Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 13

1-29-2024

Turkey vs Italy: Gender and Cyber Security

Esra Merve Caliskan
Istanbul University, ecaliskan@medipol.edu.tr

Irem Itegin

Recommended Citation
Caliskan, Esra Merve and Irem Itegin (2024) "Turkey vs Italy: Gender and Cyber Security," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 13.
DOI: https://doi.org/10.62915/2472-2707.1171
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/13

Turkey vs Italy: Gender and Cyber Security

Abstract

With the development of technology, security, a core human concern throughout history,has changed and branched out into new areas. Novel security concepts, including environmental security, economic security, and cybersecurity, have emerged as a result of these expanding areas. The importance of cybersecurity has increased in the linked world of today as a result of how prevalent technology is in our daily lives. This study looks at how the literature on international relations approaches the idea of cybersecurity, with an emphasis on the role gender dynamics play.

This study adopts a comprehensive strategy in recognition of the possibility that people of all genders may be affected by the dominant gender roles. The study seeks to offer a comprehensive understanding of cybersecurity by utilizing a mixed-methods research methodology that incorporates both qualitative and quantitative techniques.

Conducting in-depth interviews with young adults (ages 18 to 27) who identify as people of different genders will be part of the field research. Various aspects of cybersecurity, such as perceptions of cybersecurity, emotions of security, and encounters with cyber dangers, will be covered in these interviews. The research will be carried out in both Turkey and Italy, enabling a comparison of the cybersecurity laws and conditions in these two nations.

By combining theoretical underpinnings with empirical fieldwork, this study aims to give a fresh viewpoint. The survey data will also be subjected to statistical analysis. The study's findings will shed light on how young adults' perceptions of cybersecurity are influenced by gender norms and what that means for cybersecurity laws.

This research contributes to the larger discussion on cybersecurity and gender studies by broadening its focus beyond gender as a binary construct and offering insightful information about how gender roles affect cybersecurity views across a range of identities.

Keywords

cyber security, gender, cyberbullying, cyber threats, policy making

Cover Page Footnote

Acknowledgment We would like to extend our sincere thanks to all participants who took part in the in-depth interviews. We are grateful that they shared their valuable time with us and contributed to our research. We would also like to thank all the participants who took part in the survey. The time they took to answer the questionnaire was invaluable to us. Finally, we would like to thank all our friends and family who supported us during the research.

Turkey vs. Italy: Gender and Cyber Security

Esra Merve Çalışkan
Istanbul University, Institute of Social Science,
Faculty of Political Science, Department of
Political Science and International Relations
Istanbul, Türkiye
ecaliskan@medipol.edu.tr
https://orcid.org/0000-0001-5226-3177

İrem İtegin
Sapienza University
European Studies
Rome, Italy
iremitegin@gmail.com
https://orcid.org/0009-0005-4190-6946

Abstract—

With the development of technology, security, a core human concern throughout history, has changed and branched out into new areas. Novel security concepts, including environmental security, economic security, and cybersecurity, have emerged as a result of these expanding areas. The importance of cybersecurity has increased in the linked world of today as a result of how prevalent technology is in our daily lives. This study looks at how the literature on international relations approaches the idea of cybersecurity, with an emphasis on the role gender dynamics play.

This study adopts a comprehensive strategy in recognition of the possibility that people of all genders may be affected by the dominant gender roles. The study seeks a comprehensive understanding of cybersecurity by utilizing a mixed-methods research methodology that incorporates both qualitative and quantitative techniques.

Conducting in-depth interviews with young adults (ages 18 to 27) who identify as people of different genders will be part of the field research. Various aspects of cybersecurity, such as perceptions of cybersecurity, understanding of security, and encounters with cyber dangers, will be covered in these interviews. The research will be carried out in both Turkey and Italy, enabling a comparison of the cybersecurity laws and conditions in these two nations.

This study aims to give a fresh viewpoint by combining theoretical underpinnings with empirical fieldwork. The survey data will also be subjected to statistical analysis. The study's findings will shed light on how young adults' perceptions of cybersecurity are influenced by gender norms and what that means for cybersecurity laws.

This research contributes to the larger discussion on cybersecurity and gender studies by broadening its focus beyond gender as a binary construct and offering insightful information about how gender roles affect cybersecurity views across various identities.

Keywords—gender, cyber security, cyberbullying, policy-making, cyber threats.

I. Introduction

The idea of security, a persistent worry throughout the history of humanity, has experienced a revolutionary metamorphosis in line with technical advancements, expanding its reach into new fields. Due to the modern world's rapid technological growth, cybersecurity has become a significant concern affecting all parts of society. New cyber hazards and threats are escalating as our lives become more interconnected through digital gadgets and internet platforms. Due to this escalation, cybersecurity is becoming not only a technical problem but also a societal and political one. With a focus on the crucial role gender dynamics play, this study attempts a thorough investigation of how the literature on international relations connects with the complex field of cybersecurity.

There is a dearth of research on the sociocultural variables that affect cybersecurity attitudes and behaviors, even though the technological aspects of cybersecurity receive a lot of attention. Gender is a significant social aspect that affects how people view the world.

By using a thorough gender lens to investigate how various gender identities and social gender norms affect views of cybersecurity, this study seeks to fill a vacuum in the body of literature. This study aims to offer a comprehensive understanding of cybersecurity's multidimensional nature by utilizing a mixed-methods research approach that combines both qualitative and quantitative methodologies. It employs both qualitative interviews and quantitative surveys to highlight young individuals in Turkey and Italy. To achieve this, the field research component involves conducting in-depth interviews with young individuals, ranging in age from 18 to 27, who represent various gender identities. These interviews will examine many aspects of cybersecurity, such as how people perceive cybersecurity, how they feel about security, and how they have dealt with cyber threats. By contrasting the two nations, it will also examine how views of cybersecurity are shaped by various cultural situations.

This study aims to offer a new perspective on the topic by elegantly fusing theoretical underpinnings with empirical fieldwork. Additionally, a thorough statistical analysis of the survey results will be performed. The findings that follow will shed light on how much gender norms affect young adults' perceptions of cybersecurity and, consequently, the consequences this has for the creation of cybersecurity policy.

II. Ease of Use

A. Literature Review

In recent years, cybersecurity has become an issue of increasing interest among both academic circles and policymakers. As states and non-state actors place greater reliance on digital technology for communication, trade, and infrastructure, vulnerabilities in cyberspace have become a major concern for governments and international organizations (Schmitt, 2017). Traditional national security paradigms are now deeply intertwined with the digital sphere, necessitating a reassessment of conventional security frameworks (Cavelty, 2015). While cybersecurity experts focus on technical challenges, social scientists examine the human and societal dimensions of this field. Studies investigating the sociological and political aspects of cybersecurity indicate that this phenomenon is shaped not only by technical factors but also by human behaviors and perceptions.

Cybersecurity is based on gendered assumptions, biases, and shortcomings (Millat et. al. 2021). This makes it difficult for this field to be a safe area in every sense. This study aims to examine gender differences in cybersecurity perception among young adults in Turkey and Italy through a comparative perspective, focusing on a gap in the literature. Gendered perceptions, experiences, and challenges in cybersecurity have implications for both national security policies and international relations (Brown & Pytlak, 2020). Prior research shows that men tend to have greater interest in and self-efficacy related to cybersecurity compared to women (Ingala, 2018; Anwar et al., 2017). However, how gender stereotypes shape the attitudes and behaviors of youth in this field has not been adequately studied. Moreover, the limited research on cybersecurity and gender has been largely confined to Western nations. By addressing the issue in the Turkish and Italian contexts, this study seeks to compare the effects of gender dynamics on cybersecurity across different cultural settings. This promises to provide novel insights to both the academic literature and policymakers in the two countries. Cross-country comparisons can offer insights into how legal frameworks and cultural contexts shape gender dynamics in cybersecurity (Dunn Cavelty & Suter, 2009).

Studies have shown that gender norms and stereotypes can influence not just an individual's cybersecurity outlook but also societal attitudes and policies in this field (Lindsay, 2016). This broader gender perspective is critical for understanding the complex interplay between identity, security, and technology. This research acknowledges the fluidity of gender identities and their diverse influences on cybersecurity perceptions.

When we examine the concept of cybersecurity in international relations literature through the lens of gender perspectives, traditionally gender was an issue overlooked in foreign policy and security studies, but in recent years the gender perspective has gained more prominence in international relations (Tickner, 2001). Security studies have also long reflected a male-dominated perspective. However, in recent times, feminist international relations theorists have been attempting to redefine security from a gender perspective (Sjoberg, 2016).

The influence of gender roles and norms in security issues, including cybersecurity, is increasingly recognized. The gender perspective has contributed to the broadening of the security concept. Security is now associated not just with military threats but also with environmental, economic, and cyber threats. While the military and technical dimensions of cybersecurity come to the fore, the gendered experiences of individuals in this field should not be overlooked either. Cybersecurity has the potential to both reproduce and transform gender inequalities (Radu & Smaili, 2022).

B. Methodology

The mixed methods strategy used in this study combines qualitative and quantitative tools to examine research problems from many angles. The main hypothesis of the study is "Young women living in Turkey and Italy have higher cybersecurity concerns than their male peers". Cybersecurity anxiety is defined as individuals' concerns about information security, invasion of privacy, and exposure to cyber-attacks. In-depth semi-structured interviews with young adults in Turkey and Italy, ages 18 to 27, were part of the qualitative phase. The sample size was between 10 and 15 people from each nation and gender identification group. Face-to-face or video conferences were used to conduct the interviews. Participants' perspectives, attitudes, experiences, and worries about cyber security risks, privacy concerns, security habits, and national policies are examined through open-ended questions. The qualitative information gathered from these interviews will offer subtle insights into how gender dynamics and cybersecurity perceptions interact.

Based on consent, all interviews were taped and written down. Thematic analysis, a qualitative technique for locating recurring themes and patterns in textual material, was used to examine the transcripts. Deductive coding based on the major topics in the interview guide was intended, whereas inductive coding was intended to catch emergent themes.

The quantitative phase comprises the responses provided to survey questions with closed-ended prompts by young adults (18–27) in Turkey and Italy. The study includes questions about perceptions of cyber security, cyber security policies, and opinions of cyberbullying in addition to demographic data including age, gender, and citizenship.

This mixed-methods approach provides a thorough picture of how young adults from various gender backgrounds perceive and experience cybersecurity in Turkey and Italy. It generalizes the rich information from interviews and combines it with survey results. Additionally highlighting similarities and differences based on cultural contexts is the comparative method. With the help of a mixed methods strategy that incorporates both qualitative and quantitative research methodologies, the goal is to provide a comprehensive understanding of cybersecurity.

To provide a comparative comparison of cybersecurity regulations and conditions in Turkey and Italy, the research was carried out in these two nations. The main reason for selecting participants from Turkey and Italy in the study is that these two countries have different socio-cultural backgrounds and their approaches to cybersecurity can be compared. Addressing Italy, which is located in Europe and has a developed economy, and Turkey, which is in the position of a developing country, comparatively is important in terms of revealing the social and cultural factors in the perception of cybersecurity.

In future studies, investigating the perspectives of young people in different regions and countries on cybersecurity and cyberbullying will contribute to the literature. Especially research to be conducted in regions such as Asia, Africa, the Middle East, and Latin America, where the findings obtained from the sample of Turkey and Italy can be compared. Thus, the cultural contexts of perceptions and experiences regarding cybersecurity can be revealed in more detail.

This comparative method will give a more comprehensive view of the interactions between gender roles and country cybersecurity policies and practices.

This study employs a mixed-methods research approach to capture the complexity of cybersecurity views while taking gender dynamics into account. The combination of qualitative and quantitative data will enable a thorough analysis of the research issues and contribute significant knowledge to the fields of gender studies and cybersecurity.

C. Results & Discussion

In this study, the perceptions of young people aged 18-27 in Turkey and Italy on cybersecurity and gender were analyzed using quantitative and qualitative methods. 144 participants were surveyed online and in-depth interviews were conducted with a total of 20 participants, 10 from Turkey and 10 from Italy. In light of the quantitative and qualitative data obtained, it has been determined that young people from both countries largely see cybersecurity as an important issue and are concerned about policies. In this section, the survey results and interview findings will be presented in detail and discussed comparatively.

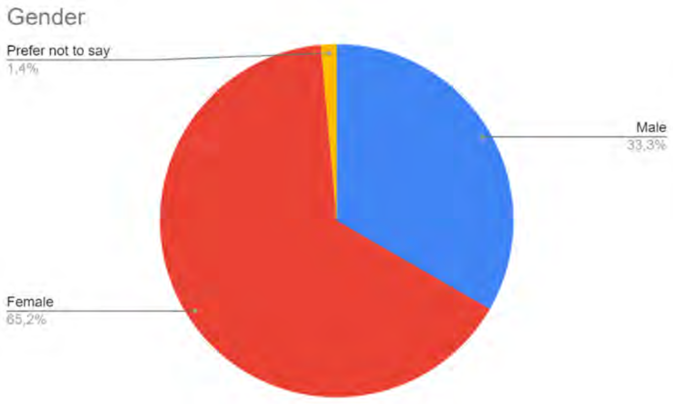

Figure 1 Demographic Questions-Gender

Both in-depth interviews and online surveys started with questions on demographic characteristics. The first of these questions was aimed at determining gender. As can be seen in Figure 1, 65.2% of the participants who answered the question were female, 33.3% were male and 1.4% did not want to specify. This shows that female participants are more interested in this study focused on gender and cyber security.

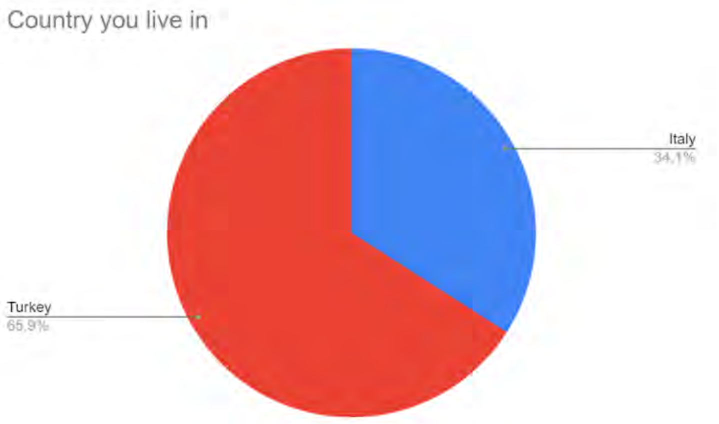

Figure 2 Demographic Questions-Country Residence

Another question asked to the participants in the section based on their demographic characteristics was aimed at determining their country of residence. Accordingly, as can be seen in Figure 2, 65.9% of the participants stated that they live in Turkey, while 34.1% stated that they live in Italy. The main reason for this situation is that the questionnaire was prepared and published in Turkish and English. The wider dissemination of the survey among university students in Turkey explains the higher number of Turkish respondents compared to Italian respondents.

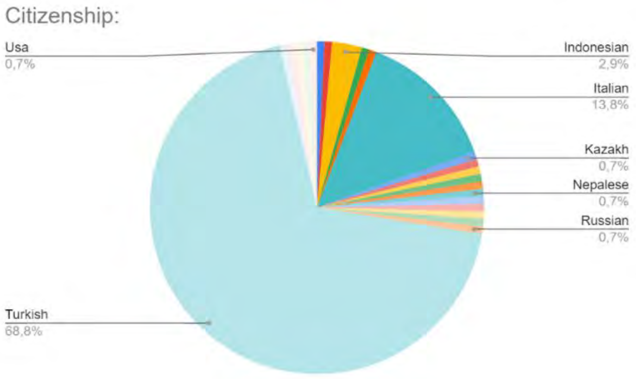

Figure 3 Demographic Questions-Citizenship

Another question in the section on demographic characteristics was about civic knowledge. As can be seen in Figure 3, 68.8% of the participants were citizens of Turkey, 13.8% were citizens of Italy, 2.9% were citizens of Indonesia, 0.7% were citizens of the United States, 0.7% were citizens of Kazakhstan, 0.7% were citizens of Russia, and 0.7% were citizens of Nepal. Turkish students have a high awareness of cybersecurity and gender issues. The lower participation from Italy indicates that this issue is not as popular among Italian youth as it is in Turkey. The data obtained provide important clues about the cybersecurity perception of Turkish and Italian youth.

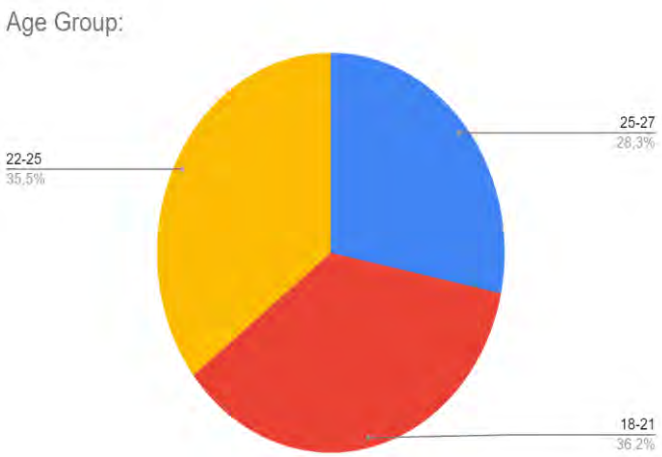

Figure 4 Demographic Questions-Age

One of the demographic questions asked of the participants was about age. As shown in Figure 4, 36.2% of participants were between the ages of 18 and 21, 35.5% from 22 to 25 and 28.3% from 25 to 27. The age groups identified for the participants are important for the details of the study.

In your study, participants between the ages of 18 and 21 make up 36.2% of the youngest participant group. This category typically consists of young adults or those attending college. Your study must examine how young people view gender issues and cybersecurity from this age group's point of view.

The middle age range of participants in your study is represented by 35.5% of participants who were between the ages of 22 and 25. This group includes recent grads as well as university graduates. The study will show variations in terms of study since participants in this age range may have different perspectives on gender in society and cybersecurity as a result of their life experiences.

28.3% of participants in your study are between the ages of 25 and 27. Those who have reached or are approaching the end of their youth are included in this age group. This group can affect gender attitudes and cybersecurity perceptions differently in society because it represents the youth-to-adult transition.

Because of this, your study presents a chance to carry out a more thorough analysis by concentrating on the participant age groups, contrasting cybersecurity attitudes across age groups, and examining perspectives on gender issues in society. various results offer crucial information for comprehending the variations and parallels in various age groups based on age.

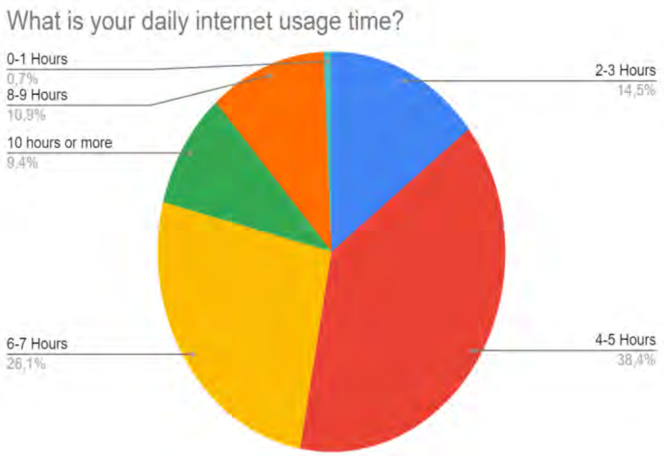

Figure 5 Internet Usage Time

Another question asked in the study was aimed at determining the daily time spent on the Internet. As shown in Figure 5, 38% of respondents used the Internet for 4-5 hours per day, 26.1% used the Internet 6-7 hours a day, 14.5% used the Internet for 2-3 hours a Day, 10.9% used the Web for 8-9 hours per Day, 9.4% used the Website for 10 hours or more a day and finally 0.7% used 0-1 hours of the Internet a Day. These findings show that young people's interests and levels of interaction in the digital world vary widely.

Even while 38% of respondents claim to use the Internet for four to five hours a day, this group is representative of a subgroup that actively engages in online activities and spends a large amount of their daily life on these platforms. These individuals spend more time on online learning or work-related activities, are more likely to engage in online groups, and are active on social media, all of which boost their connection within cyberspace.

It's still rather high to use the internet six to seven hours a day, as reported by 26.1% of respondents. Although this group may be very interested in interacting online, there is a possibility that it is more susceptible to cyber security threats.

A more modest daily time spent on the Internet was indicated by the 14.5% of respondents who stated they utilized it for two to three hours a day. Although these individuals use the Internet for their online activities, the shorter duration of their use reduces their cyber-security threats.

10.9% of respondents reported using the internet for eight to nine hours each day, and 9.4% reported using it for ten hours or more. These groups are made up of users who regularly engage in a lot of online communication. Longer online interactions may raise cybersecurity threats, indicating the importance of raising these groups' awareness of cybersecurity.

Lastly, 0.7% of respondents report using the Internet for 0–1 hours per day, which is a very low amount of time. Because they might not be as interested in online interactions, there might be less of a risk to cyber security.

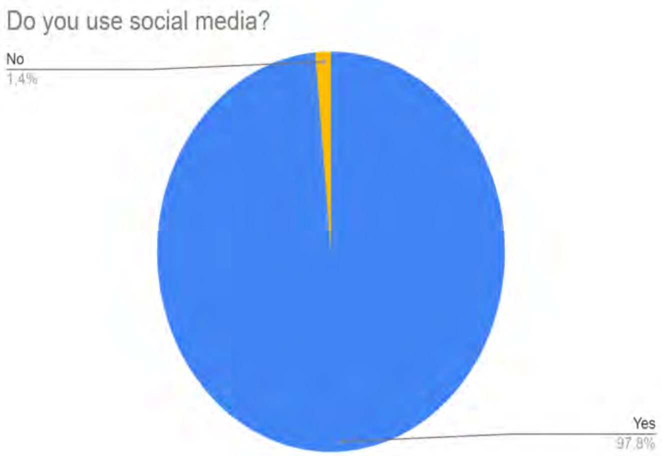

Figure 6 Social Media Usage

Another question asked to the participants was to find out whether they use social media. As can be seen in Figure 6, 97.8% of the participants stated that they use social media, while 1.4% disagreed. These results reveal very interesting and important data. The fact that 97.8% of the participants state that they use social media shows that the majority of a young group between the ages of 18-27 tend to actively use these platforms. This shows that social media is a common communication and information-sharing tool among young people.

However, it is noteworthy that a minority of 1.4% stated that they do not use social media. This minority reveals that social media is not a necessary or preferred communication tool for everyone. This result is important for the research, as social media use can increase cybersecurity risks and impact gender-related issues.

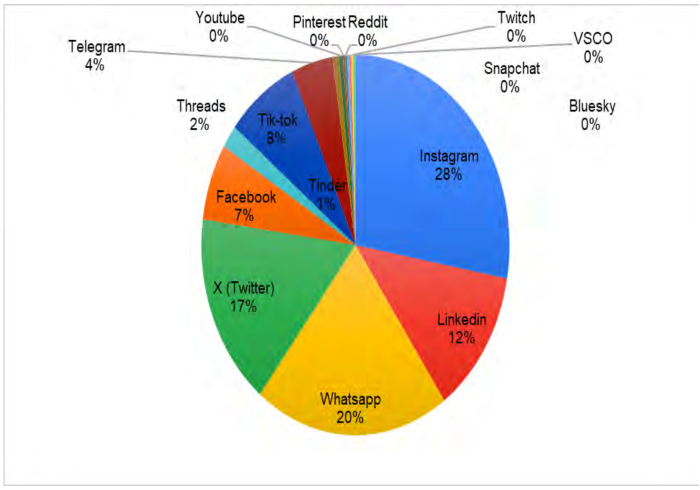

Figure 7 Social Media Applications

The information in Figure 7 was acquired from the participants when they were questioned about the social media sites they utilize. As can be seen, the instant messaging app WhatsApp scored second, while Instagram, which offers visual content, ranked first. Both Twitter and LinkedIn, which are platforms for professional networking, have a specific utilization rate. Telegram and Facebook are used less frequently. Though they are relatively new and have become more well-known recently, younger people still like TikTok and Threads. A small percentage of young individuals chose other social media channels. With the support of the in-depth interviews, it is possible to say that the use of social media is quite common among young people, WhatsApp is equally popular for young people living in Italy and Turkey, but Instagram is more popular in Turkey, while Linkedin is more popular in Italy. In conclusion, the majority of respondents prefer platforms focused on visual content and instant communication.

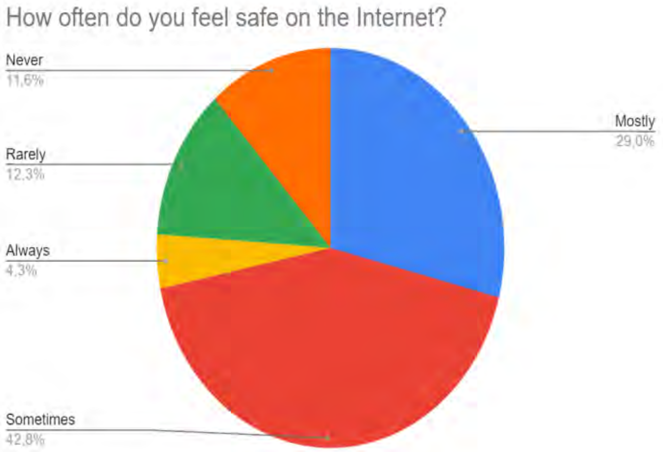

Figure 8 Internet Safity

In our research when we asked participants how often they feel secure, on the Internet the majority (42.8%) responded with "sometimes " while 29% said "mostly." On the other hand, 12.3% mentioned feeling safe rarely while 11.6% admitted to never feeling secure. Surprisingly only a small percentage of 4.3% claimed to feel online. These findings indicate that young individuals don't perceive the internet as a space. A significant portion of respondents (24%) expressed that they rarely or never feel secure while using the internet.

The fact that most participants reported feeling safe suggests that there are still security concerns and threats that affect their sense of safety online. Approximately half of the surveyed youth indicated feeling secure whereas the other half stated they felt secure frequently or always. This highlights a need for heightened awareness and measures regarding internet security. During in-depth interviews, many participants emphasized that their trust is compromised due to the openness of the internet and its potential for interaction from any direction. Overall it can be concluded that people's sense of safety, on the internet is generally low.

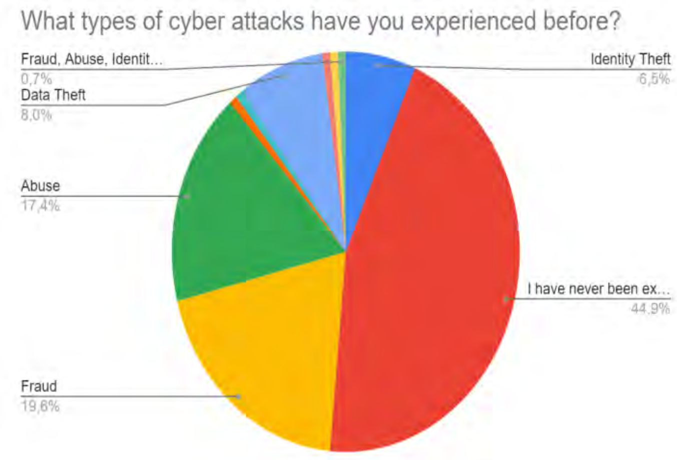

Figure 9 Experienced Cyber Attacks

We also asked, "Which type of cyber-attacks have you experienced before?" to the survey participants. Out of all the participants, 44.9% said they had never experienced a cyberattack. Nonetheless, over 50% of them have at least once fallen victim to a cyberattack. With 19.6% of attacks, fraud and forgeries are the most prevalent category. The next highest percentages are 17.4% for harassment/disturbance, 8% for data theft, and 6.5% for identity theft. These findings demonstrate the variety of cyberattacks that the respondents have encountered. Online difficulties are very widespread and include fraud and abuse. The in-depth interviews provided additional support for these findings. "Presenting themselves with identities they are not" was said to be a typical online activity.

As a result, a significant proportion of young people have been attacked online at least once. This situation reveals that the vulnerability to online attacks is more prevalent.

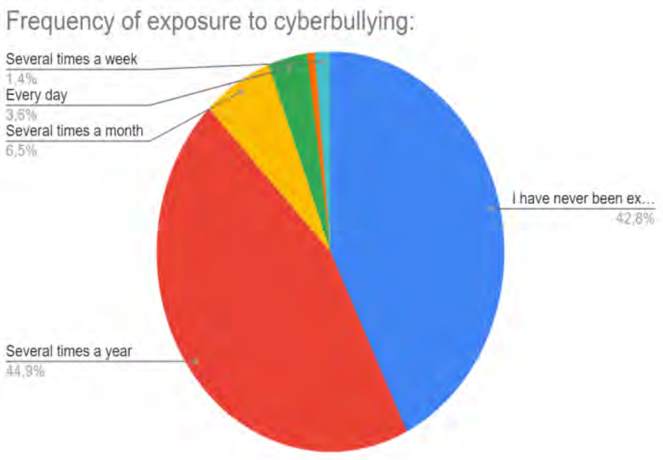

Figure 10 Cyberbullying Exposure Frequency

There is a notable variation in the responses to the question regarding the participants' frequency of exposure to cyberbullying. 42.8% of respondents said they are never subjected to cyberbullying, whilst 44.9% of respondents said they are exposed to it frequently. In terms of cybersecurity, these findings demonstrate the prevalence of this kind of cyberbullying as well as the vast range of experiences among respondents.

3.5% reported being exposed to cyberbullying every day, 1.4% a few times a week, and 6.5% a few times a month. These findings imply that some participants are exposed to cyberbullying relatively frequently and that they go through these experiences every day or every week. In-depth interviews also supported these results. In particular, among the participants who stated that they had been exposed to cyberbullying in the interviews, female participants constituted the majority in both Turkey and Italy. This shows that in general, women are more exposed to attacks from the internet world.

These results are important for understanding the impact of cyberbullying on cybersecurity and gender perceptions. Consequently, nearly 50% of young people report having at least once been the victim of harassment or cyberbullying online. Despite being small, the percentage of people who report experiencing harassment daily or multiple times per week is not insignificant.

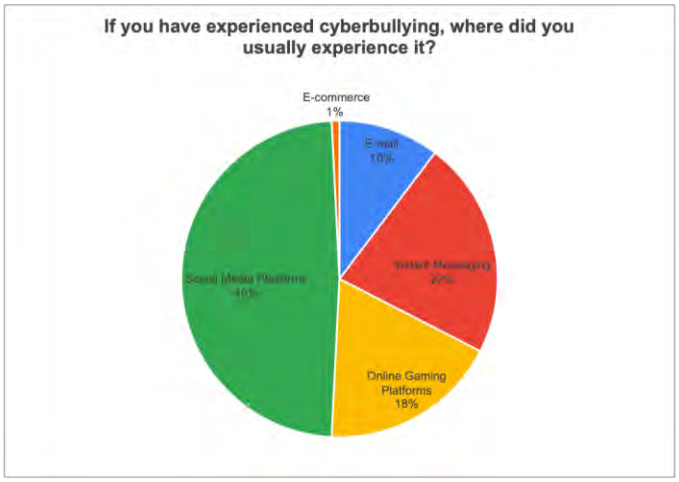

Figure 11 Cyberbullying Experienced Places

Figure –11 presents the responses provided by the participants in response to the question, "If you have experienced cyberbullying, where did you usually experience it?" When we analyze the data, we find that most of the participants had seen instances of cyberbullying on messaging and social media sites where there is a lot of contact. Another significant area that presents a risk for cyberbullying is online gaming environments. Cyberbullying occurs less frequently in more formal channels like email and online shopping. The results are useful because they shed light on the online environments where youth are most susceptible to cyberbullying. The in-depth interviews also revealed that trust in social media platforms has decreased significantly among young people living in Turkey and Italy. Young people stated that they do not feel safe on these platforms and that they feel open to all kinds of dangers.

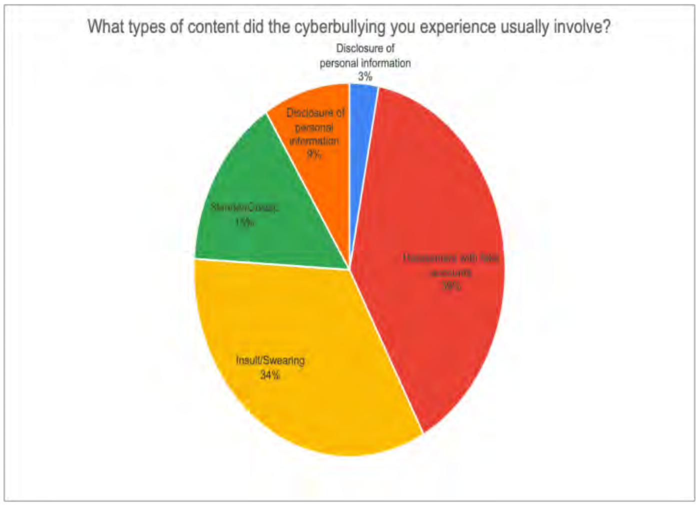

Figure 12 Cyberbullying Content

The responses provided by the participants to the question regarding the types of cyberbullying content they encountered revealed that 39% of the subjects reported experiencing harassment through fictitious accounts, 34% insults and swearing, 15% slander and gossip, and 9% disclosure of personal health information. Because of this, the majority of participants encounter cyberbullying in the form of messages that are derogatory or contain profanity, along with bogus identities that harass them. Other forms of cyberbullying that occur frequently include slander, gossip, and the revealing of personal information. The results show that cyberbullies regularly torment their victims by using anonymous identities to hide their identity and by posting a lot of offensive and harassing stuff. In the in-depth interviews related to these results, it was revealed that although the disclosure of personal data has a low rate among the attacks experienced, it is the type of cyberbullying that is the most worrisome among young people living in Turkey. In addition, young people who were exposed to bullying such as threats and blackmail stated that they were psychologically affected by this issue. As a result, it has been revealed that the failure to ensure full cyber security not only damages the sense of trust of young people but also leads to different negative consequences in the long term.

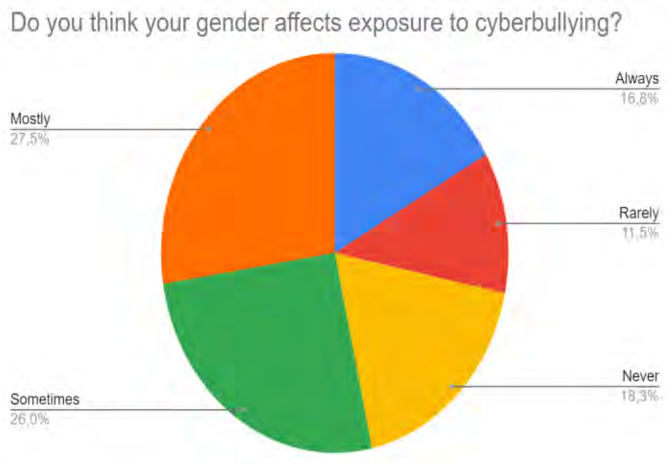

Figure 13 Gender Effects of Cyberbullying

In response to the inquiry, "Do you think your gender affects exposure to cyberbullying?" 27.5% of participants said that their gender influences their exposure to cyberbullying primarily, followed by 26% who said it does so occasionally, 18.3% who said it never, 16.8% who said it usually, and 11.5% who said it seldom. These findings show that whereas half of the participants believed that gender had a significant impact on cyberbullying exposure, the other half believed that gender had little or no effect. These findings suggest that participant perspectives regarding the impact of gender on cyberbullying are not all that similar. Nonetheless, a sizable portion of participants think that gender matters. The way this situation was handled in the in-depth interviews, women constitute the majority in the section that argues that their exposure to cyberbullying in both countries is due to their gender. Men, on the other hand, think that their gender is not effective in this regard. This again shows that women have a relatively more active concern.

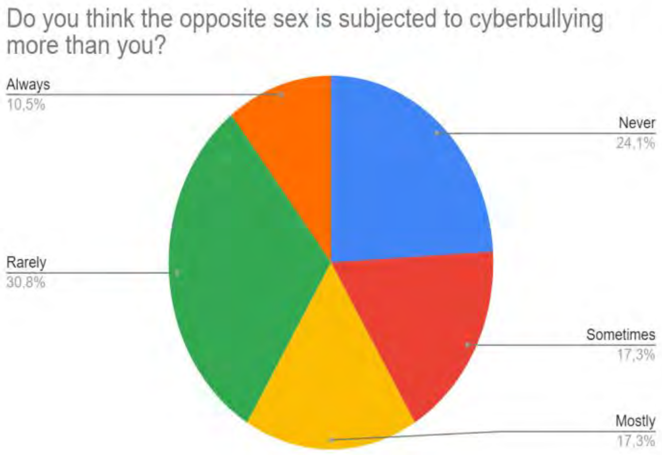

Figure 14 Opposite sex effects of cyberbullying

According to the responses to the question, "Do you think the opposite sex is subjected to cyberbullying more than you?" 30.8% seldom, 24.1% never, 17.3% occasionally, 17.3% mostly, and 10.5% always replied. These findings show that about one-third of participants believed that cyberbullying against the other sex occurs less frequently, whereas the other two-thirds believed that cyberbullying against the opposing sex occurs more frequently.

It is possible to say that there are different perceptions about cyberbullying exposure between genders. In the in-depth interviews, male participants were more likely to state that women are more exposed to cyberbullying in both countries. Among female participants, the majority of participants thought that men were not exposed to cyberbullying. This is another result showing that women are more insecure online.

These findings demonstrate the nuanced relationship between gender and perceptions of cyberbullying. The participants' disparate cognitive processes demonstrate the range of awareness and opinions on gender and cyberbullying. These findings are a valuable source of information for comprehending gender-related concerns and perceptions of cyberbullying.

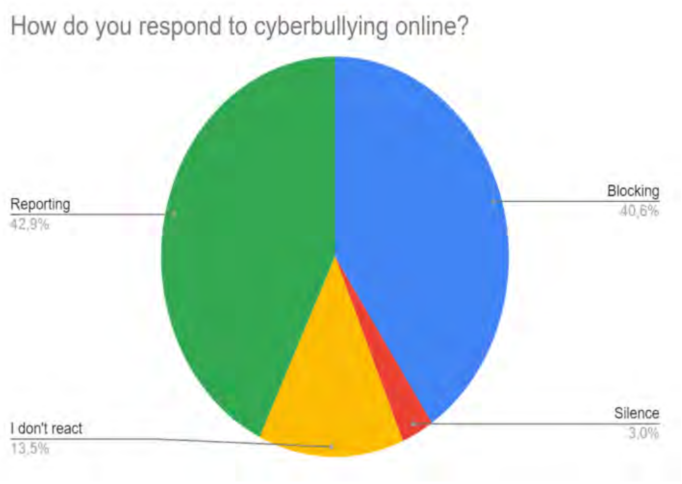

Figure 15 Cyberbullying Response

42.9% of participants indicated "reporting" in response to the question "How do you respond to cyberbullying online". This implies that those who experience cyberbullying online should report these actions to platform managers or law enforcement. By reporting instances of cyberbullying, you may help stop it and hold those guilty.

When asked the same question, 40.6% of respondents said "blocking". This indicates that when victims of cyberbullying wanted to stop communicating online, they blocked the aggressors. Blocking is a useful tactic to guarantee cybersecurity and ward off intruders.

Thirteen percent said "I don't react" in response to the same question. This demonstrates that some people who experienced cyberbullying choose not to reply. This tactic could be useful for those who would rather handle confrontation or cyberbullying in a more composed manner.

In response to the same query, 3% said "silence". This indicates that a smaller subset of participants did not choose to keep silent in the face of cyberbullying. Silence, on the other hand, may allow cyberbullying to continue and prevent the issue from being fixed.

Another interesting result was revealed during the in-depth interviews regarding the results. There is also a tendency to "reduce internet use", especially among female participants. This has emerged as an interesting solution to protect oneself and prevent possible bullying.

The various ways that individuals dealt with cyberbullying that occurred online are reflected in these data. Blocking and reporting seem to be the most widely used tactics. "I don't react" and "silence" are examples of more subdued methods of dealing with cyberbullying.

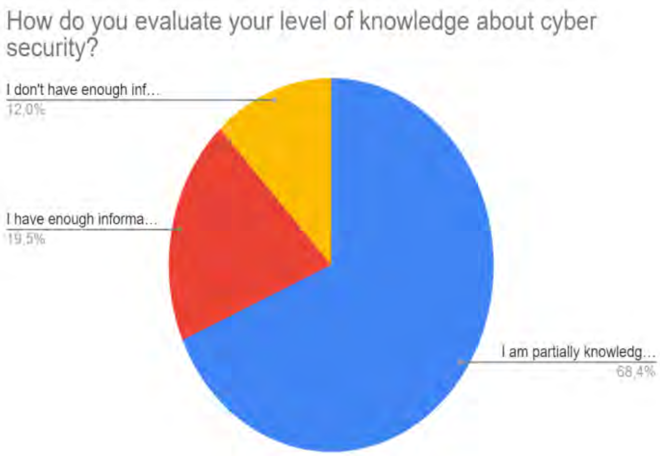

Figure 16 Cyber security knowledge

When asked "How do you evaluate your level of knowledge about cyber security?", the majority of participants (68.4%) stated that they were partially knowledgeable about cyber security. 19.5% stated that they had sufficient knowledge, while 12.5% stated that they had insufficient knowledge. According to these results, the majority of participants have only partial knowledge about cyber security. The rate of those who say they are sufficiently knowledgeable is quite low. In-depth interviews also supported these results. The interviewer stated that cyber security knowledge is partial among young people in Italy and Turkey, regardless of gender. However, among young people in Italy, the majority of those who state that they have insufficient information are women. As these results show, it would be beneficial to increase information activities for young people about cyber security.

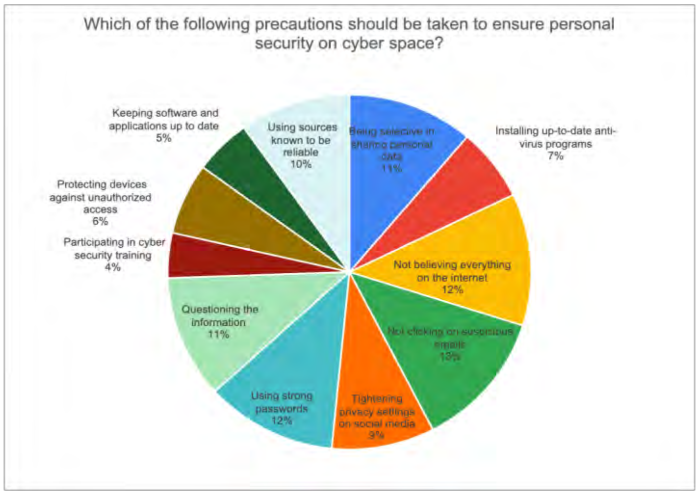

Figure 17 Personal Security on Cyber Space

When we asked the respondents what steps they should take to ensure their cyber security, 13% advised against clicking on dubious emails, 12% advised using strong passwords, 12% advised not to believe everything they read online, and 1% advised sharing personal information only with specific people.

In addition to this, the most often mentioned precautions include regular use of antivirus software, privacy settings on social media, and information searching. Using reliable sources, guarding against illegal access to equipment, and going to cybersecurity training were comparatively less common answers. Consequently, it was noted that individuals attempted to secure their cyber security using a variety of means. Although receiving cybersecurity training is seen as the least preferred option, in-depth interviews revealed that it would be interesting to receive cybersecurity training, but that there is not enough information on this subject. This shows that if policymakers provide sufficient incentives in the education section, support for this issue will increase among young people. It has been observed that the preferred protection methods for ensuring personal cyber security among young people living in Turkey and Italy are similar. This situation shows that both countries should proceed on the same ground in terms of what needs to be done and the approaches needed.

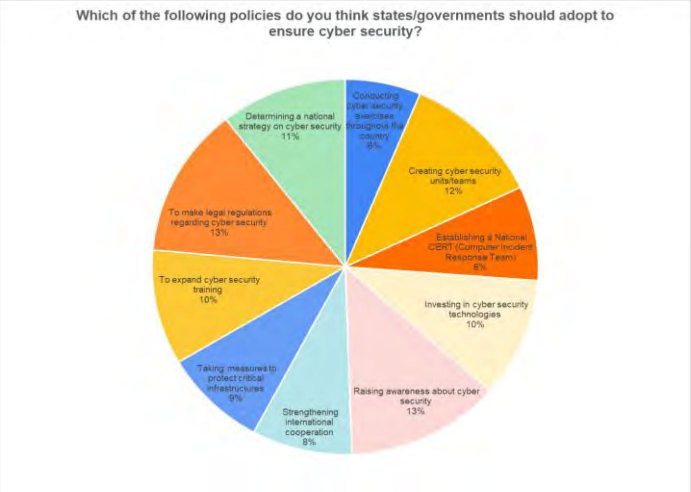

Figure 18 Policy Making

When asked what policies governments should enact to guarantee cyber security, participants had a range of responses. As Figure- demonstrates, the majority of respondents (13%) supported enacting laws about cyber security and increasing public awareness of the issue. The creation of cyber security teams or units comes next with 12%. Developing a national cyber security strategy (11%) and investing in cyber security technologies (10%) were two other widely held beliefs. Lesser amounts of time were also allocated to the following recommendations: creating a national CERT (8%) increasing cyber security training, and protecting vital infrastructures (9%).

In summary, the participants believe that to guarantee cybersecurity, both legislative and governmental actions as well as technical and operational ones should be implemented. Young people support a wide range of political policies, as evidenced by the nearly equal distribution of these measures.

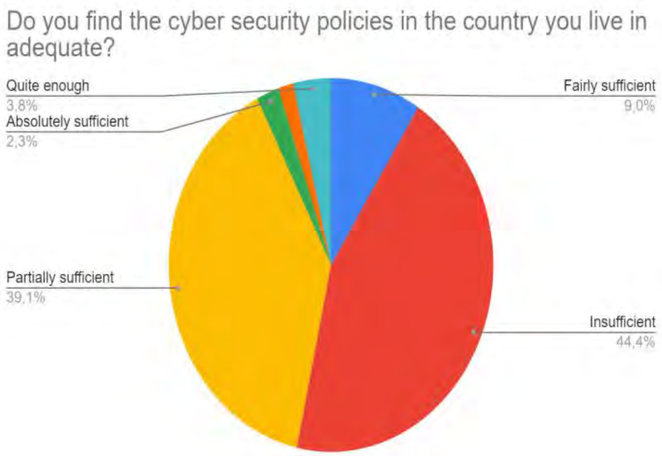

Figure 19 Cyber Security Policies in the country

The plurality of participants (44.4%) said that the cyber security policies in their country were inadequate, while 39.1% said that they were only somewhat adequate in response to the question, "Do you find the cyber security policies in the country you live in adequate?" There is a relatively small percentage of people who believe they are entirely or very sufficient. Furthermore, comprehensive interviews revealed that young individuals residing in Turkey perceived cyber security policies as inadequate, whilst those residing in Italy perceived them as somewhat adequate. Nonetheless, the findings indicate that the youth in both nations are dissatisfied with their respective governments' policies. One could argue that young people's expectations are not being met by the laws and security precautions implemented.

Nations must reevaluate their cyber security policies and tactics while considering the requirements and desires of the youth. Increasing youth knowledge and strengthening legislative rules are essential for good cyber security.

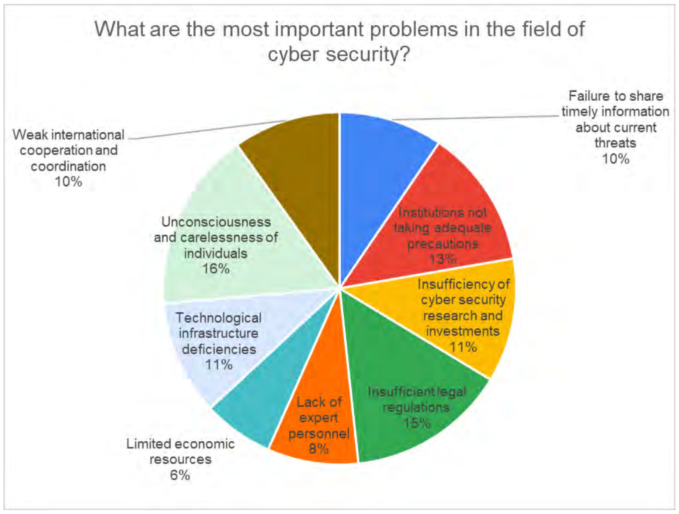

Figure 20 Problems of CyberSecurity

When questioned in the study "What are the most important problems in the field of cyber security?" participants indicated that the largest issue was people's negligence and lack of understanding, coming in at 16%. Comprehensive interviews corroborated this outcome as well. The main issue, according to young people in Italy and Turkey, is negligence and a lack of awareness. In this sense, young people in Turkey make up a larger majority, though.

With 15% of the vote, inadequate legal regulations came in second place. Compared to young people in Italy, those living in Turkey believe that legal regulations are less adequate. Other notable issue areas include inadequate investments in and research on cyber security (11%), as well as inadequate safety measures adopted by organizations (13%).

Other issues in the 10–11% range included a lack of international coordination and collaboration, inadequate technology infrastructure, scarce financial resources, a shortage of specialist workers, and a failure to promptly exchange knowledge about emerging dangers. Young Italians perceived a greater issue as the lack of specialized professionals.

Therefore, systemic factors including policy, the legal system, research, investment, cooperation, and competence are major concerns, as well as individual ignorance. Because cyber security is multifaceted, it is recognized that comprehensive solutions are needed at the individual, institutional, and global levels.

As a result, when the approaches of both countries in terms of policies and interview results are evaluated, Italy is a country that adopts and acts according to EU policies on cybersecurity, is a founding member of the European Cybersecurity Agency ENISA, and has its headquarters in Italy, and has made active strides in cybersecurity with the enactment of the Cybersecurity Framework Law in 2013 (Bianchi, 2022). Turkey, on the other hand, has a more passive policy on cybersecurity than Italy, with UN and NATO cooperation and a more disorganized legal framework (Kutlu et. al. 2019). However, surveys and interviews show that in terms of cybersecurity, young people between the ages of 18-27 living in both countries feel insecure and find the policies of the countries they live in insufficient. Although young people living in Italy feel more secure than in Turkey, this rate does not make a big difference.

Some significant findings regarding the attitudes of young people in Turkey and Italy toward gender and cybersecurity are revealed by in-depth interviews and surveys. Most respondents generally link cybersecurity to privacy and personal data protection, and they cite data security and cyberattack vulnerability as their top worries. There is a lack of satisfaction with cybersecurity methods and rules. Divergent views exist regarding how gender affects how cyber security is perceived. In both countries, women feel more insecure and see themselves as more vulnerable to cyber-attacks. To sum up, the most important things that need to be done are raising awareness of cybersecurity, making improvements to procedures and policies, and advancing gender equality. The degree of cybersecurity awareness and conduct among people and organizations needs to be raised.

Conclusion

Cybersecurity issues are too important to ignore as the internet becomes more and more involved in our everyday lives. In this study, we looked at how young people, ages 18 to 27, saw the internet and cybersecurity, and what they knew about it. We were able to gauge participant knowledge, experience, and awareness of cybersecurity and cyberbullying thanks to the data. In addition to assessing the policies of the nations in which they reside, the questionnaire and interview research sought to gauge the cybersecurity and gender-based trust of young people in Turkey and Italy. The results indicate that youth in both nations do not feel secure when using the internet. A considerable proportion of participants reported having encountered cyber-attacks, with spoofing and harassment being the most prevalent forms of attacks. Cyberbullying is a serious threat and a source of concern for most young people.

It was determined that gender has a significant impact on cyberbullying as well as overall internet safety. It was also noted that in the gender-based approach, the probability of women being subjected to cyberbullying was higher for both male and female participants. This demonstrates how intricate the connection is between gender and cyber security. Young people claim to know too little about cyber security and are dissatisfied with the laws and regulations in place in their nations.

Reaction tactics to cyberbullying also differ. Blocking and reporting appear to be the most widely used tactics. Some individuals, though, would rather talk about cyberbullying than nothing at all. These various reaction techniques represent several methods for handling cyberbullying.

Interviews and surveys show that the biggest concern of young people in cyberspace is to be able to protect their cyber data and avoid being cyberbullied. Since young people experience cyberbullying especially on social media platforms, which is the most used area by young people, ensuring the security of these platforms has emerged as a very important issue for the youth of both countries.

It has been discovered that, notwithstanding the differences in their approaches to international collaboration and policy, young people in Italy and Turkey share similar views on cybersecurity in the great majority of instances.

In conclusion, this study has improved our understanding of young people's awareness, experience, and knowledge of cybersecurity and cyberbullying. It has been observed that women are more victimized, especially in cyberbullying. Dissatisfaction with cybersecurity policies and regulations is a common trend that stands out in both countries. Topics like how gender affects these experiences and how to respond to cyberbullying could be useful for further study. The findings suggest that there is a need for more cybersecurity awareness and education among young people. States should, therefore, also evaluate and enhance their cyber security regulations. Adequate policies involving several stakeholders are necessary to ensure that youths can use the Internet more safely.

Future studies that compare this problem across national borders will add to the body of knowledge. Furthermore, assessing the efficacy of cyber security education initiatives can be a significant field of study.

References

[1] Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

[2] Bianchi, G. (2023). National Cybersecurity Strategy Launched: the Italian Breakthrough in Cybersecurity. https://www.sangfor.com/blog/cybersecurity/italian-breakthrough-in-cybersecurity Access Date: 7 November 2023.

[3] Brown, D., & Pytlak, A. (2019). Why Gender Matters in International Cyber Security https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf Access Date: 7 November 2023.

[4] Cavelty, M. D. (2015). Cybersecurity. In A. Collins (Ed.), Contemporary Security Studies (pp. 400-416). Oxford University Press. ISBN: 9780198862192

[5] Cavelty, M., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. St Antony's International Review, 15(1), 37-57. Available at SSRN:https://ssrn.com/abstract=3403971

[6] Kahraman, S., Kutlu, Ö., & Dinçer, S. (2019). Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Politikalarının Analizi. Assam Uluslararası Hakemli Dergi, 13, 1-14. https://dergipark.org.tr/tr/pub/assam/issue/48907/570664 Access Date: 7 November 2023.

[7] Lindsay, J. R. (2016). Stuxnet and the limits of cyber warfare. Security Studies, 25(1), 121-148. DOI:10.1080/09636412.2013.816122

[8] Millar, K., Shires, J., & Tropina, T. (2021). Gender Approaches to Cybersecurity: Design, Defence and Response. United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01

[9] Radu, C., & Smaili, N. (2022). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure. Journal of Business Ethics, 177, 351–374. https://doi.org/10.1007/s10551-020-04717-9

[10] Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. https://doi.org/10.1017/9781316822524

[11] Sjoberg, L. (2016). Gendering global conflict: Toward a feminist theory of war. Columbia University Press. **ISBN:**9780231148610

[12] Tickner, A. B. (2001). Gender in international relations: Feminist perspectives on achieving global security. Columbia University Press. **ISBN:**9780231075398

[13] Tickner, A. B. (2005). Gendering world politics: Issues and approaches in the post-Cold War era. Columbia University Press. **ISBN:**9780231113663