European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com

e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2023.11.02.45

**ICMC 2023**
**The 3rd International Conference on Management and Communication**

# ROTU'S PERSPECTIVE ON CYBER-SECURITY IN MALAYSIA: BALANCING AWARENESS AND SECURITY THREATS

Mohd Dino Khairri Shariffuddin (a)*, Laila Suriya Ahmad Apandi (b),
Zainal Amin Ayub (c), Muslimin Wallang (d), Ram Al Jaffri Saad (e),
Uni. W. Sagena (f), Mariah Darus @ Mat Junus (g)
* Corresponding author

(a) Asian Institute of International & Diplomacy (AIIAD)/ School of International Studies Universiti Utara Malaysia, Malaysia, dino@uum.edu.my
(b) Asian Institute of International & Diplomacy (AIIAD)/ School of International Studies Universiti Utara Malaysia, Malaysia, laila@uum.edu.my
(c) School of Law, Universiti Utara Malaysia, Malaysia, Malaysia, z.amin@uum.edu.my
(d) School of Government, Universiti Utara Malaysia, Malaysia, Malaysia, muslimin@uum.edu.my
(e) Tunku Puteri Intan Safinaz School of Accounting, Universiti Utara Malaysia, Malaysia, ram@uum.edu.my
(f) Faculty of Social and Political Sciences, Mulawarman Universitas, Indonesia, unisku@unmul.ac.id
(g) School of Government, Universiti Utara Malaysia, Malaysia, Malaysia, mariah.darus@uum.edu.my

## Abstract

Despite being a non-traditional social issue, cybersecurity is crucial in the context of technology development. The objective of this study is to investigate the level of awareness, perceived threat, and cybersecurity tools used by Reserve Officer Training Units (ROTUs) at public universities in Malaysia. A total of 2261 respondents, consisting of ROTU cadets participated through a Google Form Link. The study employed a quantitative method to conduct this population study. The primary objectives of this study were to assess the awareness level of cybersecurity among ROTU cadet respondents and to explore their perceptions regarding cybersecurity as a potential threat to the country. The findings of the study indicate that a significant majority of ROTU cadet respondents demonstrated a satisfactory level of awareness concerning cybersecurity. The results revealed that the majority of ROTU cadets associated cybersecurity predominantly with information technology. Additionally, they showed awareness of cybersecurity concepts such as hacking, protecting networks, safeguarding digital systems, and the role of cybersecurity in fostering innovation within the main database. Furthermore, the study found that a substantial majority of ROTU cadet respondents strongly agreed with the notion that cybersecurity represents a novel threat to the country. This indicates that these respondents perceive cybersecurity as a critical concern with the potential to pose significant risks to the nation's security and stability. Further research could explore specific areas where awareness might be lacking and design targeted interventions to enhance cybersecurity knowledge among ROTU cadets and other relevant groups.



*Keywords:* Cybersecurity, IR4.0, Non-Traditional Security, ROTU

https://doi.org/10.15405/epsbs.2023.11.02.45
Corresponding Author: Mohd Dino Khairri Shariffuddin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

## 1. Introduction

In the current digital era, cybersecurity has taken on greater significance. The swift advancement of technology and the emergence of the Fourth Industrial Revolution (IR4.0) have heightened the urgency to safeguard against cyber threats. The term cybersecurity pertains to the measures taken to secure electronic devices, networks, and sensitive information against unauthorized access, theft, or harm. Cyber threats can manifest in several ways, such as hacking, phishing, malware, ransomware, and social engineering attacks. The origins of these threats can vary and may come from cybercriminals, hacktivists, nation-states, and even insiders.

Generally the Reserve Officer Training Unit (ROTU) program is offered at all 20 public universities in Malaysia, including Universiti Utara Malaysia (UUM), Universiti Sains Malaysia (USM), Universiti Teknologi MARA (UiTM), Universiti Malaya (UM), Universiti Putra Malaysia (UPM), Universiti Teknologi Malaysia (UTM), and Universiti Kebangsaan Malaysia (UKM). However, there may be variations in the types of ROTU programs offered at each institution. While some universities offer all three types of ROTU programs, which include Wataniah, Royal Malaysian Naval Volunteer Reserve (PSSTLDM), and Royal Malaysian Air Force Volunteer Reserve (PSSTUDM), others offer only one or two of these programs. For instance, universities such as UUM, USM, UiTM, Universiti Malaysia Pahang (UMP), and UPNM offer all three types of ROTU programs.

Meanwhile universities such as UM, UPM, UTM, and Universiti Malaysia Terengganu (UMT) offer only Wataniah and PSSTLDM, while Universiti Malaysia Sarawak (UniMAS) and Universiti Malaysia Kelantan (UMK) offer Wataniah and PSSTUDM. Universiti Sultan Zainal Abidin (UniSHA) offers only PSSTUDM, and UKM, Universiti Tun Hussein Onn Malaysia (UTHM), Universiti Malaysia Perlis (UniMAP), Universiti Perguruan Sultan Idris (UPSI), Universiti Sains Islam Malaysia (USIM), and Universiti Teknikal Malaysia (UTEM) offer only the Wataniah program.

## 2. Problem Statement

Cybersecurity has primarily been associated with businesses and organizations operating in a digital environment, as noted by Wallang et al. (2022). While digital environments have brought convenience, freedom in trade and knowledge sharing, and other opportunities, the mismanagement of technology has resulted in negative connotations such as scams, viruses, and cyber threats. Cybersecurity threats have traditionally been focused on businesses and organizations, as supported by various academic studies, including those conducted by (Alahmari & Duncan, 2020; Bada & Nurse, 2019; Mat et al., 2020; Nobles & Burrell, 2018; Soong et al., 2020; Wallang et al., 2022). A successful cyber-attack can have grave consequences, such as financial losses, harm to reputation, and potential national security risks. In this present day, nearly sixty percent of commercial transactions are now conducted via digital wallets or online platforms (Wallang et al., 2022). The virtual agreement between parties without knowing or seeing each other has given rise to challenges, particularly when it comes to personal data protection. Given its gravity, cybersecurity has emerged as a primary concern for individuals, enterprises, and governments worldwide.

https://doi.org/10.15405/epsbs.2023.11.02.45
Corresponding Author: Mohd Dino Khairri Shariffuddin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

These studies have highlighted that the proliferation of digital environments has given rise to non-traditional security challenges, with direct implications for national security, encompassing military systems, social movements, and economic growth. Given the evolving landscape of cybersecurity threats, it has become imperative to delve into its awareness within military contexts, which often present more dangerous and complex challenges to manage. To address these objectives, the research will employ a rigorous and systematic approach, drawing on relevant literature and existing studies to establish a comprehensive foundation for the investigation.

Cybersecurity entails protecting computer systems, networks, and digital devices from unauthorized access, theft, damage, or other harmful attacks. This involves the implementation of diverse technologies, procedures, and policies to ensure the confidentiality, integrity, and availability of digital data. A cybersecurity breach can lead to dire consequences, such as financial harm, harm to reputation, and the exposure of confidential data. Hence, it is crucial for individuals and organizations to make cybersecurity a top priority and undertake requisite measures to safeguard their digital assets.

Cybersecurity is also can be highlights as cyber-attacks that have the potential to cause severe damage to a nation, even leading to loss of life as view according to Alexander (2023). Dayat (2017) states that cyber security involves computer hackers who often target government systems to steal sensitive information and cripple important services. They can achieve this by using viruses, spamming, mail bombing, disabling official websites, altering classified data, and disrupting financial systems. Such threats can have serious negative implications for a country, potentially leading to chaos and paralyzing its economy and society.

Cybersecurity entails employing technology, protocols, and practices to safeguard internet networks, devices, software, and information from unapproved access, harm, or attacks by third parties who are not accountable to individuals or organizations (Fuad & Yusof, 2022). Additionally, the goal of cybersecurity is to safeguard devices, software, data, and mobile devices, such as smartphones, to meet the needs of people against any type of cyber-attack (Boletsis et al., 2021; Ncubukezi et al., 2021). Consequently, mismanaging cybersecurity can lead to numerous cyber-crimes that may be committed directly or indirectly by individuals or groups. These crimes can include stealing private data or destroying devices, among others (Alahmari & Duncan, 2020; Fuad & Yusof, 2022; Hassan, 2022; Pitchan et al., 2017).

## 3. Research Questions

Drawing upon the concept of cybersecurity and the earlier discussed studies emphasizing threats primarily directed at businesses and organizations with far-reaching implications for national security, military systems, social movements, and economic growth, this research has outlined four primary objectives. Firstly, the study seeks to what the level of cybersecurity awareness among ROTU cadets. Secondly, it aims to examine which various instruments related to cybersecurity. Thirdly, the research endeavours to determine whether cybersecurity constitutes a significant security threat to the nation. Lastly, based on the insights derived from the preceding three objectives, this paper aims to know to what necessity for the Malaysian Armed Forces (ATM) to prepare and develop their cybersecurity capabilities in response to the prevailing cybersecurity landscape.

https://doi.org/10.15405/epsbs.2023.11.02.45
Corresponding Author: Mohd Dino Khairri Shariffuddin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

## 4. Purpose of The Study

This article aims to comprehensively analyse various aspects of cybersecurity, focusing on aspects such as awareness levels, categorization of cybersecurity as either recent threats or not, related instruments, and the need for cybersecurity development preparedness and spending within the ATM. These facets are crucially linked to strategies for safeguarding and enhancing national defence. To achieve this objective, the study has selected the ROTU cadets as the population under investigation. The rationale behind this choice lies in the ROTU cadets' involvement in the ongoing technology revolution and their specialized training, which emphasizes the prioritization of national security. The study will delve into the awareness level of ROTU cadets regarding cybersecurity. It will explore their knowledge and understanding of cybersecurity concepts, including potential threats and preventive measures. By examining the awareness levels among ROTU cadets, the research aims to gauge the readiness of future military leaders in addressing cybersecurity challenges. Instruments related to cybersecurity will also be explored, encompassing various tools, technologies, policies, and strategies employed in safeguarding digital assets and information. Understanding the available instruments is critical to crafting effective cybersecurity measures for the nation's defence.

## 5. Research Methods

Prior to commencing the report writing process, the research data obtained from the Google Forms link and the relevant literature review underwent comprehensive analysis to address the research question and fulfil the established objectives. In this study, the survey method was employed as the research methodology. The survey involved the utilization of a Google Form link questionnaire, comprising 25 queries, which was distributed to the entire population of ROTU cadets (2261 respondents) across 20 public universities in Malaysia. The response rate was considered successful when all 2261 respondents had completed the questionnaire. The 25 queries were categorized into three main sections. The first section focused on gathering personal data from the respondents. The second section cantered around assessing ROTU cadet interest in joining the ROTU program. Lastly, the third section consisted of carefully crafted questions aimed at capturing the perspectives of ROTU cadets concerning cybersecurity. This section delved into topics related to instruments pertinent to cybersecurity, the level of cybersecurity concern for the nation, and the necessity for the ATM to prepare and develop cybersecurity capabilities, all of which aligned with the research objectives.

To ensure clarity and ease of comprehension for the respondents, the questionnaire questions were formulated in a straightforward manner. The scale used for responses encompassed three categories. The first category involved respondents selecting between "yes," "no," or "unsure." The second category offered a range of options, including "strongly agree," "agree," "unsure," "disagree," or "strongly disagree." Lastly, the third category allowed respondents to indicate multiple instruments related to cybersecurity that they were familiar with or considered relevant. To disseminate the questionnaire, the Google Forms link was shared with the ROTU cadets through their respective ROTU cadet officers, utilizing a list of names provided for distribution purposes.

https://doi.org/10.15405/epsbs.2023.11.02.45
Corresponding Author: Mohd Dino Khairri Shariffuddin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

In the initial phase of the study, a pilot test was conducted to ensure the validity and reliability of the questionnaire. The pilot test involved 30 ROTU cadets, who were randomly selected to participate. The objective of the pilot test was to assess the effectiveness of each item in the questionnaire and ascertain its suitability for inclusion in the final study. Upon analysing the results of the pilot test, it was found that each item in the questionnaire performed satisfactorily. This outcome provided confidence in the questionnaire's ability to effectively measure the intended constructs related to cybersecurity awareness and knowledge among ROTU cadets. As a result, the validated questionnaire was then integrated into a Google Form link for widespread distribution to the broader population study.

The quantitative approach was adopted for this research, enabling the collection of numerical data and facilitating statistical analysis. This method allowed the researchers to gain a comprehensive understanding of the respondents' awareness and knowledge levels pertaining to the practice domain of cybersecurity. Utilizing the Google Form Link as the data collection tool offered several advantages. Its online distribution enabled the researchers to efficiently reach a large and geographically dispersed sample size, comprising ROTU cadets from different public universities. This broad representation enhanced the study's external validity and provided valuable insights into the cybersecurity awareness and knowledge levels among ROTU cadets within the broader Malaysian context.

Figure 1 illustrates the distribution of survey participants among 2261 ROTU respondents in 20 public universities. The sample size is deemed significant as it covers the entire population of ROTU cadets in public universities. The tabulated data in Figure 1 also displays the number of respondents from each university, providing an insight into the distribution of participants across the participating institutions. The distribution of ROTU respondents, indicating variations in the number of respondents across different universities. This discrepancy is attributed to the diverse enrolment of ROTU cadets within each university, leading to different sample sizes for the study. This information is vital for the study's external validity as it enables generalization of the results to the entire population of ROTU cadets in public universities. Therefore, the information displayed in Figure 1 is an essential component of the study's methodology and reinforces the credibility and dependability of the research outcomes.

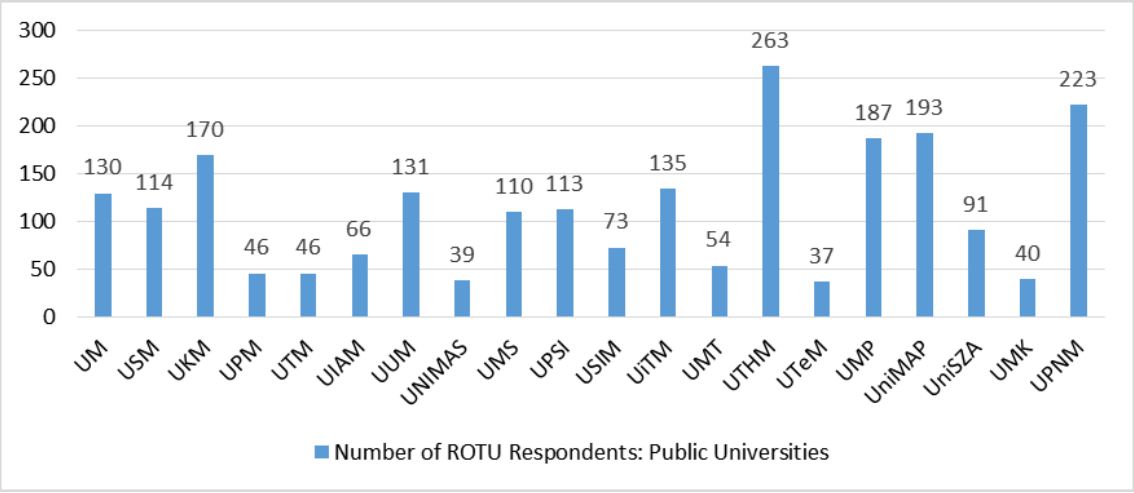


**Figure 1.** The Number of Respondent in Every Public University

https://doi.org/10.15405/epsbs.2023.11.02.45
Corresponding Author: Mohd Dino Khairri Shariffuddin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

In addition, Figure 2 provides an illustration of the distribution of respondents among the three types of ROTU programs: Wataniah, PSSTUDM, and PSSTLDM. According to the chart, most of the ROTU cadets who took part in the study were registered in the Wataniah program, representing 1574 respondents (69.6%). The second most represented group of respondents were those from the PSSTUDM program, with 530 cadets (23.4%). The smallest group of respondents were from the PSSTLDM program, with 157 cadets (7.0%). The graphical representation of this data allows for a quick and easy understanding of the distribution of respondents across the three ROTU programs, which is important for interpreting the findings of the study.

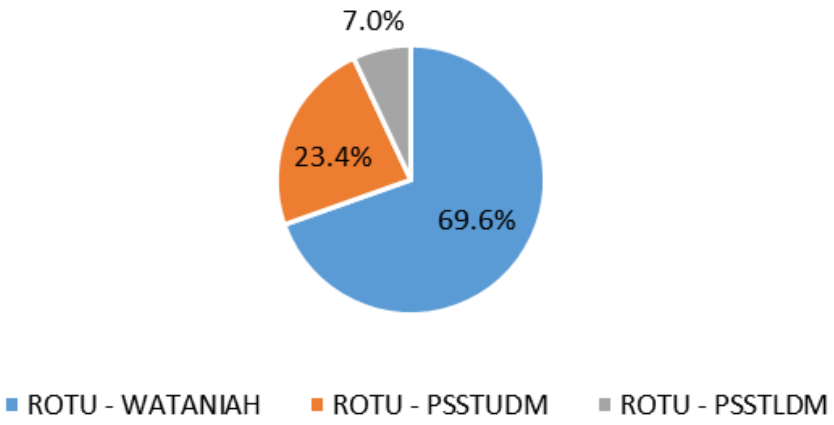


**Figure 2.** The Percentage Number of ROTU from Three Categories

Furthermore, this study has focused on examining gender differences among ROTU cadets by analysing responses from both male and female cadets. It is noteworthy that the sample size for both male and female ROTU cadets is almost equal, as shown in Figure 3. Specifically, the study has received responses from 1151 female cadets (50.9%) and 1110 male cadets (49.1%). Ensuring an equal representation of both genders in the study is a crucial component of the research methodology that enhances the validity and reliability of the study's findings.

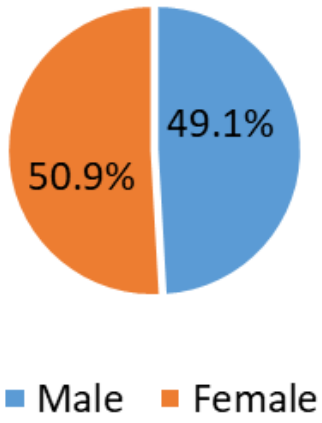


**Figure 3.** The Percentage ROTU Cadet Respondents Based on Gender

https://doi.org/10.15405/epsbs.2023.11.02.45
Corresponding Author: Mohd Dino Khairri Shariffuddin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Additionally, secondary data from a range of sources, including books, journals, theses, online materials, magazines, and newspapers, were also utilized in the research. This comprehensive approach, which incorporated both primary and secondary data sources, allows for a more thorough understanding of the research topic. Adhering to established academic practices for data collection and analysis, and utilizing multiple sources of information, increases the validity and reliability of the study's findings.

In this research, descriptive analysis techniques were used, specifically frequency analysis. This statistical method by using Excel involves summarizing data by calculating the frequency or occurrence of values or categories within a dataset. Frequency analysis enables the researcher to generate a frequency table or graph that displays the distribution of the data. This technique provides insights into the characteristics of the dataset, including the identification of patterns, trends, and outliers. The results of frequency analysis can be used to guide further analysis and aid decision-making in the research process. The descriptive analysis involved calculating the amount and percentage scores, which facilitated a comprehensive summary of the respondents' performance in the domain of awareness and knowledge.

In addition, the research has employed cross-tabulation as a statistical technique to investigate the relationship between several categorical variables. Cross-tabulation involves creating a table that demonstrates the frequency distribution of the variables, where the cells in the table correspond to the intersection of two categories. By using different methods to analyse cross-tabulation tables, such as calculating proportions or percentages of each cell with respect to the total number of observations, insights into the association between variables can be gained. This approach is useful for recognizing trends or patterns in the data.

After data collection, statistical analysis was conducted on the gathered data to identify any patterns or relationships. The outcomes were then utilized to draw conclusions and provide recommendations based on the research question and objectives. The survey method was deemed a suitable approach for this study as it allowed for the gathering of a significant volume of data from a diverse pool of participants. Furthermore, the use of statistical techniques to analyse the quantitative data facilitated the provision of impartial insights into the research question.

## 6. Finding: The ROTU and Cybersecurity

### 6.1. The awareness of cybersecurity based on ROTU different gender perspective

The level of cybersecurity awareness among the ROTU respondents was assessed using a three-category scale, consisting of "yes", "no", and "unsure". This categorization was chosen to effectively capture and examine the respondents' awareness regarding cybersecurity-related concepts and practices. By utilizing this scale, the study aimed to discern whether ROTU respondents possessed knowledge and understanding in the domain of cybersecurity. The "yes" category indicated that the respondents exhibited awareness, while the "no" category denoted a lack of awareness on the specific cybersecurity aspect. The "unsure" category allowed respondents to express uncertainty or ambiguity regarding their awareness, providing valuable insights into potential gaps or areas requiring further clarification. Employing this three-category scale offered a clear and concise method to evaluate the level of cybersecurity awareness among ROTU cadets. It facilitated straightforward data analysis, enabling the researchers to draw

https://doi.org/10.15405/epsbs.2023.11.02.45
Corresponding Author: Mohd Dino Khairri Shariffuddin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

meaningful conclusions about the respondents' familiarity with cybersecurity-related topics and their implications for the military context.

Figure 4 presents the percentage distribution of male and female ROTU cadet respondents' awareness of cybersecurity. The awareness of cybersecurity from among ROTU respondents has measured by either the ROTU respondents choose either yes, no or unsure. It is evident from the table that a large majority of both male and female ROTU cadet respondents are aware of cybersecurity, with 1001 male cadet respondents (90.2%) and 999 female cadet respondents (86.8%) indicating awareness. A small proportion of male and female ROTU cadet respondents are not aware of cybersecurity, with only 41 male cadet respondents (3.7%) and 42 female cadet respondents (3.6%) indicating lack of awareness. Moreover, some male and female ROTU cadet respondents are unsure about cybersecurity, with 68 male cadet respondents (6.1%) and 110 female cadet respondents (9.6%) indicating uncertainty.

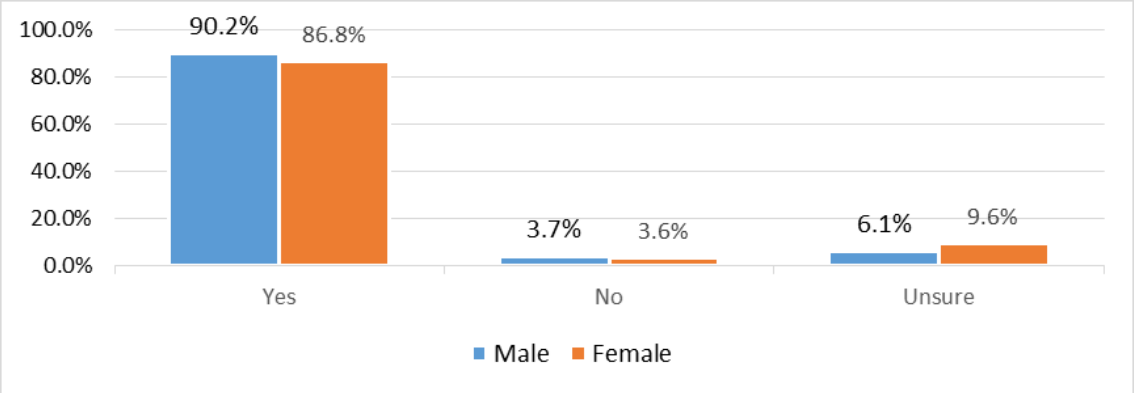


**Figure 4.** The Awareness of Cybersecurity based on ROTU Gender

### 6.2. Cybersecurity as new threat based on ROTU different gender perspective

To assess the perception of cybersecurity as a new threat, the study employed a five-category scale, encompassing the following response options: "strongly agree", "agree", "unsure", "disagree", and "strongly disagree". This categorization was deliberately chosen to comprehensively gauge the respondents' awareness and views regarding the potential status of cybersecurity as a novel threat to the country. By utilizing this scale, the researchers aimed to obtain nuanced and differentiated responses from the respondents. The "strongly agree" and "agree" categories indicated a high level of agreement with the notion that cybersecurity represents a new threat. Conversely, the "disagree" and "strongly disagree" categories signified a dissenting perspective, suggesting a belief that cybersecurity is not a recent or significant threat. The "unsure" category allowed respondents to express uncertainty or lack of clarity regarding their stance on cybersecurity as a new threat. This option was crucial in capturing varied viewpoints and acknowledging the complexity of the subject matter. Employing the five-category scale offered a comprehensive and granular approach to examining the respondents' awareness and perceptions regarding cybersecurity as a new threat to the country. The data obtained through this scale provided valuable insights into the prevailing attitudes and concerns surrounding cybersecurity's potential impact on national security

https://doi.org/10.15405/epsbs.2023.11.02.45
Corresponding Author: Mohd Dino Khairri Shariffuddin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Figure 5 provides insights into the perceptions of ROTU cadet respondents towards cybersecurity as a new threat for the country. The data indicates that a majority of male ROTU cadet respondents, with 671 respondents (60.5%), and a significant proportion of female ROTU cadet respondents, with 538 respondents (46.7%), strongly agree that cybersecurity is a new threat towards the country. Additionally, 327 male ROTU cadet respondents (29.5%) and 426 female ROTU cadet respondents (37%) agree that cybersecurity poses a new threat for the country. On the contrary, a small number of male and female ROTU cadet respondents disagree with this perception, with 33 male ROTU respondents (3.0%) and 38 female ROTU respondents (3.3%) respectively. Moreover, only 4 male ROTU cadet respondents (0.4%) and 4 female ROTU cadet respondents (0.3%) strongly disagree that cybersecurity is a new threat towards the country. Finally, a considerable number of ROTU cadet respondents, with 75 male ROTU respondents (6.8%) and 145 female ROTU respondents (12.6%), are unsure about whether cybersecurity is a new threat or not.

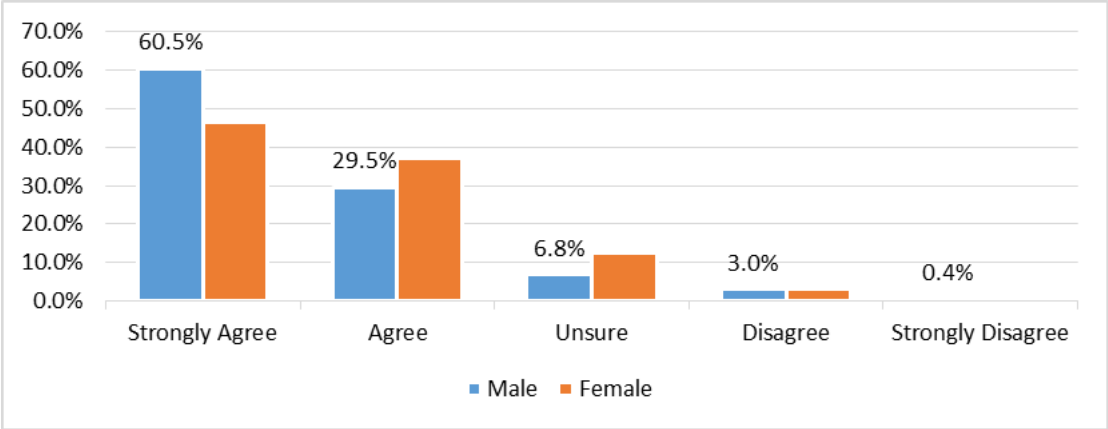


**Figure 5.** Cybersecurity as New Threat based on ROTU different Gender Perspective

### 6.3. The instruments relate with cyber security by ROTU different gender perspective

To evaluate the respondents' perception of instruments related to cybersecurity, the study utilized a five-category scale comprising the following response options: "information technology", "protecting networks", "protecting digital systems", "innovation in the main database" and "hacking." This categorization was deliberately selected to encompass a comprehensive range of instruments and aspects associated with cybersecurity practices. By utilizing this five-category scale, the researchers aimed to capture a diverse set of responses, thereby enabling a comprehensive assessment of the ROTU cadets' awareness and understanding of various instruments related to cybersecurity. Importantly, the respondents were allowed to choose more than one instrument that they perceived as relevant to the cybersecurity domain. By adopting this five-category scale and allowing for multiple selections, the study aimed to obtain a rich dataset, offering valuable insights into the diverse perspectives and preferences related to cybersecurity instruments among the ROTU respondents.

Figure 6 presents the relationship between the respondents' perception of cybersecurity and several related concepts. The data shows that 984 male ROTU cadet respondents (88.6%) and 943 female ROTU cadet respondents (81.9%) associate cybersecurity with information technology. Additionally, 897 male

https://doi.org/10.15405/epsbs.2023.11.02.45
Corresponding Author: Mohd Dino Khairri Shariffuddin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

ROTU cadet respondents (80.9%) and 874 female ROTU cadet respondents (76.1%) relate cybersecurity with hacking. Furthermore, 912 male ROTU cadet respondents (82.1%) and 690 female ROTU cadet respondents (60.1%) believe that cybersecurity is associated with protecting networks. Moreover, 817 male ROTU cadet respondents (73.7%) and 698 female ROTU cadet respondents (60.8%) associate cybersecurity with protecting digital systems. Lastly, 885 male ROTU cadet respondents (79.7%) and 866 female ROTU cadet respondents (75.4%) perceive cybersecurity as being related to innovation in the main database.

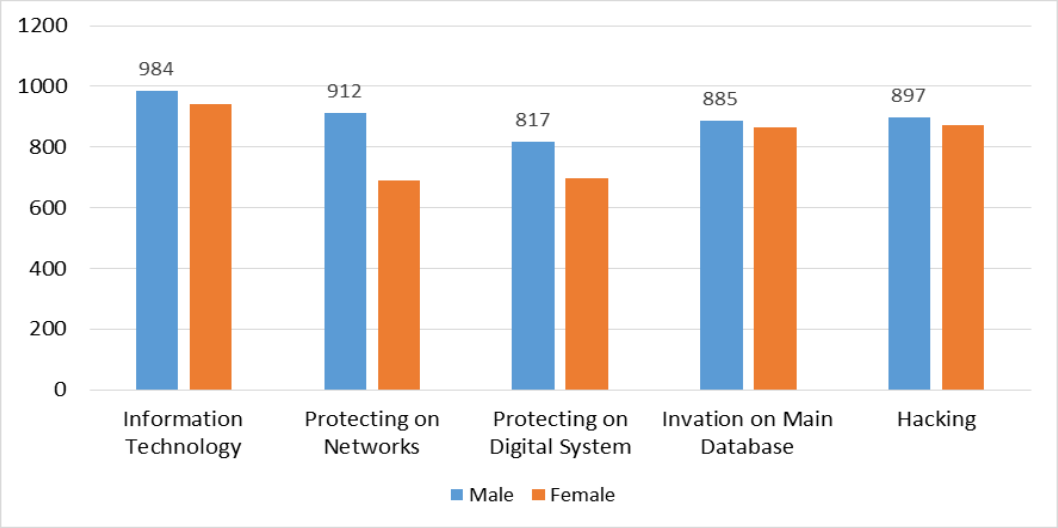


**Figure 6.** The Instruments that Relate with Cyber security by ROTU Different Gender Perspective

### 6.4. ATM and cyber security from ROTU difference gender perspective

To gauge the perception of whether the ATM should or should not prepare and develop its cybersecurity needs, the study utilized a five-category scale. This scale included the following response options: "strongly agree", "agree", "unsure", "disagree" and "strongly disagree." The deliberate selection of this categorization aimed to capture a comprehensive range of viewpoints and opinions regarding the necessity of cybersecurity preparedness and development within the military context. By employing a five-category scale, the researchers sought to obtain nuanced and differentiated responses from the respondents, allowing for a more in-depth understanding of their perspectives. The "strongly agree" and "agree" categories indicated a high level of endorsement for the necessity of enhancing cybersecurity capabilities within the ATM. On the other hand, the "disagree" and "strongly disagree" categories represented opposing views, suggesting a belief that significant investments in cybersecurity may not be warranted. The "unsure" category provided an essential space for respondents to express uncertainty or ambivalence concerning the extent to which the ATM should prioritize cybersecurity preparedness and development. This option recognized the complexity of the subject matter and allowed respondents to offer candid responses based on their knowledge and understanding.

https://doi.org/10.15405/epsbs.2023.11.02.45
Corresponding Author: Mohd Dino Khairri Shariffuddin
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Figure 7 presents the responses of male and female ROTU cadet respondents regarding the necessity for ATM to prepare and develop their cybersecurity needs. The table reveals that a significant proportion of the respondents agree with this viewpoint, with 825 male ROTU cadet respondents (74.3%) and 764 female ROTU cadet respondents (66.7%) strongly agreeing. Moreover, 251 male ROTU cadet respondents (22.6%) and 342 female ROTU cadet respondents (29.7%) also agree that ATM should prepare and develop their cybersecurity needs. However, only one male ROTU cadet respondent (0.1%) expressed disagreement and strongly disagreement on this matter. Meanwhile, a small proportion of the respondents, 32 male ROTU cadet respondents (2.9%) and 45 female ROTU cadet respondents (3.9%), were unsure about the need for ATM to prepare and develop their cyber security needs.

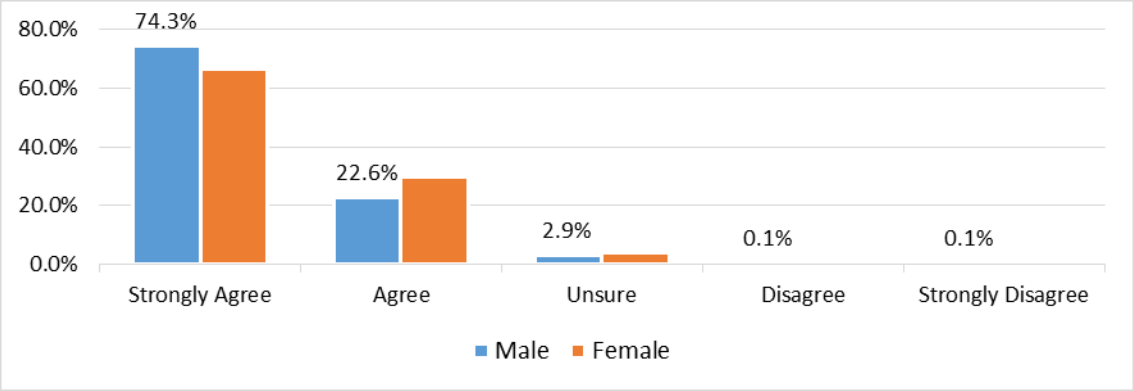


**Figure 7.** ATM Should Prepare on Cyber Security Needs Based on ROTU Difference Gender Perspective

## 7. Conclusion

In conclusion, cybersecurity has become a critical component of contemporary society due to the growing dependence on technology and the internet in our daily lives. The various cyber threats, including hacking, phishing, and malware, present a significant risk to individuals, organizations, and governments. Therefore, it is imperative to adopt proactive measures to safeguard against cyber-attacks and guarantee the security of sensitive information. One of the key measures for protecting against cyber-attacks is implementing strong passwords. In addition, it is important to use firewalls and antivirus software to prevent unauthorized access to networks and devices, and to be cautious of suspicious emails or messages that may contain malicious links or attachments. Organizations should also invest in cybersecurity training and education for their employees to raise awareness of potential threats and best practices for staying safe online. In addition, governments and international organizations should work together to develop robust cybersecurity policies and regulations to prevent cyber-attacks and prosecute cyber criminals. Taking proactive measures to safeguard against cyber threats and prioritizing cybersecurity can help mitigate the risk of data breaches, and promote the safety and security of digital information for individuals, businesses, and governments.

Despite cybersecurity being a non-traditional security issue, Malaysia must prepare for this threat, especially given the rapid growth of technology. The study found that the majority of ROTU cadets were aware of cybersecurity and agreed with the threat it posed to the country. Consequently, a significant

number of ROTU cadet respondents strongly believed that ATM should prepare and develop its cybersecurity needs. The results also showed that ROTU cadet respondents associated cybersecurity with instruments such as information technology, hacking, protecting networks and digital systems, and innovation in the main database.

## Acknowledgement

This research was supported by Ministry of Higher Education (MoHE) of Malaysia through Fundamental Research Grant Scheme (FRGS/1/2020/SS0/UUM/02/18). We also want to thank to the Government of Malaysia which provide MyBrain15 program for sponsoring this work under the self-fund research grant and L00022 from Ministry of Science, Technology, and Innovation (MOSTI).

## References

Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (CyberSA). https://doi.org/10.1109/cybersa49311.2020.9139638

Alexander, S. (2023). *Cyberwarface*. https://www.techtarget.com/searchsecurity/definition/cyberwarfare

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security, 27*(3), 393-410. https://doi.org/10.1108/ics-07-2018-0080

Boletsis, C., Halvorsrud, R., Pickering, J., Phillips, S., & Surridge, M. (2021). Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. *Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*. https://doi.org/10.5220/0010332902660274

Dayat, H. (2017). The threat of cyber war in Malaysia. In *The Journal of the Malaysian Army*, *2*(70). https://www.thestar.com.my/tech/tech-opinion/2016/01/28/facing-cyber-attacks-in-2016-and-beyond/

Fuad, N. S. M., & Yusof, A. R. M. (2022). Memahami jenayah siber dan keselamatan siber di Malaysia: suatu pemerhatian terhadap pandangan sarjana dan intelektual [Understanding on Cyber crime and cyber security in Malaysia: view from scholars and professional]. *Asian Journal of Environment, History and Heritage*, *6*(1).

Hassan, M. S. (2022). *Ancaman Keselamatan Siber* [Cyber security Threat]. My Metro.

Mat, B., Pero, S. D., Wahid, R., & Shuib, M. S. (2020). Cyber security threat to Malaysia: a small state security discourse. in sustaining global strategic partnership. *The Age of Uncertainties Proceedings of the 8th International Conference on International Studies.*

Ncubukezi, T., Mwansa, L., & Rocaries, F. (2021). Analysis and Impact of the Cybercrimes in the Western Cape Small and Medium-Sized Businesses. *International Conference on Cyber Warfare and Security, 16*, 235–425.

Nobles, C., & Burrell, D. (2018). Using Cybersecurity Communities of Practice (CoP) to Support Small and Medium Businesses. *ICIE 2018 6th International Conference on Innovation and Entrepreneurship: ICIE 2018*.

Pitchan, M. A., Omar, S. Z., Bolong, J., & Ahmad Ghazal, A. H. (2017). Analisis Keselamatan Siber Dari Perspektif Persekitaran Sosial: Kajian Terhadap Pengguna Internet Di Lembah Klang [Cyber security on the social perseptive: case study on internet user in Lembah Klang]. *Journal of Social Sciences and Humanities, 12*(2), 16–29.

Soong, K. K., Ahmed, E. M., & Tan, K. S. (2020). Factors influencing Malaysian small and medium enterprises adoption of electronic government procurement. *Journal of Public Procurement, 20*(1), 38-61. https://doi.org/10.1108/jopp-09-2019-0066

Wallang, M., Shariffuddin, M. D. K., & Mokhtar, M. (2022). Cyber security in small and medium enterprises (smes): what's good or bad? *Journal of Governance and Development (JGD), 18*(1), 75-87. https://doi.org/10.32890/jgd2022.18.1.5