikipedia.org/wiki/Leet</a>). Furthermore, on occasions examples of computer text symbols and computer text art were visible on the profiles (see Figure 1).



1488	14881488	1488 44.4	
1488	148814	881488	W.P.W.W.
1488	1488_		/′/′/,
1488_	1488	//	///
148814	8814881488	81488 ('(	WHITES~/'')
148814	1881488148	81488_\N	IUST FIGHT/
	1488	_1488\	FOR OUR.•′
	1488	1488	.\.RIGHTS!(
14881	4881488	1488	\ITS A_\
14881	4881488	_1488	\_W.A.R.,\

Figure 1: An example of computer text symbols on the profile

In addition to making use of different cultures of net-speak, the profile owners had also broadened the scale and genres of their posts. In addition to song lyrics, nationalist poems and various slogans, short fictions for instance about Adolf Hitler and personal diary entries were uploaded on the site under the Additional Information section. Furthermore, profile owners were also quite active in uploading different YouTube videos as well as various images representing symbols and other memorabilia, or historical figures and OI! groups on their profiles. Furthermore, in contrast to the previous findings a multitude of new acronyms and number combinations had been employed as secret codes. Considering the fact that according to the research by Michael Weiss [33] around 150 secret neo-Nazi codes have been found to be currently in use in Germany, the expansion of secret codes used by the Estonian neo-Nazis cannot be considered such a huge surprise.

Some of the communities e.g. Eesti Leegion (Eng. Estonian Legion), Eestlane olen ja eestlaseks jään! (Eng. I am an Estonian and will stay an Estonian!), and Hoiame oma kodumaa väärika ja puhtana! (Eng. Let's keep our homeland dignified and clean!), which had been most popular amongst the extreme nationalist users of Rate on 2007, had been closed down. Although there were some communities that could be regarded to spread nationalist or extreme right-wing world-views, the majority of such communities were closed for the general public. In other words, one needed to get acceptance from the "owner" of the community before being able to see and take part of its discussions. As the number of users in each of these nationalist or radical communities was small, it can be expected that skinheads and extreme nationalist users of Rate are making more active use of some other and more private online environments.

All of the above indicates that the extreme-nationalist users of Rate have not only broadened their scope in terms of strategies, but these strategies have clearly become more sophisticated and not that easily interpretable as the ones from 2007. The secret codes and messages the profile owners are exchanging can be grasped and understood only by the "ideal readers" [13] of their posts, i.e. their peers supporting the same world-views. In other words, the meanings behind the messages of social steganography tend to be posted to appeal and "speak" with the "the mirror-image of the user" [13] not the potentially limitless audience of social media. The latter claim can also be supported by the fact that while commenting each others' posts the extreme nationalist users were mainly making use of acronyms, number combinations and other secret codes the real meaning of which can only be grasped by the "ideal reader".

14 - 6 RTO-MP-HFM-201

#### CONCLUSION

Social media and SNS in particular have played a crucial role in facilitating the events of the April Unrest, the Arab Spring, London riots and the Occupy movement. Furthermore, social media platforms have also become frequently used tools not only in the hands of terrorists but also extreme nationalist users like Anders Behring Breivik who was responsible for Norway attacks in July 2011 [34]. All the above-mentioned events also refer to the fact that as social media environments "effectively *merge* the digital and the physical" into one we finally need the get accustomed to living in the conditions of "augmented reality" [4].

Terrorists and different radical groupings have been amongst the very first users of the electronic communication which later developed into the Internet [35]. Since then their presence on the Internet and more recently on various social media environments has been very active. Furthermore, these extremist groups and individuals with radical world-views have adapted quite quickly both to the changes occurring on the field of digital technologies but also to the changed social conditions brought along by the fact that numerous intelligence services and police forces are monitoring their actions.

The aim of the paper was to refer to the changes that have occurred in the user and self-presentation practices of extreme nationalist users of Estonian language-based SNS Rate from 2007 to 2011. The analysis of the user profiles indicates that in comparison to the results from 2007 the extreme nationalist users on Rate have started to use much more complex strategies for introducing their ideology. For instance, examples of Padonki and Leet-speak, that is, counter-culture versions of netspeak; and a privacy technique known as social steganography could be found on the profiles. Furthermore, compared to the acronyms and numbers used on the profiles in 2007, their variety had grown remarkably. All the above-mentioned changes in the user practices indicate that on social media were multiple audiences are blended into one [13], the profiles and posts made by the extreme nationalist users are mainly targeted to the members of their "ideal readers", i.e. their peers and those individuals who share and hence are able to interpret their world-views.

Social media and SNS have demonstrated their potential of being "liberation technologies" [36], however, we should not forget the fact that they also serve a potential of turning into a nasty "double-edged-sword". Hence, I agree with Kohlmann who has argued that governments and intelligence services need not only to develop their IT capacity to learn how to monitor the extremist activities in online environments, but they also need to continue developing their cultural and linguistic capacity for assessing the online content [37]. Still, as "total message control is both impossible and unwise" [38], national governments and intelligence services should invest more time and effort in composing and propagating counter-narratives which would serve as a part of the broader projects which aim to counter violence, hatred and xenophobia in the society.

### ACKNOWLEDGMENT

The preparation of this article was supported by the research grant no 8527 financed by Estonian Science Foundation and the target financed project SF0180017s07.

### **REFERENCES**

[1] Dellicastelli, C. (2011). Every Tool is a Weapon if you Hold it Right. The Role of Social Media in the Pro-Democratic Uprisings of the Arab Spring. *Journal of Digital Research and Publishing*: 52-60. Retrieved February, from

http://ses.library.usvd.edu.au/bitstream/2123/8137/1/DRPJournal 5pm S2 2011.pdf#page=29



- [2] Khondker, H. H. (2011). Role of New Media in the Arab Spring. Globalizations 8(5), 575-679.
- [3] Skinner, J. (2011). Social Media and Revolution: The Arab Spring and the Occupy Movement as Seen through Three Information Studies Paradigms. *Sprouts: Working Papers on Information Systems*, 11(169). http://sprouts.aisnet.org/11-169
- [4] Jurgenson, N. (2012). When Atoms Meet Bits: Social Media, the Mobile Web and Augmented Revolution. *Future Internet* 4, 83-91.
- [5] Demidov, O. (2012). Social Networks in the International and National Security. Security Index: A Russian Journal on International Security 18(1), 23-36.
- [6] Briggs, D. (2012). What we did when it happened: a timeline analysis of the social disorder in London, *Safer Communities* 11(1): 6 16.
- [7] Baker, S. A. (2012). From the Criminal Crowd to the "Mediated Crowd": the Impact of Social Media on the 2011 English Riots, *Safer Communities* 11(1): 40 49.
- [8] Empowering Local Partners to Prevent Violent Extremism in the United States (2011). Retrieved 22 February from <a href="http://www.whitehouse.gov/sites/default/files/empowering">http://www.whitehouse.gov/sites/default/files/empowering</a> local partners.pdf
- [9] Shachtman, N. (2009). Exclusive: U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets. *Wired Magazine*, 19. October. Retrieved 22 February from, <a href="http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/">http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/</a>
- [10] Espiner, T. (2009). U.K. To Monitor, Store All Social-Network Traffic? Retrieved 22 February, from <a href="http://news.cnet.com/8301-1009\_3-10199107-83.html">http://news.cnet.com/8301-1009\_3-10199107-83.html</a>
- [11] Triner, D. (2010). Privacy Impact Assessment for the Office of Operations Coordination and Planning. Publicly Available Social Media Monitoring and Situational Awareness Initiative. Department of Homeland Security. Retrieved 22 February, from <a href="http://www.dhs.gov/xlibrary/assets/privacy/privacy\_pia\_ops\_publiclyavailablesocialmedia.pdf">http://www.dhs.gov/xlibrary/assets/privacy/privacy\_pia\_ops\_publiclyavailablesocialmedia.pdf</a>
- [12] Naquin, D. (2007). Remarks by Doug Naquin. *CIRA Newsletter* 32(4): 3-9. Retrieved 22 February, from <a href="http://www.fas.org/irp/eprint/naquin.pdf">http://www.fas.org/irp/eprint/naquin.pdf</a>
- [13] Marwick, A.E. & boyd, d. (2010). I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience. *New Media & Society*, 13(1): 114-133.
- [14] boyd, d. (2010). Social Steganography: Learning to Hide in Plain Sight. *danah boyd's blog*, URL (accessed in January 2011) <a href="http://www.zephoria.org/thoughts/archives/2010/08/23/social-steganography-learning-to-hide-in-plain-sight.html">http://www.zephoria.org/thoughts/archives/2010/08/23/social-steganography-learning-to-hide-in-plain-sight.html</a>
- [15] Ede, L. & Lunsford, A. (1984). Audience Addressed/ Audience Invoked: the Role of Audience in Composition Theory and Pedagogy. College Composition and Communication 35(2): 155-171.
- [16] Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security* 4(2): 49-60.
- [17] Guadagno, R. E., Cialdini, R. B. & Evron ,G. (2010). Storming the Servers: A Social

14 - 8 RTO-MP-HFM-201

- Psychological Analysis of the First Internet War. *Cyberpsychology, Behavior, and Social Networking* 13(4): 447-453.
- [18] Goodman, W. (2010). Cyber Deterrence. Tougher in Theory than in Practice? *Strategic Studies Quarterly* 4(3). 102-135. Retrieved 23 February from, <a href="http://nsci-va.com/CyberReferenceLib/2010-09-Cyber%20DeterrenceTougher%20in%20Theory%20than%20in%20Practice.pdf">http://nsci-va.com/CyberReferenceLib/2010-09-Cyber%20DeterrenceTougher%20in%20Theory%20than%20in%20Practice.pdf</a>
- [19] Jenik, A. (2009). Cyberwar in Estonia and the Middle East. Network Security 4: 4-6.
- [20] Barletta, W. A. (2007). Cyberwar or Cyber-Terrorism: the attack on Estonia. In: Zichichi, A. & Ragaini, R. (eds.) (2007). *International seminar on nuclear war and planetary emergencies 38th session*. World Scientific Publishing, Co, 481-487.
- [21] Öine märul: üks surnu, 57 vigastatut, 99 lõhkumisjuhtu ja 300 kinnipeetut. (2007). *Postimees Online*, 27 April. Retrieved 22 February, from <a href="http://arter.postimees.ee/270407/esileht/siseuudised/257508">http://arter.postimees.ee/270407/esileht/siseuudised/257508</a> foto.php
- [22] Pino, K. (2007). EMT: Rate miks me seda ometi kinni ei pane? *Õhtuleht* 18.05. Retrieved 23 February from <a href="http://www.ohtuleht.ee/230332">http://www.ohtuleht.ee/230332</a>
- [23] Pruul, R. (2007). *Rahvusäärmuslus rate.ee profiilides*. Bakalaureusetöö. Tartu Ülikool, ajakirjanduse ja kommunikatsiooni instituut.
- [24] Kalmus, V., P. Pruulmann-Vengerfeldt, P. Runnel & A. Siibak. (2009). Mapping the terrain of "Generation C": Places and practices of online content creation among Estonian teenagers. *Journal of Computer-Mediated Communication*, Special Issue on *Young People, Mediated Discourse and Communication Technologies*, 14(4).
- [25] Siibak, A. (2010). Constructing masculinity on a social networking website. The case-study of visual self-presentations of young men on the profile images of SNS *Rate.ee*, *Young 18(4), 403-425*.
- [26] boyd, d. & A. Marwick. (2011, May 28). Social Steganography: Privacy in Networked Publics. *International Communication Association*. Boston, MA.
- [27] boyd, d. (2008). Taken out of context: American teen sociality in networked publics. Ph.D.
- [28] Jensen, J. L. (2010). The Internet Omnopticon Mutual Surveillance in Social Media. *Report. Internet Research 11.0: Sustainability, Participation, Action. Gothenburg Sweden,* 19-21 October 2010.
- [29] Extremist Groups Using Facebook, MySpace, YouTube to "recruit members". Retrieved 22 February, from
- $\frac{http://www.thefreelibrary.com/Extremist+groups+using+Facebook,+MySpace,+YouTube+to+\%27 recruit...-a0199283337}{20199283337}$
- [30] Dunn, J. E. (2011). Extremists are Tech Early Adopters, Counter-Terror Report Notes. Retrieved 22 February, from <a href="http://www.computerworlduk.com/news/security/3291197/extremists-are-tech-early-adopters-counter-terror-report-notes/">http://www.computerworlduk.com/news/security/3291197/extremists-are-tech-early-adopters-counter-terror-report-notes/</a>
- [31] Murumaa, M. & Siibak, A. (2011). Exploring the 'Nothing to Hide' Paradox: Estonian Teens Experiences and Perceptions About Privacy Online. In: Proceedings of the A Decade In Internet Time: OII



Symposium on the Dynamics of the Internet and Society, 21 - 24 September 2011, University of Oxford. pp. 1-18. URL (accessed in January 2012) http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1928498

- [32] Lange, P. G. (2008). Publicly Private and Privately Public: Social Networking on YouTube. *Journal of Computer-Mediated Communication*, 13, pp. 361–380.
- [33] The Truth About 88. New Book Reveals Secret Meaning of Neo-Nazi Codes. Retrieved 22 February, from http://www.spiegel.de/international/germany/0,1518,770820,00.html
- [34] Taylor, C. (2011). Norway Attacks: Suspect's Social Media Trail Examined. Retrieved 29 February from, <a href="http://mashable.com/2011/07/22/norway-shootings-suspects-social-media-trail-examined/">http://mashable.com/2011/07/22/norway-shootings-suspects-social-media-trail-examined/</a>
- [35] Gerstenfeld, P. B. (2003). Hate Online: A Content Analysis of Extremist Internet Sites. *Analysis of Social Issues and Public Policy* 3(1): 29-44.
- [36] Diamond, L. (2010). Liberation Technologies, The Journal of Democracy, 21(3): 69-82.
- [37] Kohlmann, E. (2006). The Real Online Terrorist Threat. Foreign Affairs, 85(5), 115-124.
- [38] Stevens, T. (2010). New Media and Counter-Narrative Strategies *Countering Violent Extremist Narratives* (pp. 112-123). The Hague: National Coordinator for Counterterrorism.

14 - 10 RTO-MP-HFM-201