AN EXPERIMENTAL CASE STUDY ANALYSIS ON CYBERBULLYING AWARENESS

Iulian F. POPA[1]

ABSTRACT

BROADLY KNOWN IN HUMAN HISTORY FOR ITS GREAT CONTRIBUTION TO THE DEVELOPMENT OF HUMAN KIND, THE INFORMATION AGE HAS BEEN CHANGING THE OVERALL SECURITY ENVIRONMENT TOO. COMPLEX AND LESS KNOWN THREATS, RISKS, AND VULNERABILITIES FOR BOTH NATIONAL AND INTERNATIONAL SECURITY EMERGE CONTINUOUSLY. THERE IS NO DOUBT THAT CYBERBULLYING POSES SERIOUS SECURITY THREATS NOWADAYS. THE PAPER AIMS TO FILL THE CURRENT GAP OF QUANTITATIVE RESEARCH ON ROMANIAN CITIZEN'S AWARENESS LEVEL REGARDING CYBERBULLYING. THE RAW DATA WERE COLLECTED BETWEEN 31st of JANUARY 2012 AND 1st OF MAY (2012) VIA AN ONLINE AVAILABLE SURVEY. THE POLLING SAMPLE CONSISTED OF 997 ELIGIBLE ROMANIAN CITIZENS WHO WERE INTERVIEWED ON VARIOUS CYBER SECURITY ISSUES USING CASI (COMPUTER-ASSISTED SELF INTERVIEW) METHOD. UPON PRELIMINARY SCREENING AND DATA PROCESSING, SOME OF THE RESULTS ARE STILL SURPRISING EVEN FOR THE AUTHOR.

KEYWORDS: CYBER SECURITY, CYBER VIOLENCE, CYBERBULLYING, NATIONAL SECURITY.

INTRODUCTION

The paper aims to fill the current gap of quantitative researches on Romanian citizen's awareness level regarding cyberbullying phenomena. The case of Romania has been selected for both illustrative and practical reasons. Between 2007 and 2013 several reports released to public by DIICOT[2] and SCCI[3] indicated a clear escalation of cyberbullying phenomena among online users. Using specific elements of CASI[4] method, a number of 1097

[1] Iulian F. POPA, M.A. is currently Ph.D. candidate in Cyber Security&Defense field at Babeș-Bolyai University, Cluj-Napoca (Romania). E-mail: ifp2@georgetown.edu.

[2] DIICOT is the official acronym for Directorate for Investigating Organized Crime and Terrorism – the only structure within the Romanian Public Ministry specialized in investigating and countering organized crime and terrorism acts. DIICOT carries out special investigations in cases of serious crimes as they are defined by Romanian Law No. 39/2003. *Look for more at* http://www.diicot.ro/images/documents/english%20presentation.pdf, accessed October, 27, 2013.

[3] SCCI is the acronym for Counter-Organized Cybercrime Service (known as Serviciul de Combatere a Criminalității Informatice din cadrul Poliției Române) it is the specialized Romanian Police department responsible for investigating and countering organized cybercrime. Look for more at http://www.efrauda.ro, accessed October, 27, 2013.

[4] CASI is the acronym for Computer-Assisted Self Interview.

respondents (polling sample[5]) were interviewed to collect specific information on their interaction and awareness level regarding cyberbullying phenomena. The targeted respondents were asked to answer a number of 9 factual, concise, and closed-ended (multiple choice, dichotomous, nominal-polytomous) questions regarding current cyber issues via an online survey available on Survey Monkey[6] platform.

1. METHODOLOGY DESCRIPTION

The current research is intended to be both an experimental case study based poll and structural semi-quantitative analysis on the cyber issue presented below. The standard polling sample consisted of 997 previously selected people which were formally invited to fill-up an online survey if the eligibility requirements set forth were successfully met. In order to adequately verify the correlation between theoretical aspects and answers given by the polling sample, the interaction between the researcher and the respondents was formal and distant from the very beginning. All those interviewed stated they have at least basic ICT skills and knowledge beforehand. No written guidelines were provided and everyone verbally agreed on any personal data storage for further use.

Two out of the nine questions (namely question no. 2 and no. 4) were allocated for filtering purposes. Thus 10 out of 1097 respondents did not meet the minimum requirements for interviewing and their answers were excluded from the interpretation. The minimum condition for participating in the survey was given by the age and educational level at the time of the interview. Hence the answers given by the respondents under 18 years old and those given by respondents with secondary education/training only were excluded as being not eligible. Depending on the specificity of respondents age groups for the entire population, positive and/or negative correction factors were applied when needed.

2. Analysis Purpose

The purpose of the current analysis relies on the stringent need for accurate understanding of Romanians cyberbullying awareness level. This research is not intended to be a major sociological approach, but a custom analysis useful for future research on the current topic.

3. Analysis Objective

The information collected via the survey are designed to confirm or refute the validity of the assumptions expressed in detail prior the current analytic approach.

4. Initial Hypotheses

From the outset it should be noted that the initial hypotheses (referred bellow as *research hypotheses*) were empirically formulated to validate or refute the author's theoretical ascertainments established prior to this analysis. In short, the hypotheses are:

Hypothesis no. 1: The cyberbullying perception is broader and more significant in case of women.

Hypothesis no. 2: The way users interact within cyberspace it is similar to real-life interpersonal interaction[7].

Hypothesis no. 3: Complex and less known security challenges emerge continuously. Therefore enhancing overall cyber security requires new public private cooperation

[5] *Look for more in* Paul J. Lavrakas, Encyclopedia of Survey Research Methods (SAGE Publications, Inc.: Thousand Oaks, CA , 2008). doi: http://dx.doi.org/10.4135/978141296394, accessed October, 27, 2013.
[6] Look for more at http://www.surveymonkey.com, accessed October, 27, 2013.
[7] George Friedman. *The Next 100 Years: A Forecast for the 21st Century* (London: Doubleday, 2009), 60-64.

approaches as most of cyber threats to critical infrastructures and/or endpoints are constantly expanding, being more pervasive.

Hypothesis no. 4: In term of cyber governance, the cyberspace is poorly regulated. Moreover, cyber security has become one of the most pressing economic challenges.

Hypothesis no. 5: The threat of cyber terrorism can't the neglected, but it is unlikely to occur on a large scale during next years.

5. Data Collection Approach

The sample consists of 997 eligible Romanian citizens residing in Romania at the time of the poll. To test and improve the general specificity of the survey form, a preliminary pre-testing pilot survey consisting of 21 respondents was used prior to final raw data collection. Any data collected during pre-testing were not taken into consideration and were not analyzed afterwards. Following pre-testing sessions, the question no. 3 was adjusted and modified to its current version (*see figure 3)*. As a conclusive remark, the survey form was designed to collect data on the respondents educational attainment; age; type of academic and/or professional daily activities; comprehension level of cyber security language; and past individual cyberbullying incidents.

6. Additional information

In terms of general methodology, the current analysis belongs to the group of experimental methods of study and quantitative research. The initial data collection and subsequent data analysis were performed according to the original research plan. From a polling perspective the survey form was especially designed for a sample size of approximate 1000 respondents. Thus the confidence interval is estimated to +/-3% or 19 times out of 20 which means a 95% confidence level. For practical purpose, the number of questions was limited to 9 since a larger number of questions would not have changed significantly the final results. The raw data collection was carried out between 31st of January (2012) and 1st of May (2012).

7. Raw Results

Table 1. Question no. 1: Gender selection

Question no. 1 – Please select your gender	
Gender	**Response percent**
man	50.0%
woman	50.0%

Table 2. Question no. 2: Age selection

Question no. 2 – Please select your age	
Years	**Response percent**
Under 18	0.0%
18-25	69.0%
25-45	27.0%
Over 45	4.0%

Table 3. – Question 3: Working field selection.

Question no. 3 – Where do you work?	
Place of work	**Response percent**
Public administration	15.3%
Security and defense	7.1%
NGOs, think-thanks, journalism, academia	17.3%
None of the above but I have basic security and defense knowledge	17.3%
None of the above	45.9

Table 4. Question 4: Educational level selection.

Question no. 4 – Please select your educational level	
Education level	**Response percent**
Primary school	0.0%
Middle school	1.0%
High school	22.2%
Bachelor degree	47.5%
Master degree	23.2%
Doctoral or post-doc degree	6.1%

Table 5. Question 5: Have you ever experienced any forms of cyberbullying?

Question no. 5 – Have you ever experienced any forms of cyberbullying?	
Answer	**Response percent**
Yes	38.8%
No	45.9%
Don’t know/No answer	15.3%

Table 6. Question 6: Do you think that cyberbullying within cyberspace is normal and/or usual?

Question no. 6 – Do you think that cyberbullying within cyberspace is normal and/or usual?	
Answer	**Response percent**
Yes	71.4%
No	17.3%
Don’t know/No answer	11.2%

Table 7. Question 7: Which threats are most common within cyberspace?

Question 7: Which threats are most common within cyberspace?	
Answer	**Response percent**
Hate speech	53.1%
Psychological aggresion	27.6%
Cybercrime (data theft, scams, phishing)	77.6%
Cyber terrorism	20.4%
Don’t know/No answer	5.1%

Table 8. Question 8: Who do you think is responsible for cyberbullying and/or cyber threats?

Question 8: Who do you think is responsible for cyberbullying and/or cyber threats?	
Answer	**Response percent**
Common online user	63.8%
Cyber terrorists	22.3%
Hackers or hacktivists	58.5%
State actors	22.3%
Don't know/No answer	6.4%

Table 9 – Question 9: What is cyberbullying in your opinion?

Question 9: What is cyberbullying in your opinion?	
Answer	**Response percent**
An easy way to generate fear/panic among users	26.6%
A crime	41.5%
A modern warfare tool	26.6%
Don't know/No answer	5.3%

8. Results precision

As the current analysis complexity level is medium, the results collected and disseminated are experimental and predictive in essence. As the author recommends, the results from below should be used only for similar approaches.

Data Dissemination and Conclusions

As a conclusive remark, the cyberbullying awareness level must be substantially improved among Romanian citizens in the next years. Despite actual criticism, I strongly believe that public private cooperation based on confidence, efficient information sharing, mutual trust, and transparency can effectively enhance the overall cyber security culture.

Following the initial raw data collection and the subsequent analysis of the answers given by the respondents, the following conclusions come out:

a. considering the corroborated answers given by the respondents to question no. 1, no. 5, no. 6, no. 7, and no. 9 it follows that the hypothesis no. 1 according to which *the cyberbullying perception is broader and more significant in case of women* is false. Very similar cyberbullying perception and/or awareness level was remarked in case of men as the distribution of awareness level is divided to ~ 48% (in case of women) and ~52% (in case of men) within the analyzed sample. The confidence interval was estimated to +/-3%.
b. both the users' age and their degree of interaction with the cyberspace cannot be considered decisive factors for the users' awareness level of cyberbullying phenomena; 77.6% of respondents (68% of those aged between 18-25 years, 89.9% of those aged 45-45 years, and 74.9% of those aged over 45 years) correctly assessed cyberbullying phenomena;
c. the cybercrime phenomena continuously expand and emerge, posing serious threats to international/national security and individual safety as well *(see figure 6*); as it has been accurately assumed previously that cyberspace appears to be a poorly regulated medium in terms of governance *(see figures 5, 6, 7, and 8)*, the hypothesis according to which the users' behavior within cyberspace is little regulated – being somehow similar to real-life interpersonal interaction, is true; consequently the hypotheses no. 2 and no. 4 are valid;

d. both academic and professional background decisively influence the users' awareness level regarding risks, vulnerabilities, and threats to cyber security; 91.1% of respondents holding at least one academic degree correctly assessed the potential of cyber threats to national security (*see figures 7 and 8)*;
e. 20.4% of respondents acknowledged the threat posed by the cyber terrorism *(see figure 7);* therefore the hypothesis no. 5 is partially valid;
f. 71.4% of respondents (regardless academic and/or professional background!) assessed cyberspace as being an environment characterized by substantial levels of violence and/or aggression (*see figure 6)*; therefore the hypothesis no. 3 is valid.

REFERENCES

1. Counter-Organized Cybercrime Service. http://www.efrauda.ro.
2. Directorate for Investigating Organized Crime and Terrorism. *Presentation.* http://www.diicot.ro/images/documents/english%20presentation.pdf.
3. Friedman, George. *The Next 100 Years: A Forecast for the 21st Century*. London: Doubleday, 2009.
4. Lavrakas, Paul J. *Encyclopedia of Survey Research Methods*. Thousand Oaks, CA: SAGE Publications, Inc., 2008. doi: http://dx.doi.org/10.4135/978141296394.
5. Survey Monkey. http://www.surveymonkey.com.