2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Socially Engineered Commoners as Cyber Warriors – Estonian Future or Present?

Birgy Lorenz
Institute of Informatics
Tallinn University
Tallinn, Estonia
birgy.lorenz@tlu.ee

Kaido Kikkas
Institute of Informatics
Tallinn University
Tallinn, Estonia
kaido.kikkas@tlu.ee

Abstract: The goal of our paper is to find out the readiness in Estonia to raise awareness of cyber security-related social engineering, especially among common people. We suggest that the awareness and understanding of online social engineering can raise the Estonian defence potential to a new level. Future cyber attacks may complement server attacks with human engineering and spreading misinformation in order to create incentives for treason or mutiny against the decisions of the state. Social engineering of information and people is one way to wage modern information wars.

Estonia is probably closer than anyone else to a functioning e-society, so it is important to build it up as safely and trustworthy as possible, inform people about potential downsides and suggest solutions for them. Due to widespread adoption of various e-solutions, the Estonian situation of e-safety and awareness could be considered adequate, but it can also turn out to be a weakness. Trust in the e-government, e-police, e-tax office etc. can lead to complete trust in e-channels as a whole, in turn creating extensive dependence on them.

We have conducted a study involving schoolchildren and ICT students, as well as members of the Estonian Defence League Cyber Defence Unit (EDLCDU). The findings suggest a way to carry out related training programmes or campaigns. The recommendations are useful for coordinating the efforts of the four Ministries involved, addressing the crossroads of technical cyber security, social interaction, communication and education.

Keywords: *: cyber security; social engineering; education policy*

1. INTRODUCTION

Our hypothesis is that in the cyber war situation, when information is scarce and the circumstances are hard to understand, ordinary citizens (lay people) can turn against their government and critical services (e.g. public transport and infrastructure), carrying the conflict over from the cyberspace into actual space – but this kind of process can be largely prevented by proper policies as well as education.

Moreover, it is possible to turn the liability into an asset, using adequately trained and motivated lay people as a kind of "cyber militia" to complement the efforts of "regular forces" or cyber defence specialists. In Estonia, this has already been partially achieved in the form of the Estonian Defence League Cyber Defence Unit (EDLCDU) which was founded after the 2007 cyber-attacks after the Bronze Soldier riots [1].

We expand the term "cyber warfare" from politically-motivated attacks on systems (to conduct sabotage or espionage) to large-scale manipulation of information (media, government, hackers) and potential crowd control in this situation. We believe that understanding chain reactions in this area provides valuable information to governments acting in crises, SCADA (supervisory control and data acquisition) units and different Ministries whose responsibility should be raising awareness. Thus our goal is to find out the public stance on the implementation of cyber war-related training in elementary, secondary and higher education.

2. BACKGROUND

A. Similar Studies

The digital landscape has developed from the initial technological phenomenon into a complex and increasingly social one (social engineering, new applications and interpersonal trust), including new types of devices, applications and end-systems (e.g. iPads, Facebook, e-Banking, iPlayer, etc.), as well as network and infrastructure vulnerabilities (e.g. network attacks, failures and misconfiguration) [2]. Modern cyber-attacks have more to do with manipulating humans than ever [3].

The Information Technology education Model Curriculum still discusses whether cyber security should be a part of the programme or if it is something that is unique in the field [4]. For designers of security systems it is important to understand how users evaluate and make decisions regarding security [5]. Ordinary people do not think about the risks at home, why should they be better at work?

The Internet habits of adolescents have changed. Social behaviour, belonging and being a part of something is more important than ever [6]. Social engineering is considered a low-cost and effective form of attack because of the lack of awareness in this matter [7]. Some feel that social networking raises also the risk of automated social engineering, hijacking and phishing [8]. The weakest link is human behaviour [9], which has been largely missing from systematic analysis compared with other aspects of cyberspace [1].

B. The Changing World

Robert Theobald, an American futurist, has used the term "mind-quake" to denote a situation where an old dominant way of thinking is overridden by undeniable new understandings [11]. A good illustration in a recent context is provided by Rick Falkvinge (a Swedish IT entrepreneur), recalling the once well-established business of selling ice for cooling foodstuff during summertime and its subsequent fall after electric refrigerators became available [12].

A similar change of mentality occurred when Gutenberg introduced printing to Europe. It allowed people to spread knowledge and boost education. The Internet has done the same on an even larger scale – people are spreading the word and sharing materials etc. The Internet's main point is to spread, not to restrict, data sharing [13].

But as some kinds of data should not be accessible for everyone, it also leads to a possible way to manipulate people – one can feed them false information or sow distrust towards leaders or a currency etc. [14]. When this is done by governments to their own subjects, it is considered an internal affair (e.g. in Belarus or Syria). But when other governments or politically motivated groups intervene with other countries' politics by influencing the residents (e.g. Nashi [15]), it is much more likely to be considered as a psychological/cyber-attack or a case of social engineering – and if it happens repeatedly it can be considered to be a cyber-war.

Finally, there seems to be a growing need for two different terms for the current "cyber warfare" – one to denote cyber-attacks during military operations leading to a military objective (e.g. blinding enemy drones or radars) and another to reflect the emerging tendencies that also relate to cyber-attacks but use humans as a primary asset (but can produce similarly effective outcomes to straightforward military activity).

C. The Human Factor in Cyberwar

A definition of cyber war [16] states that:

- there should be consequences in real life;
- it is detectable afterwards;
- there are no persistent solutions that we can rely on;
- there are no limits to the physical distance;
- both sides (attacker and defender) have same rights and use same tools;
- whoever controls the opponent's resources controls the opponent.

In most of the current policies, the main priorities to be protected in the occurrence of a cyber-attack are either data or hardware – to detect the intrusion and regain control of, clean and patch the systems [17]. On the one hand, it is understandable; the government's main concern is to keep up critical services like finance, sustenance, medical assistance, transport, water and electricity, ICT services and public administration [18].

On the other hand, the role of patching the "human factor" has been seriously neglected. For example, playing with human thoughts and behaviour can incite devaluation panic (e.g. attempts to influence the Russian-speaking population in Estonia before the adoption of the euro in 2007) [19] or massive unrest (e.g. the Bronze Soldier affair in Estonia in 2007 [20] or similar events in Denmark in 2008 [21], the UK [22] or France [23]), as well as influence financial markets or incite large-scale protests (Middle-East, Egypt [24]). A recent example is the influx of malware using social engineering techniques after disasters like the Japan earthquake in 2011 [25].

D. Psychological and Sociological Factors

There are three ideas that contribute to the possibility of mass manipulation: we are all connected, tend to overreact and "with the right weather conditions, all Hell can break loose". So, the following points apply:

- In the age of social networking, "who knows who" has gained major importance. The concept of "six degrees of separation" refers to the idea that everyone is on average approximately six steps away. Nowadays we see it happening in real social networks [26]. For example, I know my country's political leader, who knows the President of the US, who knows everybody. So the steps can be even less numerous [27];
- Positive feedback loops are well known to describe the dynamics of change in biological evolution. Today, the same effects are seen on the net: a small disturbance launches several opinions from others and the result will be greatly amplified [28,29]. Sometimes it will not last long, but in cases of larger public interest [30,31] it can end up gathering to dance like Michael Jackson [32]. Essentially the same process worked for the Bronze Soldier riots or more currently the Arabian Spring, Occupy Wall Street [33] or the ongoing protests against ACTA [34];
- Nowadays the police consider weather conditions as one of the key elements to influence the risk of massive unrest. The threat is lower when it is too cold or too warm [35,36].

Kalev Leetaru, a computer scientist, has claimed that "pooling together the global tone of all news mentions of a country over time appears to accurately forecast its near–term stability, including predicting the revolutions in Egypt, Tunisia, and Libya, conflict in Serbia, and the stability of Saudi Arabia [37]".

Putting these three ideas together, we get an explosive mix. For example, Mr. Smith hears from a friend's friend that the Euro will be devalued in a few days. How would he act? When that information is fed to the public, how can the government be quicker and more reliable than the biased (as seen by many people) mass media or other Web 2.0 tools and social networks? Also (and perhaps most importantly), who is the enemy to blame?

E. Changes in Cyber-Warfare

Some would argue that, in recent years, the rapid development of technology has outrun the capability of governments to keep pace with it, while others would assume that Moore's Law is still valid [38]. The intervals between technology renewals have shortened – it is common to have a new smartphone every year and a new computer every two years [39]. Common people possess adequate (and rapidly evolving) computing power which cannot be sufficiently neutralised in cases of misuse or hijack. To make things worse, legislation lags far behind the situation and the processing queue of online crime-related cases is long and increasing [40-42].

All this makes detecting cyber incidents and forensics difficult; attackers evolve more quickly than defence [43,44]. Yet, manipulating people's mindsets can be even more devastating than getting unrestricted access to a service or server.

In general, the countries which have recently experienced some form of cyber conflict (e.g. Estonia or Russia) also tend to be more conscious in terms of related policies. The countries which have a strict "command line" (formal or informal) in either the government (e.g. Belarus or China) or a parallel structure (e.g. trade unions, CDL, diaspora, organised crime etc.) or the ones without strong dependence on ICT (e.g. some developing countries) are generally more resistant to cyber war [45].

F. The Situation in Estonia

"The Estonian way in cyber war issues is above all defence-oriented. Historically, Nordic Finno-Ugric tribes traditionally lived in peace with nature and neighbours. It's a lifestyle. At the same time, awareness against threats (cold climate, predators etc) has always been a normal part of life. This way, passively defending itself against threats, adjusts itself well to the Internet threats. It is important to notice and keep in mind that when Finno-Ugric people say "defence", it really is defence only – defending their lifestyle – and it is not including any deep hidden aggression or hidden agenda," says Anto Veldre (a cyber security specialist from Estonia).

In Estonia, raising the layperson's awareness in e-safety belongs to the domain of the Ministries of Education and Social Affairs, as well as Economy and Communication. However, it has recently also caught the attention of the Estonian Ministry of Defence, leading to the formation of the EDLCDU. Adults are usually trained by universities, voluntary trainers, media, workplaces and also schools (via children). It is still easier to train students and teachers by adapting school curricula – presuming that children will grow up to knowledgeable citizens or maybe even influence their parents and grandparents.

There is a Masters programme at the Tallinn University of Technology focusing on technical aspects of cyber security, yet no one is currently working on the lower stages of education [46]. There are some efforts supported by the EU (e.g. the InSafe programme) [47] as well the business sector programme "Be Included!" by the Look@World Foundation, that trained approximately 100,000 elderly people to use the national ID card and hence increase their security online [48]). There is the Cyber-Defence League which harbours both IT security experts and military personnel, focusing on educating its members. However, the National Defence curriculum sponsored by the Estonian Ministry of Defence does not currently focus on the layperson's cyber security awareness.

3. METHODS

We used triangulation with an interview and a survey to get better understanding of human behaviour and people's attitudes towards cyber war issues in their life:

- stage I – an interview with three cyber security experts, where we also got input to the stage II questionnaire from;
- stage II – the focus group study. We used the open source web application called Limesurvey. We collected 98 responses over two weeks;
- stage III – the results were analysed by five experts (two representing education, two ICT, one legislation), using the group analysis method.

Stage II focused on: students (42), 27 from secondary school, others from university (eight ICT related); ICT experts (25), six were EDLCDU-related; and other adults (31), 14 in education and two were EDLCDU-related. We used a survey with 37 questions divided into six sub-categories: general, government and cyberspace, cyber war means, ethics, incident response and background information. The data was collected using the Likert scale [49] and Q Methodology [50] rankings, plus open questions that were mainly used for clarification.

4. RESULTS

For background information we collected the participants' thoughts about understanding information from cyberspace. We found out that the most trusted channels they get information from are still traditional (TV, radio, newspaper – 58%). ICT specialists tend to also trust forums (12%), as do EDLCDU members (13%). EDLCDU members trust mailing lists (17%). Secondary school students (16%) are more open to online news, as are ICT specialists (11%). All participants trust academic texts (23%) more than any other media, including European (19%), local (16%), Northern (13%) and World (12%) news. It is interesting to note that even an informal chat with a friend (8%) is more trusted than official news channels from Russia (1%).

To understand what is perceived as cyber war and what is not, we described different scenarios and asked whether they are seen as such. The respondents seemed to consider it as something strictly related to online attacks, not real life. The term is still foggy but the main features chosen by respondents are: it happens online (63%), it is related to computers and the net (79%), it can be information distortion involving the government (65%), media (61%) and lay people (56%). Online piracy, massive unrest in the streets and rebellious activities on the net did not qualify.

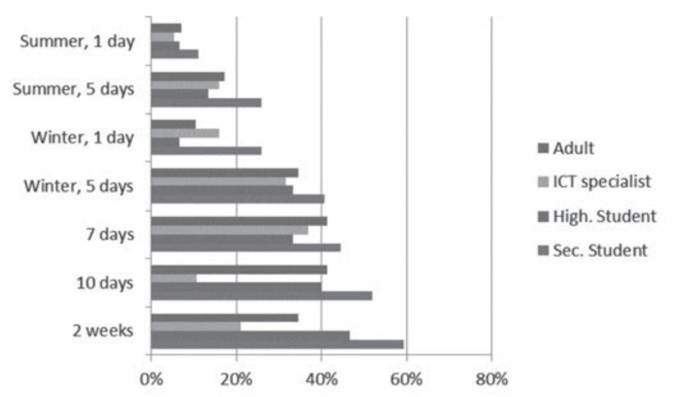
In the next section we focused on the questions of who should be held responsible for cyber war and how the government should manage the problem. We found that governments are perceived as primary participants (90%). In addition, they are also blamed for individual people's acts (44%), especially when the attack comes from that location (47%). Governments should have the option to ask for help from international committees (86%), use other rights under the law (61%) or defend themselves using cyber defence tools (86%), EDLCDU (55%) or even with the help of individual hackers (41%). People's understanding and knowledge of related legislation is weak; 66% did not feel there is any legislation in that area at all. Also, more than 80% of the ICT and EDLCDU respondents claim to not have enough legal support in these issues.

The most important thing that a government can do in a cyber war situation is to provide true, accurate and plentiful information. Massive unrest can be triggered when people find out that governments have manipulated information (61%) or restricted or filtered Internet usage (68%). People might understand if the government cuts some communication in that situation (75%) or gives informal groups special rights to regain control online (67%). The support for the EDLCDU and other supporting ICT cyber specialist groups is high (72%). The respondents would also like to have a government database of these specialists to ask for help from (77%).

For the third and fourth sub-categories we studied people's readiness to "go out to the streets" and possible chances to raise awareness in that area. Some interesting results were found among the answers to the question “When internet, mobile network, electricity is unstable, ATM does not work, workplaces/ schools are closed, when would you start rallying in the streets or online (if possible)?” (see Figure 1). 100% of EDLCDU respondents answered this question that they would not act in any way that will cause more panic than there already is.

The difference between summer and winter was introduced to check people”s interest towards more peaceful solutions (go to the beach, visit grandparents or take a vacation). In summer there is no constant need for electricity and homes are warm, unlike in winter where it can reach -20 degrees etc. However, when something happens in the winter it is much more problematic. The difference can also be seen in the number of days of system downtime. The critical point is at days 5 to 7 when people would start going out onto the streets, before attacking shops to steal food. After the 10th day, some groups would start to find other solutions. After two weeks other adults’ participation in rallying in the streets would also start to increase.

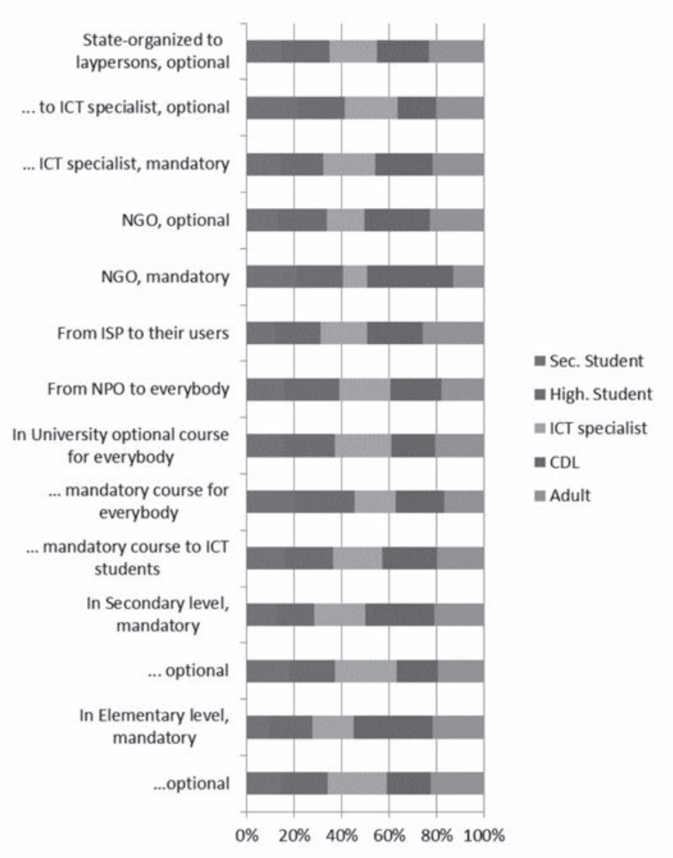
FIGURE 1. WHEN I WILL ACT?



In the ethics section we focused on awareness training – where, when and how should it be carried out. 29% preferred theoretical training while the majority (71%) wanted a practical, hands-on approach. Practical training was relatively unimportant for secondary level students (59%). According to the respondents, the possibility of receiving practical training in cyber defence should be available to lay people (64%), CDL members (86%), university students (86%), secondary school students (68%) and elementary level students (40%). There were also implications that the training should not involve playing cyber war games (77%); the solution lies in building special information centres (54%) and events (53%) where people could be trained (e.g. in ICT security or programming). The perceived levels and locations are shown in Figure 2.

This kind of awareness is deemed to be the responsibility of the Estonian Ministries (and their affiliates): Economy and Communication (91%), Defence (86%) and Education (49%). However, the Estonian reality is that awareness in this area relies rather on the Ministry of Social Affairs (mentioned by 15%), the Tiger Leap Foundation (responsible for ICT and innovative methods implementation in Estonian schools; 10%), the children’s welfare system (4%), and volunteers (17%). It was also interesting that 24% of respondents expect their ISP and 17% the mass media to protect and advise them in this area.

FIGURE 2. CYBER WAR-RELATED EDUCATION – WHERE AND WHEN?



5. DISCUSSION

The results were somewhat expected – the ICT people have heard of cyber war, others see it as related only to "cyberspace and servers". At the same time, the most crucial finding seems to be that both the lack of information and (even perceived) manipulation attempts from the government will raise unrest in society.

We also see a problem when the media presents news originating from "an independent research agency" and is believed to be reliable a priori – only a few people will search more information about the topic or think about how newspapers translate original texts or "lend" coverage to each other (making it similar to the children's "telephone game"). It is also noteworthy that all information originating from Russia is considered by far the least reliable (compared to the information from EU and the rest of the world). This can be at least partially explained by the fact that older generations learned to distrust everything Soviet (i.e. Russian) due to extensive (and often unreasonable) Communist propaganda during the occupation period, while the younger generations (especially the most active, Internet-savvy groups) developed almost the same level of distrust towards Russian information after the April 2007 riots.

Cyber war is in some ways like cyber bullying – it happens on the Internet and is often believed to be separate from real life. But as there are links between real-life bullying and cyber bullying, there are links between cyber war and real-life conflicts. When we see massive unrest in several countries, it has often started from discussions on the Internet where everybody can join – positive feedback takes place. It is easy to think that cyber incidents are related only to servers and systems, but it is important to see that these attacks are more and more related to information manipulation, lack of information and affecting people.

An interesting finding is the fact that 77% of the respondents would support the establishment of a central database of cyber defence specialists (the support was even seen among the EDLCDU and specialist groups). The idea is controversial at best, allowing any potential enemy to target a specific resource – and in case of success would compromise a large share of national cyber defence capability.

In Figure 1, we see children’s dependence on online needs and quick reactions to problems. While adults tend to wait before acting and are more patient, youngsters usually want quick and simple results and are not patient. This can be illustrated by two events in Estonian history spanning over more than a dozen years – defending the TV Tower in 1991 [51] and the Bronze Soldier removal affair in 2007 – when schoolchildren and young adults were manifest in the streets. Young adults and students also formed the core of anti-ACTA protesters on February 11, 2012 [52].

It is interesting to see that by the 10th day, ICT specialists will start searching for other ways than demonstration. This may be due to the awareness of the different war games and scenarios, which ICT specialists have already faced; resource exploration, management etc. will be of prime importance.

The positive feedback that amplifies the oscillation may become problematic in such a situation, e.g. one person screams on the Internet and others will start to scream, then soon everybody will scream louder and louder. In that case rallying in the streets will happen faster and will involve more people.

When something related to spamming or phishing happens, people do not want to get involved, so usually they will not do anything, even if they see illegal things happening. When they see something unusual on TV (e.g. taking over the station) they will either dismiss it as a joke or search for additional information on the Internet to get confirmation.

We also see responsibility issues between awareness trainers – while one of the four Ministries is active, providing awareness training in the e-safety area, others are still wondering what to do or not to do. There is also a problem with projects which are imported from outside of Estonia and do not fit into the society. More coordinated management is needed in this area.

By raising awareness of e-safety and cyber war issues, as well social engineering, less people will be affected by misleading information from any channels. Trusted and open government is also of vital importance. Awareness training should be carried out by specialists in that very area, not volunteers or different generic programmes. When people are treated respectfully by the government sharing valid information, there will be no or less rallying in the streets during the next crisis.

Education in cyber defence should be a part of national curricula at elementary, secondary and university levels. An interesting finding was that while people would like to have more practical skills to defend themselves, which is also seen as an opportunity to include NGO or ISP in the training process, government institutions were given preference over private enterprises. Establishment of information centres and the organisation of events like LAN-parties or training camps are also considered useful.

6. CONCLUSIONS

The respondents were willing to give up some rights during a crisis, but how it should be regulated perhaps needs an additional analysis. When the government needs help, they are happy to do that, but the request for assistance must be correct and well-addressed. The government must also consider that clear and abundant information during a crisis is very much appreciated.

The secondary level students and young adults were more willing to act in the streets and on the Internet when something negative occurs. Season and weather also play a role when considering the risk of public unrest. Due to the use of the Internet and social networking, simple events will get positive feedback (outburst) and they might create a snowball effect before calming down. These factors should be considered by SCADA specialists.

The responding experts also pointed out problems in the legislation and forensics area. On the one hand, there is a lack of awareness in that area; on the other hand there is a shortage of experts and funding to carry out these tasks, even when something serious happens. There is no official strategy and continuity yet to produce cyber security specialists.

The awareness training for common people should be a part of educational programmes in national curricula at secondary and university levels. It should be up to schools to decide how to execute it. The respondents also seemed to rely on government institutions to spread the "word", rather than trusting private enterprises to save the day. While the adults' training should be more practical, more theory is needed at the elementary level. Thus, we call for Estonian Ministries to further cooperate in raising cyber defence awareness among common people.

REFERENCES:

[1] K. Jõevere, (2011, Jan. 20) *Täna loodi Küberkaitseliit*, Eesti Päevaleht [onine] Avalilable: http://www.epl.ee/news/eesti/tana-loodi-kuberkaitseliit.d?id=51290517.

[2] A. Schaeffer-Filho et al *Future and Emerging Threats to Network Operation: A Quantitative Research Analysis*, Interim Report, Lancaster University, UK. Aug. 2011.

[3] B. Blunden, "Manufactured Consent and Cyberwar," in *LockDown Conference proceedings* University of Wisconsin-Madison, 2010.

[4] D. C. Rowe et al "The Role of Cyber-Security in Information Technology Education," in *ACM SIGITE 2011*, New York, USA, October 2011.

[5] B. West, "The Psychology of Security," *Communications of the ACM* Vol 51. No. 4 2008.

[6] R. Zheng et al "Effects of Motives for Internet Use, Aloneness, and Age Identity Gratifications on Online Social Behaviors and Social Support among Adolescents," in *Adolescent Online Social Communication and Behavior: Relationship Formation on the Internet*. Hershey, PA: IGI Global, Inc. 2008.

[7] T. Mataracioglu and S. Ozkan "User Awareness Mesaurment Through Social Engineering," in *Int. J. Managing Value and Supply Chains* 2010.

[8] M. Huber et al "Towards Automating Social Engineering Using Social Networking Sites," in *Computational Science and Engineering*, Vancouver BC. October 2009.

[9] J. R. C. Nurse et al "Trustworthy and Effective Communication of Cybersecurity Risks: A Review," *Socio-Technical Aspects in Security and Trust* (STAST), Nov. 2011.

[10] F. Stech et al "Scientometrics of Deception, Counter-deception, and Deception Detection in Cyber-space," in *PsychNology Journal* vol. 9 no.2 pp.79-122, 2011.

[11] R. Theobald, *The Rapids of Change: Social Entrepreneurship in Turbulent Times*. Knowledge Systems, Inc., Indianapolis, Indiana 1987, pp.82.

[12] R. Falkvinge, (2012, Feb. 4) *Nobody Asked for a Refrigerator Fee*. Falkvinge & Co on Infopolicy [online] Available: http://falkvinge.net/2012/02/04/nobody-asked-for-a-refrigerator-fee/.

[13] J. Naughton, "The internet: is it changing the way we think?" in *The Observer*, Aug. 2010 pp.20.

[14] T. R. Peltier, "Social Engineering: Concepts and Solutions," in *Auerbach Publications*, Nov. 2006.

[15] A. Raun, (2012, Feb. 7) *Lekkinud info: sajad našistid olid valmis Eestisse tulema*, Postimees. [online] Available: http://www.postimees.ee/731176/lekkinud-info-sajad-nasistid-olid-valmis-eestisse-tulema/.

[16] D. B. Farmer, *Do the Principles of War Apply to Cyber War?*, School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas 2010.

[17] G. V. Hulme, (2012 Jan. 4). *Government engineers actively plan for cyberwar*. CSOonline's Malware [online] Available: http://www.csoonline.com/article/697365/government-engineers-actively-plan-for-cyberwar.

[18] *Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta*, Nõukogu direktiiv 2011/114/EÜ, Euroopa Liidu Teataja pp 345/75.

[19] *Kapo: krooni devalveerimise paanika tekitajad teada* (2007, Dec. 13) Äripäev [online] Available: http://www.ap3.ee/?PublicationId=07d16439-8b41-4314-9fe6-e980bcaed68d.

[20] A. Lepa, "Eesti 2007. a. aprillirahutuste kajastamine Vene noorteorganisatsioon Na_i kodulehel" M.S. thesis, Dep. Phil. University of Tartu. Tartu, 2010.

[21] *Danish youths riot for 7th night, several arrested* (2008, Feb. 17) Reuters [online] Available: http://in.reuters.com/article/2008/02/17/idINIndia-31995320080217.

[22] *London riots: Looting and violence continues* (2011, Aug. 8) BBC News London [online] Available: http://www.bbc.co.uk/news/uk-england-london-14439970.

[23] J. Lichfield, (2010 Oct. 19). *France braces for riots as protests turn violent*, The Independent [online] Available: http://www.independent.co.uk/news/world/europe/france-braces-for-riots-as-protests-turn-violent-2110305.html.

[24] L. Wood, The Arabian Spring and its Impact on MENA Economies, *Research and Markets*, Dec 2011.

[25] M. Lennon, (2011, Mar. 11). *Massive Influx of Scams Surrounding Japan's Earthquake and Tsunami Expected*. Security Week [online] Available: http://www.securityweek.com/massive-influx-scams-surrounding-japans-earthquake-and-tsunami-expected.

[26] J. Ugander, et al "The Anatomy of the Facebook Social Graph," *Cornell University Library*, NY, US. 2011.

[27] L. Backstrom, et al, "Four Degrees of Separation," *Cornell University Library*, NY, US. 2011.

[28] T. Goetz, "Harnessing the Power of Feedback Loops," *Wired Magazine*, Jun. 2011.

[29] P. McRae, "Argumentum ad infinitum: The complex nature of echoing voices on the Internet," *Complexity Science and Educational Research (CSER)*, Vancouver, BC: University of British Columbia. 2007.

[30] K. Lewis, (2010, Feb 11) *The Network Effect* [online] Available: http://www.kieranlevis.com/the-network-effect/.

[31] L. Rosales, (2011, Oct 18) *Anatomy of a social media chain reaction – case study* [online] Available: http://agbeat.com/real-estate-technology-new-media/anatomy-of-a-social-media-chain-reaction-case-study/.

[32] D. Paap, (2009, Aug. 3) *Dance Tributes Around the World for the Dance Legend, Michael Jackson* [online] Available: http://movetheframe.wordpress.com/2009/08/03/dance-tributes-around-the-world-for-the-dance-legend-michael-jackson/.

[33] *Hundreds of Occupy Wall Street protesters arrested* (2011, Oct. 2) BBC News US&Canada [online] Available: http://www.bbc.co.uk/news/world-us-canada-15140671.

[34] *Acta: Europe braced for protests over anti-piracy treaty* (2012 Feb. 6) BBC News Technology [online] Available: http://www.bbc.co.uk/news/technology-16906086.

[35] E. G. Cohn, “Weather ans Crime,” *Brit. J. Criminol* vol 30 no. 1. 1990.

[36] P. Butke and S. Sheridan, “An Analysis of Relationships between Weather ans Aggressive Crime in Cleavland, Ohio,” Dep. Geography, Ken State Univerity, 2010.

[37] K. Leetaru, “Cultoromics 2.0: Forecasting large-scale human behaviour using news media tone in time and space,” *FM* Vol 16 no 9 2011.

[38] B. Schaller and R. Stough, “The Origin, Nature, and Implications of MOORE’S LAW,” *PUBP801*, Sept. 1996.

[39] K. Jaroslaw, “Civiliziting events ans chronology,” *Proceedings of the 2nd International Meeting A Revised Chronology and Alternative History*, Rüspe, Germany, June, 2001.

[40] *Politsei süüteoennetusliku tegevuse 2011. aasta plaan* [online] Available: http://www.politsei.ee/dotAsset/174500.pdf 2011.

[41] *Kuritegevus Eestis 2010*, Kriminaalpoliitika uuringud 15 [online] Available: http://www.just.ee/orb.aw/class=file/action=preview/id=54601/KuritegevusEestis2010_web.pdf 2010.

[42] *Kriminaalpoliitika arengusuunad aastani 2018* [online] Available: https://www.riigiteataja.ee/akt/13329831 2010.

[43] J. Boyd, “Information Warfare OODA loop,” in *Value Based Management* 2003.

[44] K. Saalbach, “Cyber war Methods ans Practice,” *LV Internet policy Universität Osnabrück* Jan 2011.

[45] A. Veldre, “E-ühiskond,” *Pühajärve suvekool* [online] Available: xyz.ee/2011-08-23-suvekool Aug. 2011.

[46] E. Tõugu, (2008 Jun. 17) *Kompetentsikeskus on, kus on kompetents?* Eesti Päevaleht [online] Available: http://www.epl.ee/news/melu/kompetentsikeskus-on-kus-on-kompetents.d?id=51133361.

[47] *About the project Targalt Internetis* (2010, Oct. 28) [online] Available: http://www.targaltinternetis.ee/projektist/?lang=en 2010.

[48] *Ole Kaasas! Eesmärk* (2011, Feb. 12) [online] Available: http://www.olekaasas.ee/eesmark/ 2011

[49] R. Kumar, *Research Methodology*, APH Publishing, 2005.

[50] Z. Todd, *Mixing methods in psychology: the integration of qualitative and practice*, Psychology Press Taylor ans Francis Group, 2004.

[51] *Saatuslikud tunnid teletornis?* (2006 Aug. 17) Maaleht [online] Available: http://www.levira.ee/dyna/site/696est.html.

[52] *Tartu ACTA vastaste protesti lõpukõne: Siim Tuisk* (2012, Feb. 11) Youtube [onlne] Available: http://www.youtube.com/watch?v=gDz8MAG4jj4.