

Cyberspace – Awareness of Vulnerabilities of the Technology Enabled Communication Environment

Demush Bajrami

South East European University, Faculty of Languages Cultures and Communication, Republic of North Macedonia
d.bajrami@seeu.edu.mk

Zamir Dika

South East European University, Faculty of Contemporary Sciences and Technologies, Republic of North Macedonia
z.dika@seeu.edu.mk

Arafat Shabani

South East European University, Faculty of Languages Cultures and Communication, Republic of North Macedonia
a.shabani@seeu.edu.mk

Neroida Selimi

South East European University, Faculty of Languages Cultures and Communication, Republic of North Macedonia
neroida.selimi@seeu.edu.mk

Technology usage and development has created a new environment of communication – cyberspace. From the moment we have exchanged information by using technology, we are part of it. But are we aware of the benefits and loss we may be exposed to while being part of it? Are we aware of the security and safety measurements we can apply? This paper tackles the awareness of cyberspace vulnerabilities in Generation Y and Z, in Pollog region¹ of the Republic of North Macedonia. In this paper we have firstly analysed the researchers views for the cyberspace, defining the advantages and disadvantages of it. Then we have analysed cases of cyberspace regulations, as a prerequisite for the research conducted, in the specific ‘regional’ context. We have used the quantitative design to assess the awareness, using closed ended questionnaires, focusing on the generation (Y and Z) outcomes; the usage of the social media – as a medium exposed to risk; as well and the forms of experiencing cyberattacks; and the knowledge about the tools for security and safety in cyberspace. Even though, in this paper, the limitation is that the data are related with the regional context in one country, and it was difficult to find similar research approaches to compare outcomes with, the conclusions about the level of knowledge about the cyberspace, experience of cybersecurity on social media usage and the awareness about the ways of security and safety, are important for the scholars and other stakeholders and participants in designing the information secure environment.

Keywords: Cyberspace, vulnerability, security, safety, awareness

1 Introduction

Being part of cyberspace is inevitable. Why? Because from the moment we own and use a smart gadget, being it a smartwatch, smartphone, tablet, personal computer, laptop, or any other device that enables communication through network, we are part of the cyberspace. We call and send messages to friends and family, we exchange information with our co-workers, we work on team projects online without the

¹ https://en.wikipedia.org/wiki/Pollog_Statistical_Region

need of being present at the time and place, as well as other information exchanges enabled by technology development are executed in cyberspace. One of the earliest definitions of cyberspace: “an infinite artificial world where humans navigate in information-based space” [1]. The technology has changed drastically from its early years, but, in cyberspace case, this definition is still valid.

Cyberspace importance and usability emerges from its various features, among others including digitalization and availability of information, social networking, and entertainment [2]. These features formed a cyberspace with various advantages and disadvantages. Even though the advantages are numerous: connections between people worldwide instantly, information flow, communication channels, socialization, etc.; the disadvantages follow: leakage of sensitive information, cyberbullying, hacker attacks, identity theft, development of medical conditions, etc. [3]. Scholars are intensively working and proposing models to enable a secure and safe presence in cyberspace, following the newest challenges brought by Big Data and Internet of Things. Due to the complexity of offered models, tools and solutions for a secure cyberspace, we have focused our work on the awareness of the vulnerabilities in the local context within a typical upper-middle-income country, such as North Macedonia [13]. We are bringing the awareness based on their knowledge upon the protection measurements in the cyberspace, results that could help scholars to refine the proposed solutions. This paper contains the conducted analysis on this question by sampling a group of participants of two generations (Generation Y and Generation Z) in Pollog region of Republic of North Macedonia.

2 Secondary research

The term “cyberspace” initially was not linked to technology, but it was used as a tool to define space management [4]. It was firstly used in visual arts in 1960s, by Danish artist Susanne Using and architect Carsten Hoff, for their creations, which were using open systems adaptable to human movement and behaviour of new materials.

Afterwards, cyberspace has continued to be used as a term in philosophy, art, geography and communication. All the mentioned categories accompany cyberspace with definitions in which it contributes to them.

Its latest definition is: “*Cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and the electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share, and extract, use, eliminate information and disrupt physical resources*” [5]. It includes [6]:

- technology and telecommunication devices which enable connection and communication of system networks (SCADA devices, smartphones/tablets, computers, servers, etc.);
- computer systems and software which enable the domain's basic operational functioning and connectivity;
- computer systems networks;
- internal and external connection networks of the computer systems;
- the access nodes of users and intermediaries routing nodes;
- constituent data.

2.1 Cyberspace vs. internet

The definition of cyberspace makes it a harder to distinguish from the Internet. In most of the cases, both cyberspace and the Internet are seen as the same thing. This is common because of the interrelation they have. In the other hand, they are also seen as totally different.

Internet is a network of global networks created by linking smaller networks to computers and servers that use Internet Protocol suite (TCP/IP) [7]. Internet exists physically. It is made of computers, servers, cables, routers, etc. Cyberspace has derived from Internet as the “virtual” computer world in which the

interaction between network participants is made possible, and mainly represents the information through the internet.

2.2 Advantages and disadvantages of cyberspace

Although the cyberspace is known to be one of the greatest achievements in the internet technology that facilitates life and the virtual communication between people, it has also arisen concerns that are increasing with the same intensity as it is developing further.

Below are listed the main advantages and disadvantages of cyberspace, starting with the advantages that include:

- quick and easy access to huge amount of data and information;
- opportunities of communication;
- entertaining purposes including movies, music, sports, online gaming and others.

Whereas the disadvantages include:

- significant reduction of privacy and misuse of personal and other information;
- development of cyber-crime including cyber theft, cyber bullying, child pornography and similar;
- un-supervised access of children in the internet world leading to violent online gaming, bullying and other serious psychological effects;
- easy access of different predators to children and young victims.

2.3 Cyberspace regulations

The arising disadvantages and misuse of cyberspace brought the need of creating regulations with the purpose of ensuring cyber-safety and cyber-security. Because cyberspace is a global virtual reality, different regulations apply to different part of the world. There are laws and regulations which are trying to “regulate” this delicate topic, and most advanced are in United States, including most recent one, such as: Cybersecurity Information Sharing Act (CISA); Cybersecurity Enhancement Act of 2014; Federal Data Breach Notification Act of 2015; and National Cybersecurity Protection Advancement Act of 2015. These are followed by State Laws and the Cyber Security Laws of New York. In the European Union there is a Directive on Security of network and information systems (NIs Directive), as a first piece of the legislation on cybersecurity in EU, as well as the newly approved EU Cybersecurity Act to support and strengthen the initiatives of the Agency for Cybersecurity. Laws and regulations may differ on country basis. Cyberspace laws and regulations protect from cyber-attacks, leakage, misdirection and damage of information, which includes identity theft, accounts hacking, sensitive information publishing, and others.

There are three main forms of regulations according to Ofcom [8]: direct regulation, co-regulation, self-regulation. Direct regulation is when the statutory body is empowered by law to create, maintain, monitor, and enforce its own regulations. Co-regulation is when the statutory body in collaboration with the relevant industry creates, maintains and monitors regulations, with the ability to intervene where necessary. Self-regulation is when a group of firms/individuals exert control over their own membership and behaviour.

Except for the above stated laws and regulations, there are developed several other alternative solutions which ensure privacy to individuals, such as anti-viruses, firewalls, intrusion detection systems, different forms of verification and authentication, operating system securities, trainings, etc.

3 Research questions

Our aim for conducting this research is to “measure” the awareness of cyberspace users on the vulnerabilities of it, in the Pollog region.

The main question expands further on several issues, such as:

- awareness of being part of cyberspace;
- the differentiation between cyberspace and Internet;
- cybercrime;
- awareness on available protection measurements;
- usage of the available protection measurements;
- authorities in charge to fight cybercrime;
- procedure of reporting cybercrime.

4 Research methodology

The research is being conducted by using the quantitative methodology. Quantitative methodology is defined as analysis and testing of a theory or hypothesis upon numerical data with usage of statistical, mathematical, or computational techniques [9]. Quantitative methodology applies to this research in collation and analysis of data from distributed questionnaires.

The quantitative design used in this research is descriptive. The aim of the distributed questionnaires is to gather information about the current knowledge of participants in the cyberspace of its vulnerabilities, and prevention measurements. The gathered data output results which further describe the current situation, awareness, and knowledge of the target group upon the research topic.

4.1 Target group

Target group for this research is made of two generations which are noted as the generic users of cyberspace: Generation Z and Generation Y [10]. The target group is demographically sampled from Pollog region of Republic of North Macedonia. Generation Z [11] are considered the individuals born from mid-1990s until mid-2000s. This generation interacts and uses the technology since a young age. Generation Y [12], or else known as the Millennials, are the individuals born from early 1980s until mid-1990s. This generation is considered as transitional because it starts in the era when technology started to develop and was in the development phase, and continues in the “technology era”, where technology is in fast development and applied in every sector.

4.2 Data collation

The research data is gathered through questionnaire distribution to the target group via email and social media. The questionnaire is created online by using Google Forms. It consists of close ended questions. The questionnaire collects information of age of the participants; gender; knowledge upon cyberspace; differentiation between cyberspace and Internet; Internet usage; social media usage; experience of cyberattacks; resolving cyberattacks; knowledge upon existence of security and safety tools for cyberspace; usage of security and safety tools while in cyberspace.

The questionnaire is filled anonymously by 397 individuals, who are using internet actively, from 450 distributed questionnaires. Data gathered is further analysed and mapped graphically for visual comparison and result distribution.

5 Results and discussion

The results emerged from data collection stated the following regarding research questions and aim:

Generations’ outcome: the question determining in which generation do the participants belong relates to their current stated age. From the overall target group, 67% of the participants in the survey are Generation Y, the other 33% are Generation Z.

Knowledge upon cyberspace: next section of the questionnaire tackles familiarity with the meaning of cyberspace by the participants. Most of the participants, 48% of them have understanding about the

cyberspace. By generations, the Generation Z dominates with 65% of them having identified the cyberspace meaning, while 48% of Generation Y respondents have declared that they have understanding about Cyberspace. The rest of the participants, 52%, have not heard about the term of cyberspace at all.

Internet usage: the purpose of Internet usage and how much time daily is spent on it, is seen through the data collected from this question. From the participants, on the question of the purpose of use of internet, measured by Lychard scale, is as follows: 48% of the time is used for social media, 17% are used for research/ work/ school, 15% use it for entertainment, 11% of time is used for professional development (tutorials, reading, etc.), and 9% is used for other purposes (Figure 1). By the generations, in Figure 2 is presented the usage by purpose. It can be noticed that generation Z are using more social media and entertainment, and generation Y are advancing in the search and professional usage of internet. Most of the participants, being it 45% use Internet for more than 4 hours daily, 26% use it 3 to 4 hours daily, 23% use it 2 to 3 hours daily, 6% use it 1 to 2 hours daily, and 2% using it less than 1 hour daily.

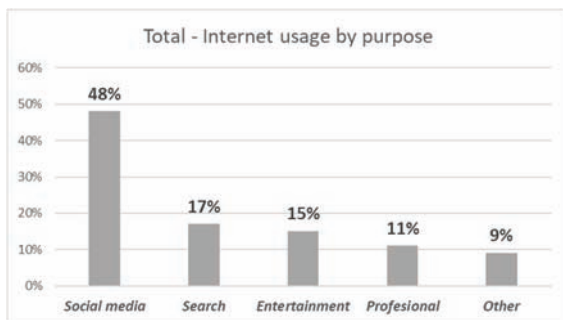


Figure 1. Internet usage by purpose

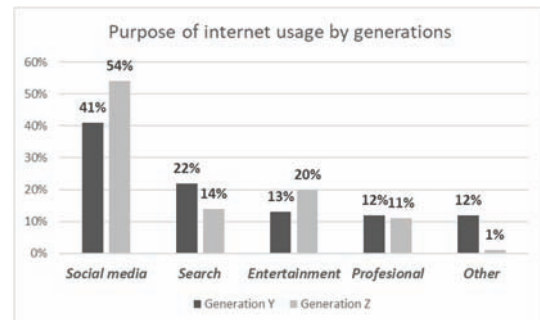


Figure 2. Internet usage by generations

Social media usage: this part of the questionnaire collects the data about the daily average time the participants use social media and for what purpose, in case when they have an account. Only 9% of the participants did not have social media accounts. From them, 43% of the participants use the social media more than 3 hours daily, 20% use it 2 to 3 hours daily, and the rest, 35%, use it from 1 to 2 hours daily. In Figure 3, these data are presented by the generations. Social media is mostly used for communication (64% of the participants), 17% using it for entertainment, and 10% using social media professionally related, while others have using it for other purposes. The purpose of social media usage by generations

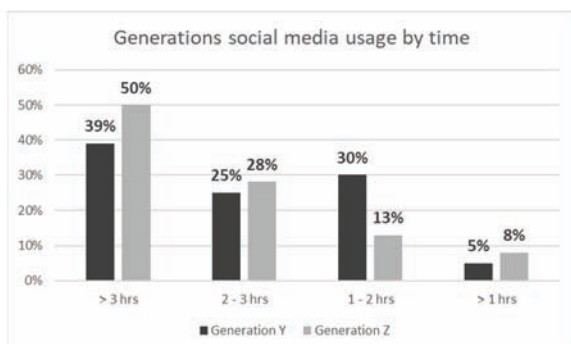


Figure 4. Social media usage by time and generations

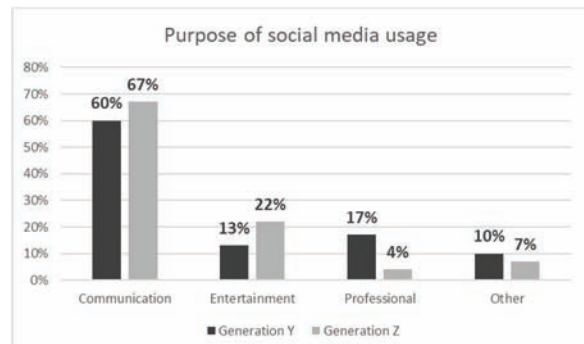


Figure 3. Purpose of social media usage by generations

is presented in Figure 4. While both generations are using social media for communication purposes, it

can be verified that the generation Y is using it more for professional purposes, while the generation Z for entertainment.

Experience of cyberattacks: being it a hacked social media account, hacked credit card, misuse of your personal information through Internet, identity theft, etc. from the overall number of the participants, only 38% have experienced them. From those experienced forms of cyberattacks, 66% have experienced cyberattacks in the form of hacked social media accounts, 16% of them have experienced misuse of their personal information through Internet, and 18% of them have experienced identity theft. The experience from cyberattacks by generations divide is presented in the Figure 5. The generation Y is more vulnerable to personal information misuse and the identity theft, while generation Z are facing more social media accounts attacks.

Resolving cyberattacks: this part of the questionnaire applies to the participants who have experienced cyberattack. The only way they have resolved cyberattacks is through reporting the profiles hacked and misusing their personal information.

Knowledge upon existence of security and safety tools for cyberspace: there are plenty of measurements developed to protect from cyberattacks and this question gathers data about the knowledge of our targeted group upon them. Participants are aware of existence of security and safety tools for cyberspace, mainly of antiviruses (100%), anti-malware (20%), and firewalls (7%). In the Figure 6 the awareness about the main security and safety tools for cyberspace are presented by the generation divide. It can be seen that the generation Y are more aware about the anti-malware and firewalls tools, while generation Z are less aware about the technology “vocabulary” and the technologies behind the security and safety tools.

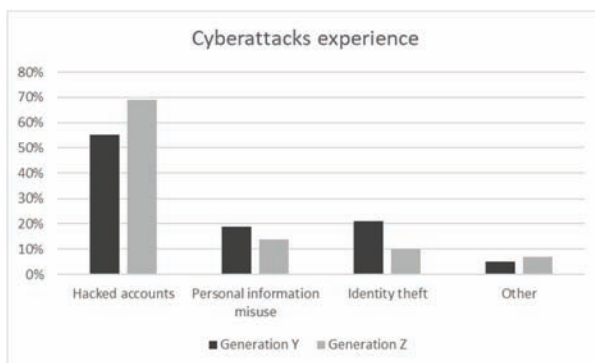


Figure 6. Cyberattack experience

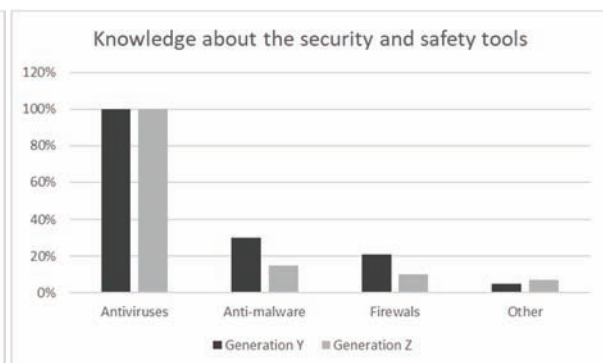


Figure 5. Knowledge about the security and safety tools

Usage of security and safety tools while in cyberspace: All participants stated they use security and safety tools such as antiviruses. Only 20% mentioned anti-malware except antiviruses, and 7% added firewalls.

6 Conclusion

From the results gathered we can conclude that the usage of the cyberspace is mostly done by the Generation Z in the Pollog region of the Republic of North Macedonia, if we take in consideration the time they spend on Internet and social media daily. Most of the participants in this research do not differ between Internet and cyberspace. Being daily on cyberspace, be it by browsing Internet or communicating through social media, it has made the participants aware of the vulnerabilities of it and

the cyberattacks which may be done to them. The mostly used protecting measure known is the antivirus. For resolving the cyberattacks, the only known method is reporting.

By the generation divide, it can be noticed that the generation Z are using social media longer the generation Y, while concerning the purpose of the usage – the generation Y are using internet (mainly social media) for the professional purposes, while the younger generation for entertainment. Concerning the component of the communication, both generations are using internet and social media for creating and expanding their networks.

Concerning the awareness of the existing tools for safety and security in the cyberspace, generation Y are more prone to have additional information about the potentials and possibilities of this tools, as it can be seen in the Figure 6 – about the distinction between antivirus and anti-malware awareness, while generation Z are more intuitive and they are more focused on the actual usage of this tools rather than on the technology behind them. The vulnerability from cyberattacks, the younger generation are more prone to be faced with the hacking activities on their social media accounts, while the generation Y are more vulnerable on the personal information as well as identity theft – because their activity with online transactions (or having the banking accounts). Cyberspace has plenty of vulnerabilities and as twice protection measurements which exceed the known ones by participants in the research. Also, for resolving of the cyberattacks, there are plenty of methods which can be apply except of reporting.

6.1 Future works

The future works of this research should comprise of widening the research in other regions as well as in the neighbouring countries, to extend the research with the comparison component as well.

References

- [1] Benedickt, M. (1991). Cyberspace: first steps. The MIT Press, Cambridge, MA and London, UK.
- [2] Helie, S. G. (2013). Cyber Power - Crime, Conflict and Security in Cyberspace. New York : EPFL Press.
- [3] Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Security Studies, 316-348.
- [4] Lillemose, J., & Kryger, M. (2015, August 24). The (Re)invention of Cyberspace. Retrieved from Kunstkritikk: <https://kunstkritikk.com/the-reinvention-of-cyberspace/>
- [5] Kuehl, D. (2009). From Cyberspace to Cyber-power: Defining the Problem. Washington D.C.: National Defense University Press.
- [6] Mayer, M., Martino, L., Mazurier, P., & Tzvetkova, G. (2014, May 19). How would you define Cyberspace? Retrieved from Academia: https://www.academia.edu/7096442/How_would_you_define_Cyberspace
- [7] Albert, R., Jeong, H., & Barabasi, A. -L. (1999). Internet: Diameter of the World-Wide Web . Nature , 130-131.
- [8] Marsden, C. T. (2011). Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace . New York: Cambridge University Press.
- [9] McCusker, K., & Gunaydin, S. (2014). Research using qualitative, quantitative or mixed methods and choice based on the research. SAGE journals.
- [10] Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. International Conference on Information Warfare and Security. Conferences International Limited.
- [11] Tulgan, B. (2013). Meet Generation Z: The second generation within the giant "Millennial" cohort. Retrieved from Rainmaker Thinking : <http://www.rainmakerthinking.com/assets/uploads/2013/10/Gen-Z-Whitepaper.pdf>
- [12] N.Bolton, R., Parasuraman, A., Hoefnagels, A., Migchels, N., Kabadayi, S., Gruber, T., . . . Solnet,

- D. (2013). Understanding Generation Y and their use of social media: a review and research agenda. *Journal of Service Management*, 245-267
- [13] "The World Bank in North Macedonia". World Bank. Retrieved 11 August 2019.