Karadeniz Teknik Üniversitesi İletisim Fakültesi Elektronik Dergisi | Karadeniz Technical University E-Journal Of Faculty of Communication

Cilt / Vol:5 Sayı / No :16 Temmuz/July :2018

CYBERSECURITY PERCEPTIONS OF UNIVERSITY STUDENTS IN TURKEY[1][2]

Bahar EROĞLU YALIN[3]

Çiğdem ŞAHİN BAŞFIRINCI[4]

Abstract

Globalisation and the internet have given individuals, organizations and the nations an incredible new power (Geers, 2011:9). This new force brought new concepts and responsibilities, such as cybersecurity. Cybersecurity has been an important topic on not only almost all science fields, but also for everyone in a contemporary everyday life. However, a methodological review of the literature demonstrates that there are limited studies on exploring cybersecurity perceptions of people.Within this context, the goal of this study is to reveal how the cybersecurity is perceived among Turkish university students. In other words, it is aimed to understand the cybersecurity associations and behaviors of Turkish university students. Results show that students' awareness level is quite high, they feel unsecure with regard to cybercrimes and most of them use multiple cautions in the cyberspace.

Key Words: Cyber security, cyber crime, digital age, university students.

TÜRKİYE'DE ÜNİVERSİTE ÖĞRENCİLERİ ARASINDA SİBER GÜVENLİK ALGISI

Öz

Küreselleşme ve internet birey, kurum ve uluslara inanılmaz bir güç vermiştir (Geers, 2011:9). Bu yeni güç siber güvenlik gibi yeni kavramları ve sorumlulukları da beraberinde getirmektedir. Siber güvenlik yalnızca bilimsel alan için değil aynı zamanda herkesin gündelik yaşantısı için önemli bir konudur. Buna karşın literatüre bakıldığında siber güvenlik algısını ölçümleyen sınırlı sayıda çalışma mevcuttur. Bu bağlamda, bu çalışmanın amacı siber güvenliğin üniversite öğrencileri arasında nasıl bir algısı olduğunu ortya çıkarmaktır. Başka bir ifade ile, bu çalışmaüniversite öğrencileri arasında sibergüvenlik çağrışımlarını ve

[1] Bu çalışma 20 Kasım 2017 tarihinde İstanbul'da düzenlenen First International Interdisciplinary Conference on Information and Cyber Security-Global Konferansında sözlü bildiri olarak sunulmuştur.

[2] Geliş Tarihi: 14. 05. 2018 Kabul Tarihi: 18. 06.2018

[3] Doç. Dr., Trabzon Üniversitesi, İletişim Fakültesi, beroglu@ktu.edu.tr, ORCID ID: 0000-0003-4619-3584

[4] Prof. Dr., Trabzon Üniversitesi, İletişim Fakültesi, cbasfirinci@ktu.edu.tr, ORCID ID: 0000-0003-1194-9804

davranışlarını anlamayı amaçlamaktadır. Sonuçlar, öğrencilerin farkındalık düzeyinin son derece yüksek olduğunu, siber suçlara karşın kendilerini güvensiz hissettiklerini, çoğunun siberalanda ihtiyatlı davrandıklarını göstermektedir.

Anahtar Kelimeler: Siber güvenlik, siber suç, dijital çağ, üniversite öğrencileri.

INTRODUCTION

We are in the age of a new revolution that witnesses the birth of a new culture. Internet is the most important element of this culture. As an opportunity, space and medium, the internet has redefined social and political frontiers in politics, economics, sociology and anthropology in addition to digital and virtual frontiers on a local and universal level. The field of law, which sets the rules for enabling common life experiences, has to broaden the scope of rights and responsibilities, crime and punishment in the face of these developments where new changes are added to the list every day. At this point, a new terminology of security and crime was developed, which is defined by names such as cyber, digital, information, internet, electronic, computer, technology, and it increasingly become one of the most controversial topics in public and private platforms.

1. TheNew Security Area on Digital Age: Cyber Security and Cyber Crimes

Cyber is used to describe concepts or entities that involve or contain computer and computer networks and cyberspace is used to describe the abstract or concrete area in which interconnected hardware, software, systems and people interact and/or interact (Klimburg, 2012). Cyber security term is also used with interchangeably information security term,and goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself (von Solms, Niekerk, 2013:97).

Cyber security is the secrecy, integrity and accessibility of the information used in all these cyber elements (Goodrich and Tamassia, 2010).According to NICE (The National Initiative for Cybersecurity Education) cyber security is an activity or process in which information and communication systems and the information contained in these systems are defended and protected against any criminal, attack or destruction.The ITU (International Telecommunications Union) defines cyber security as "the sum of tools, policies, security concepts, safety directives, risk management approaches, actions, courses, best practices, security and technologies that can be used to protect the assets of cyber environments,

institutions and individuals"(Göçoğlu, 2018:78-79). Cyber security can be defined as security provided by cyberspace. Cyber space is a non-physical field in which all systems of information and information that are spread all over the world and into the world are involved, and the systems of information systems that are interdependent and interacted with each other by people are connected with each other or with people(Bıçakçı, 2014:107;Göçoğlu, 2018:77-78). Moreover, cyberspace is now considered the fifth domain of warfare after land, sea, air, and space (Economist, 2010).

In order to understand the security of cyberspace, the layers forming the cyber space must be known. These layers are(Bıçakçı, 2014:107-111):

1. ***Physical Layer:*** Physical and physical equipment and people and assets provide the formation of cyber space.
2. ***Codes Layer and Software:***Codes layers that bring the existence of space closer to physical reality.
3. ***Content Layer:***The content layer consist of data about financial transactions are kept, strategic information of countries is stored, and medical information of patients in hospitals are kept.
4. ***Regulatory Layer:*** National and international legal regulations are restricting internet and content usage.

All these layers draw the boundaries of the use and exchange of local and global spaces and tools on the basis of individuals, institutions, and so on. Also Tikk, (2011:120) mentions that ten rules about cyber security arising from discussions among experts or in the course of cyber-incident handling can be identified; The Territoriality Rule, The Responsibility Rule, The Cooperation Rule, The Self-Defence Rule, The Data Protection Rule, The Duty of Care Rule, The Early Warning Rule, The Access to Information Rule, The Criminality Rule, The Mandate Rule. As a guide these rules present main frame for cyber security areas and praticess. These rules point to the responsibility of the nations about cyber security against risks and threats to the national and regional boundaries of individuals and institutions' information and documents. Therefore, cyber security is a broad issue that encompasses individuals, institutions and states at national and international levels. In particular, the individual use of this study is also considered as a very important element and problem area since the other two uses are also determinants.

Cyber crime is defined as, "Information is subject to automatic processing or holding an illegal system for the transmission of data, performed all kinds of unethical or unauthorized behavior"(Arslan,2018:2).At the same time cyber security is a concept addressed in the direction of risk of threat. The most important threat is the cyber attacks.

By cyber attack, it is meant the act of stealing, changing and destroying information in virtual networks to destroy the confidentiality, integrity and accessibility (Göçoğlu, 2018:80).In cyberspace societies need individuals who need to take place in both countries in terms of very vital information, cyberspace for malicious individuals, institutions and has become a clear target for the state. The unauthorized access of malicious people to information and documents in cyber space is very damaging to individuals, institutions and countries and these persons may destroy, change and disclose this information(Ünver and Canbay, 2010:96;Şahinaslan et al. 2013:1081).

For the understand thar cyber security perception we need to look at the categories of cyber attacks. Cyber attacks can be broadly categorized as follows (Ünver and Canbay, 2010:96, Arslan, 2018:3-9):

- **Spam:**Unspecified electronic mail.
- **Sniffing, Monitoring:**Intercept data,the rest of the network traffic.
- **Denial Of Service(dos):**Service disruptionor completely destroy the function of the service.
- **Distrubuted Denial of Service (ddos):**Target to attack with machine or computer community before the attacker's attack.
- **IP Spoofing:**Displaying the actual IP address to connect to a computer.
- **Social Engineering:**Utilizing human weakness inactivation of cyber security process or warping.
- **SQL Injection:** Attack the structure of the database using a query language.
- **Backdoors:**Methods that provide remote access to the computer.
- **Phishing:** Online fraud.
- **Spyware:** They are installed on the computer to collect information and send this information to the people who created these programs.
- **Virus:**Spreading malware to other files can infect a specific type.

- **Trojan:**There seems to have a useful function, but it also contains secret and potentially harmful functions that can bypass the security mechanisms and sometimes a computer program that exploits a system of units to be authorized as legitimate.
- **Worm**: Just as in the virus, they are designed to copy itself from one device to another, but that they perform on their own.
- **Bot:**Web robots or bots and called briefly as a special agent software group developed to show movement on the internet.
- **Botnet:**The computer without the user's computer can be used to commit serious crimes.
- **Chameleon:**Multiuser recording system with a username and a confidential file with the ability to imitate the password, give a warning that temporarily shut down for maintenance of the system, the name and password to seize the person who uses the meantime program.
- **Keyloggers:**The applets Save the keyboard actions.

All these types of attacks come into the domain of cybercrime and therefore cyber security, especially for the individual, as the most important problem area of the digital world.

2. Literature

There has been a significant increase in the related literature in cyber security in recent years.These studies generally approaches to cyber security as technological process and products.On the other hand,there are some other studies approaches to the concept from the perspective of individuals. Kritzinger E., von Solms (2010) in their study, investigated the position of the home user, and proposes a new model, the E-Awareness Model (E-AM), in which home users can be forced to acquaint themselves with the risks involved in venturing into cyber space.Ahmad, et al. (2012), have made focus group research about cyber security perception study among participants were representatives from the defense&security and the government sectors of the Critical National Information Infrastructure (CNII) in Malaysia. However, when compared to the signifiance of the cyber security concept, the academic studies in the area are very limited. This fact constitutes the main motivation of this study. Besides of these, to our best knowledge there is no any study that exploring cybersecurity perceptions of people in Turkey exist to date. As to original contribution of this study, it is the first one that has empirically demonstrated the cybersecurity associations of Turkish university students.

3. Methodology

This research will try the answer questions such as "What does cyber security mean to Turkish people?", "How much do they know about cyber security?", and "What are experiences, thoughts and feelings about the concept?". As an exploratory study mainly qualitative method was used in this study. Main data was collected with a survey that involving mainly open ended and one close ended questions. Population of the study is students of Karadeniz Technical University (A state university in Trabzon city). A convenience sample was used; all students of Communication Faculty were invited to fill the survey. Survey was conducted between 18-29 September 2017. A total of 283 respondents participated and completed the survey properly. In data analysis, mainly content analysis (in categorizing answers ofthe open ended questions) chi-square tests (in comparing female and male respondents' perceptions and preferences) were used.

4. Findings

Table 1. *Demographic Characteristic of Respondents*

PROFILE OF RESPONDENTS (N=283)					
GENDER	**N**	**%**	**AGE**	**N**	**%**
Female	159	56	Between 18-22 years	226	80
Male	123	43	Between 23-25 years	47	17
Other	1	1	Between 26-28 years	5	2
Total	283	100	29 years or older	3	1
DEPARTMENT	**N**	**%**	**Total**	283	100
PR&Advertising	195	69			
Journalism	88	31			
Total	283	100			

As seen in the Table 1, the demographic profile of respondents shows mainly a balanced structure with regard to their gender.

Then first of all, in order to develop a general understanding about perceptions toward cybersecurity, students were asked to write the first three things that came to their minds when they thought about cybersecurity through an open ended question.

Table 2. *The First Three Things that Came to the Minds about Cybersecurity (By priority)*

	First Mentioned		**Second Mentioned**		**Third Mentioned**		**Total Mentions**	
Internet	47	%17	33	%12	21	%7	101	%36
Hacker	21	%7	19	%7	12	%4	52	%18
Security	11	%4	23	%8	7	%3	41	%15
Total of Three	79	%28	75	%27	40	%14		

As you can see, internet, hacker and security were the most remembered words by university students. Internet was ranked as first, second or third by 36 percent of the respondents, while 17 percent of them ranked internet first, second or third. Hacker took the second place with 18 percent of the total mentions.

The other findings that following Internet, hacker and security, we also see that:

Computer, Social media, Virus, Privacy, Protection, Attack, Internet security, Crime, Technology, Fraud, Password were among other commonly remembered words.

Then we tested the feelings of respondents with regard to the cybersecurity.In this context we asked them if they were wanted to match the cybersecurity concept with one of your feelings, which feeling they would choose.

Table 3. *If You were Wanted to Match the Cybersecurity Concept with One of Your Feelings, Which Feeling You Would Choose? (You can write more than one)*

	Frequency	**Percent**
Fear	58	20%
Concern	49	17%
Insecurity	47	17%
Total of Three	154	54%

As you can see here, more than half of the respondents shared similar feelings such as fear, concern and insecurity in common. The other feelings stated were also mainly negative:

- Protection,
- Suspicion,
- Anger,
- Privacy and discomfort

Then we asked their experiences about cybersecurity.

Table 4 : *Have You ever Had a Cybersecurity Problem by now? (If the answer is yes, what problem/s have you experienced?)*

NO=244 (86%) YES=39 (14%)		
N=39	**Frequency**	**Percent**
Theft of social media accounts	22	37%
Virus attacks	16	27%
Theft of e-mail accounts	8	14%
Opening fake social media accounts	6	10%
Theft of IP number	2	3%
Theft of game accounts	2	3%
Fake letter of applications though internet	1	2%
Theft of blog account	1	2%
Internet fraud through scholarship application	1	2%
Total	59	100 %

As can be seen on Table 4, most of the respondents (86%) stated that they haven't experienced a cybersecurity problem before. Theft of accounts in different Internet media is among most often cited cybersecurity problems of students.

In order to gain a deeper understanding of students' cybersecurity perceptions, we also explored through an open ended question that have they ever witnessed a cybersecurity problem of close people around them. Despite the previous finding, this time 34% of the respondents didn't stated any witness to a cybersecurity problem, while 66 % of them declared one or more experiences. Considering that people may not prefer their bad experiences, we also asked them have they ever witnessed a cybersecurity problem of close people around them.

Table 5. *Have You Ever Witnessed a Cybersecurity Problem of Close People around You? (If your answer is yes, please state)*

NO=96 (34%) YES=187 (66%)		
N=187	**Frequency**	**Percent**
Theft of social media accounts	48	23%
Virus attacks	47	22%
Credit card frauds	45	21%
Theft of e-mail accounts	32	15%
Internet harassment	18	9%
Defamation on internet	10	5%
Hackers	7	3%
Theft of state secrets	5	2%
Total	212	100 %

As you can see on the Table 5, this time, respondents stated many different problems than their own experiences:

- Credit card frauds,
- Internet harassment,
- Defamation on internet,
- Theft of state secrets.

Also, the percentage of crimes is quite high. Taking these two findings together, the data indicates that despite students often declared that they do not have problems with regard to cybersecurity, when asked about the experiences of people around them, it appears that their awareness in this regard is not only high but also diversified.

Then, we wanted to reveal their perceptions about significance of the concept. Results can be seen on Table 6.

Table 6 . *Do You Think Cybersecurity is an Important Issue? Why?**

NO=5 (2%) NO IDEA= 6 (2%) YES=272 (96%)		
	N=272 Frequency	**Percent**
Personal information privacy and security	130	48%
The increasing role of the internet in our lives and the diversification of its functions in the digital era	42	15%
The protection of state secrets	16	6%
The protection of bank accounts	11	4%
Internet fraud prevention	8	3%
Prevention of cyberattacks	6	2%
Prevention of internet harassment	6	2%
Preventing the risks associated with internet shopping	5	2%
Total	224	82 %

*Frequencies below 5 are not included here.

As can be seen, overwhelming majority of the respondents (96%) evaluated concept as important.

Protecting personal information privacy and security, and the increasing role of the internet in our lives and the diversification of its functions in the digital era were mentioned by more than half of the participants, as the justification of its importance.

After exploring their perceptions about cybersecurity, we also want to see their actual information level and behaviors with regard to the cybercrime.

Within this context, we asked them:Have you ever officially complained about as a victim of any cybercrime case? If yes, please state.

From the Table 7, it can be seen that 94% of the respondents has never officially complained any official institution although 34% of them previously stated that they had experienced a cybersecurity problem before.

Table 7. *Have You ever Officially Complained about as a Victim of any Cybercrime Case? (If yes, please state)*

	Frequency	**Percent**
No	266	94%
Missing	5	2%
Yes	12	4%

Respondents who had an official complaint have opted not to mention what their complaints are. Only one of them mentioned fraud, another respondent did not explain the reason but stated that the complaint was not taken seriously enough by related institutions.

Also we conducted Chi-Square tests and saw that mainly there was no significant difference in complain behaviors of the male and female respondents.

5. Discussion

The basic motivation of our power to being alive is to survive. That's why security is one of the most fundamental values that guide human thought and action. The need of security has guided people to live together, to establish communities and states, and to play a crucial role in the development of science and culture. At the present situation, the digital age expressed by concepts such as network society, cyberarea, cyberspace has facilitated life at a level that humanity has not experiencedso far. But with it, it brings new areas of responsibility and the difficulties of these areas. In this respect, digital information and culture that will take the place of information and culture on traditional necessities require redefining and becoming functional on the basis of security which enable the communitiest olive with themselves and with each other. As with every new discovery, the risk posed by thisera of discovery is being perceived by the same risk, suspicion, and fear as it develop sthrough doubt and fear.

It should not be forgotten that perception is always a psychological phenomenon that comes before knowledge and whose change is more time consuming than knowledge. In this context, this is a perceptual study from the Turkish university student's stance with regard to cybersecurity concept. Results show that students' awareness level is quite high, they feel unsecure with regard to cybercrimes and most of them use multiple cautions in the cyberspace. Since the attitudes, values and perceptions with regard to the cybersecurity directly influence people's participation in the current and future technology world, our findings enlighten the authorized institutions understanding about what they need to do for a correct and complete understanding of the cybersecurity concept by the target audience.

The following issues should be emphasized limitations of this study. First of all, this is an exploratory study using a convenience sample. So, comprehensive studies with larger samples and random sampling can provide more sound data. Secondly, cross cultural studies can reveal richer information on the topic.

The path to be opened forthe new discovery of the age and especially the cybersecurity are apasses through the establishment of safer systems. It is human who will make these discoverie sand lead the formation of this newcult. Theincrease of such individual focusedstudies is of utmostimportancefortheharmony of thehumanbeingwithtechnology, languageandculture.

Acknowledgements

As the corresponding author Bahar YALIN has conducted abstract, literature review, data collection, discussion of the results, writing of the paper.

As co-author Cigdem BASFIRINCIhas been mainly responsible of the development of research idea and design research model, and all data collection process, data processing, analysis, and discussion and presentation of the results.

References

Rabiah, A., Zahri, Y., Shahib, S. and Yusoff, M. (2012). Perception on cyber terrorism: A focus group discussion approach. *Journal of Information Security,* 3(3), 231-237.

Arslan, M. E. (2018). Siber Güvenlik ve Siber Saldırı Türleri. https://s3.amazonaws.com/academia.edu.documents/52122013/SIBER_GUVENLIK_VE_SIBER_SALDIRI_TURLERI.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1519135648&Signature=NcTkY9%2BoTsGrHriEOeiz36etFUs%3D&response-content-disposition=inline%3B%20filename%3DSIBER_GUVENLIK_VE_SIBER_SALDIRI_TURLERI.pdf (Date of Access: 31.01.2018).

Ben-Asher, N. and Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior***,** 48, 51–61.

Craig, A. and Valerıano, B. (2018). Realism and Cyber Conflict: Security in the Digital Age. Davide Orsi, J. R. Avgustın & Max Nurnus (Ed.), *Realism in Practice An Appraisal* içinde (85-102). http://www.e-ir.info/wp-content/uploads/2018/01/Realism-in-Practice-E-IR.pdf#page=100, (Date of Access: 20.01.2018).

Bıçakçı, S. (2014). NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik.*Uluslararası İlişkiler,* 10 (40) (Kış), 101-130.

Geers, K. (2011). *Strategic Cyber Security*. CCD COE Publication, Estonia. https://ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF, (Date of Access: 09.02.2018).

Goodrich, M. and Tamassia, R. (2010). *Introduction To Computer Security*. Addison-Wesley.

Göçoğlu, V. (2018). *Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi.* Yayınlanmamış Doktora Tezi. Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı Kamu Yönetimi Doktora Programı, Ankara.

Insch, G. S. Moore, J. E. and Murphy, L. D. (1997). Content analysis in leadership research: Examples, procedures, and suggestions for future use. *Leadership Quarterly*,8, 1–25.

Kassarjian, H. H. (1977). Content analysis in consumer research. *Journal of Consumer Research***,** 4(1), 8–16.

Krippendorff, K. (1980). *Content Analysis: An Introduction To Its Methodology***.**Sage Publications. Beverly Hills.

Kritzinger, E. and von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29, 840 -847.

Şahinaslan, Ö., Şahinaslan, E., Borandağ, E. ve Şahinaslan, A. M. (2013). Güvenli bir toplum için son kullanıcı siber güvenliği. *XV. Akademik Bilişim Konferansı, Bildiriler, 23-25 Ocak 2013***,** Akdeniz Üniversitesi, Antalya, 1081-1085.

Tikk, E. (2011). Ten rules for cyber security. *Survival*, 53 (3), 119-132.

Ünver, M. ve Canbay, C. (2010). Ulusal ve uluslararası boyutlarıyla siber güvenlik. *Elektrik Mühendisliği Dergisi***,** 438, 94-103.

von Solms, R. and van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97 -102.

Zimmer, M. R. and Golden, L. L. (1988). Impressions of retail stores: A content analysis of consumer images. *Journal of Retailing*, 64(3), 265–294.