European Journal of Social Sciences Studies
ISSN: 2501-8590
ISSN-L: 2501-8590
Available on-line at: www.oapub.org/soc

DOI: 10.46827/ejsss.v11i3.2032 Volume 11 | Issue 3 | 2025

SECURING TOMORROW'S LEADERS OF AN INSTITUTIONAL SAFETY NET FOR STUDENTS' PROTECTION IN SOCIAL MEDIA RECRUITMENT TO TERRORISM: THE CASE OF STATE UNIVERSITIES AND COLLEGES IN DAVAO REGION, PHILIPPINES

Rommel V. Recla[i]
Associate Professor, PhD,
College of Development and Management,
University of Southeastern Philippines,
Philippines

Abstract:
This policy research investigates the awareness levels of students in State Universities and Colleges (SUCs) within Davao Region on the risk of social media recruitment into terrorism. With the increase of digital reliance during the COVID-19 pandemic, the rise of cyber threats and extremist exploitation through online platforms, this study explores the need for institutional safety nets that protect students from digital radicalization. Utilising a mixed-methods approach, this study employed descriptive statistics, exploratory factor analysis, and inferential tests to examine the socio-demographic profile of students and identify key protective dimensions. Results revealed two major components: (1) Institutional Safeguarding Frameworks for Heightened Awareness and Information Sensitivity, (2) Global Knowledge Synthesis for Holistic Mitigation. Further, findings underscore significant differences in perception based on gender, year level, and type of gadget use, among female, first-year students and those students engaged in school organizations, expressing higher awareness levels. Through this, the study recommends urgency for policy reforms, institutional frameworks and global strategies tailored to equip SUCs with proactive measures against cyberterrorism recruitment and thereby reinforcing the digital resilience and safety of the students.

Keywords: bridging gaps, needs analysis, effective research community extension program

[i] Correspondence: email rommel.recla@usep.edu.ph

1. Introduction

Cybersecurity is a worldwide concern that calls for government involvement, especially from Filipino youth and students. Various concerns about social media recruitment for terrorism call for a thorough "Whole-Nation Approach" from law enforcement, security and public safety organizations. Aside from it's a global security threat, there is a lack of understanding and engagement in its implementation. A remarkable disparity between hearing and understanding was exacerbated by the cultural outcomes of individuals, which is crucial to bridge this gap and develop an effective policy response against the so-called social media avenue recruitment into terrorism. The transition towards digital control was accelerated because of the COVID-19 pandemic, which prompts organisations to reevaluate their goods, services and digital infrastructure that requires careful attention and sustained diligence (The Asia Foundation, 2022). The presence of technological advancements raises concerns such as security, privacy, ethical and strategic concerns (Fortiss, 2020).

During pandemic time, cybercriminals swiftly adapted to the "new normal", exploiting emerging vulnerabilities and reshaping their tactics to match evolving digital landscapes (Alawida *et al.*, 2022; Furnell *et al.*, 2021; Murashkin & Tyravainenm, 2020). With that, the report showed that cyberattacks surged in 2020 and 2021 with no indication of slowing down in 2022. In the long run, these threats grew more sophisticated, integrating advanced techniques and tools into their arsenals (Saeed *et al.*, 2023; Jasiwal *et al.*, 2022; Tariq *et al.*, 2023).

The professionalisation of cybercrime led to high-impact campaigns that often affect unintended targets and increase the complexity of response and prevention mechanisms (Aslan *et al.*, 2023; Castillon, 2023; Jaiswal *et al.*, 2022). At the international level, institution like NATO continues to face challenges in counter terrorism. This is due to the fragmented and evolving nature (Brangetto & Veenendaal, 2016; Salmon, 2022; Maschmeyer, 2022; Sukumar, 2022).

Cyberspace and IoT have exposed developed societies to new threats, which make them more vulnerable to targeted cyberterrorism due to their increased reliance on electronic communication and commerce (Adap, 2023; Zeiger & Gyte, 2020). The internet and mobile penetration globally reached 57% and 42% which creates an interconnected environment, and ideas may be positive or harmful, but are still rapidly shared (Froment *et al.,* 2017; Mohammadi *et al.*, 2020; Filho *et al.*, 2021). These days, various digital platforms are being exploited by terrorists to disseminate propaganda, polished videos, and recruit followers and donors online (Burker, 2016).

Relative to this, Adap's (2023) study highlighted critical insight into how technological progress and social media are being weaponised by terrorist organizations. These groups have transformed themselves into highly organized digital networks. Moreover, it was emphasised by Tariq *et al.* (2023) that vulnerabilities in hyperconnected systems, particularly in IoT networks, compromised the confidentiality, integrity and

availability of critical infrastructure, which called for the revision of existing legislation of the Cyber Prevention Act to ensure alignment of present digital threats (Adap, 2023). Clearly, it is stated in the studies that there is a gap in institutional capacity, government regulation, and market responses, which contributed to the increase in cyberterrorism.

2. Policy Research Questions

The study aims to address the following inquiries comprehensively:

1) What is the socio-demographic profile of students from SUCs in terms of:
a) age;
b) gender;
c) year level;
d) membership in a school organization;
e) geographical location (address);
f) gadgets;
g) commonly used social media platforms?

2) What are the dimensions of an institutional safety net for students' protection in social media recruitment to terrorism?

3) Is there a significant difference between the identified dimensions for students' protection in social media recruitment to terrorism when grouped according to socio-demographic profile?

3. Literature Review

Cybersecurity lies in its intangible and complex nature, which makes it difficult to communicate to a broader public (de Burjin & Janssen, 2017). Perhaps the inadequacy of cybersecurity awareness is a direct result of these complexities. Supporting this perspective, Carcary *et al.* (2019) and Jones *et al.* (2018) highlighted the evolving nature of cybersecurity threats and the corresponding urgency for proactive educational and institutional responses.

This shows a deficit in cybersecurity awareness, but also the existence of moral hazards where gaps in public understanding, institutional policy and risk communication have been the vulnerabilities which can be exploited. UK interests and nationals face increased global risk due to instability in Iraq and Syria, necessitating increased vigilance and international collaboration during radicalization and extremist mobilization (Gross *et al.*, 2017).

To discuss, in the Philippine context, the rise of ISIS-East Asia was considered the most lethal terrorist threat, further that Daulah Islamiya-Lanao, the Abu-Sayaf Group, Bangsamoro Islamic Freedom Fighters (BIFF) and other elements of Moro Islamic Liberation Front (MILF) (Country Report, 2021). The Philippines experienced terrorist activity targeting civilians and security forces, often using IEDs in 2021. In fact, a notable

incident included bus bombings and a volleyball court explosion. The BIFF was reportedly responsible. UK Counter-Terrorism Policing's 2023 strategic communication highlights a credible threat of terrorist attacks in high-traffic urban areas.

Figure 1 shows that factors such as gender, year level, and gadget usage significantly contribute to an institutional safety net for students' protection against social media recruitment to terrorism. Female students, first-year students, and school organizations are more likely to agree on these measures.

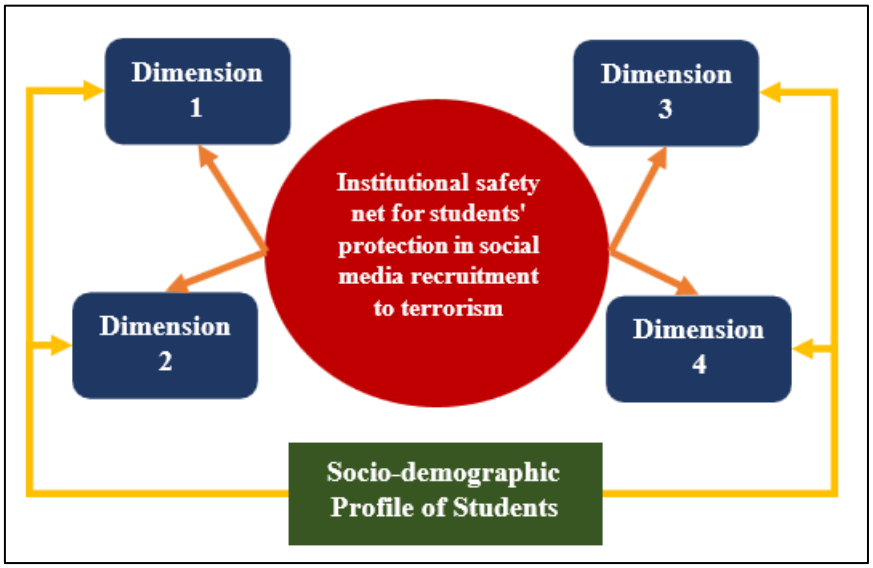

Figure 1: Analytical Framework of the Study

4. Methodology

The study will make use of three different statistical tools for each of the different policy research questions, which are as follows:

1) Descriptive Statistics to describe the socio-demographic profile of the respondents of the study;
2) Exploratory Factor Analysis to pinpoint which are the necessary dimensions of an institutional safety net for students' protection in social media recruitment to terrorism; and
3) Independent Samples t-test and Analysis of Variance (ANOVA) to determine whether there is a significant difference in the dimensions of an institutional safety net for students' protection in social media recruitment to terrorism when grouped according to their socio-demographic profile.

5. Results, Interpretation and Analysis

5.1 Socio-demographic Profile of Students

5.1.1 Age

Based on the visual presentation below, most respondents who participated in the survey are nineteen (19) years old (124), followed by twenty year (20) old students (106), and eighteen-year-old students (86). The youngest respondent is seventeen years (17) old while the oldest is a forty-two (42) year old college student.

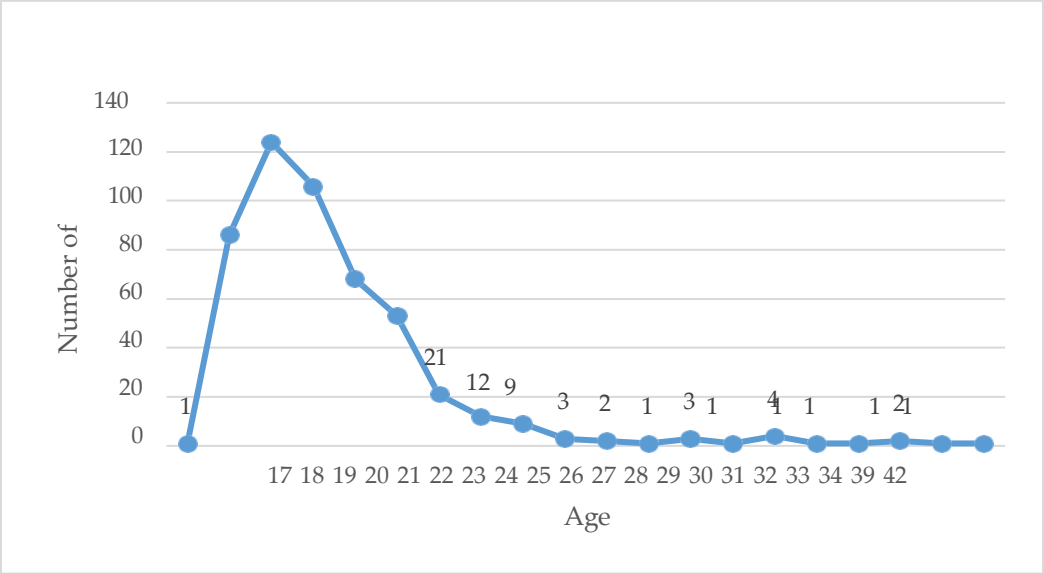

Figure 2: Distribution of Students According to Age

5.1.2 Gender

The table shows the distribution of respondents according to gender, wherein the majority of them are female students, comprising three hundred fifty-six (356) out of 500. The rest are male (140), bisexual (2), and respondents who preferred not to say their gender (2).

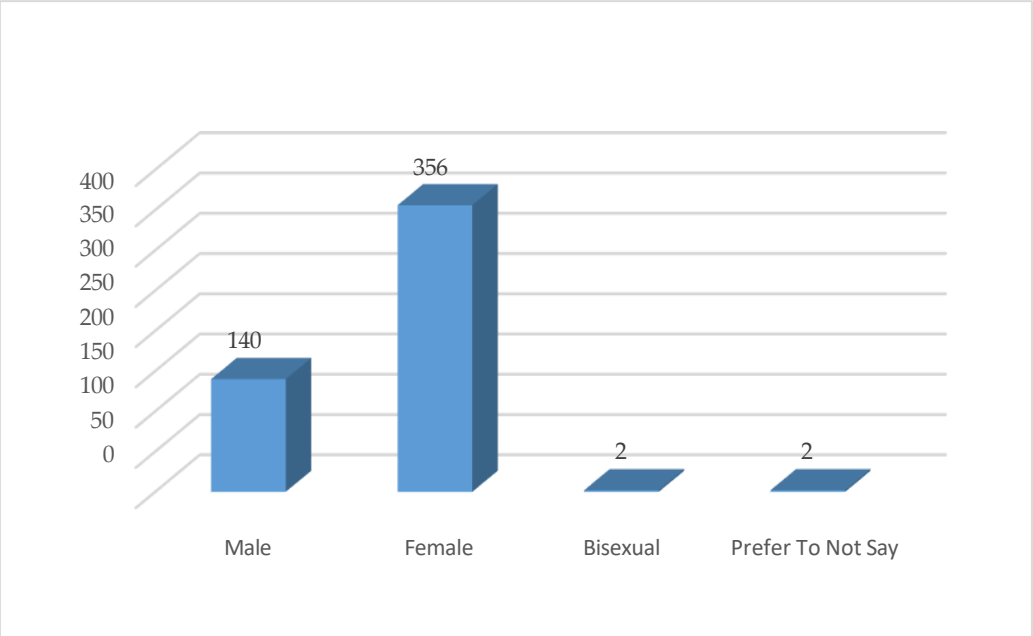

Figure 3: Distribution of Students According to Gender

5.1.3 Year Level

According to the result, two hundred eighty-one (281) respondents are freshmen students, while one hundred fifteen (115) respondents are in their junior year. Ninety (90) respondents are in their second year, while the remaining fourteen (14) out of 500 are in their senior year.

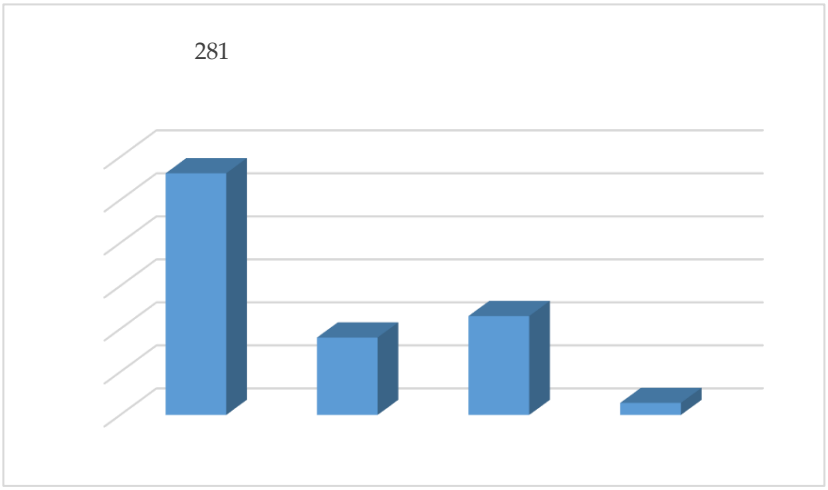

Figure 4: Distribution of Students According to Year Level

5.1.4 Membership in School Organization

Accordingly, two hundred ninety-five (295) respondents are members of various school organizations, while the rest (205) are local student councils, music, and dance–related organizations.

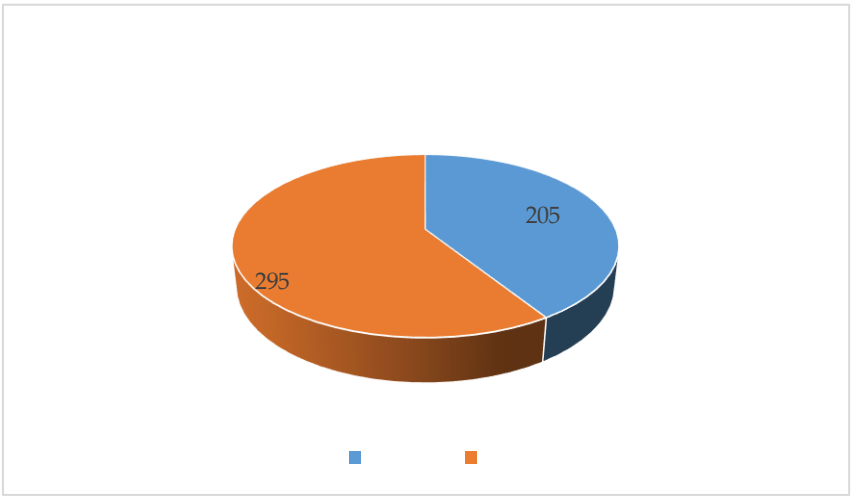

Figure 5: Distribution of Students According to Organization Membership

5.1.5 Geographical Location of Address

Accordingly, most of the respondents (294) of the study come from the rural areas of Davao Region. The rest are from the urban part (206), particularly Davao City.

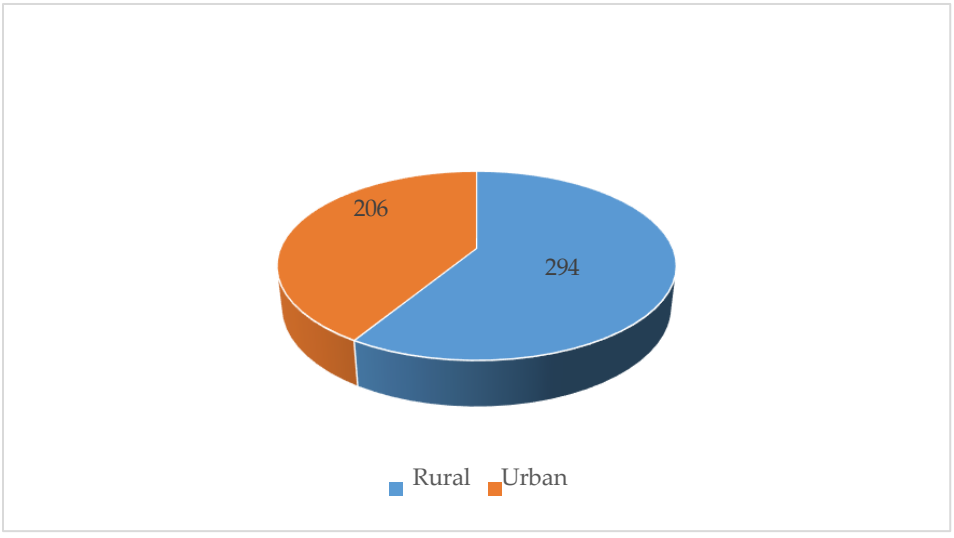

Figure 6: Distribution of Students According to their Home's Geographical Location

5.1.6 Gadget Owned

The majority of the students, or four hundred seventy (470) respondents, own cell phones with access to data/internet. The rest of the data are as follows: sixteen (16) respondents have cell phones without access to data/internet, eleven respondents (11) have laptops with access to data/internet, two (2) respondents have laptops but without access to data/internet, and one (1) respondent has a desktop computer with access to data/internet.

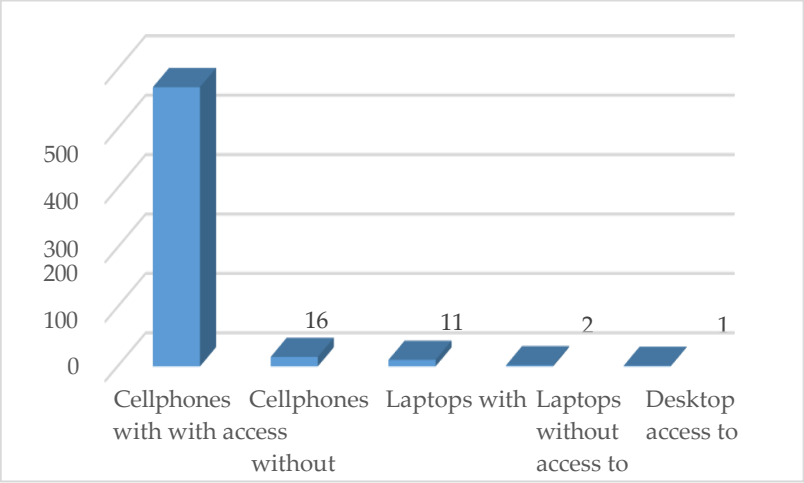

Figure 7: Distribution of Students According to the Gadgets They Own

5.1.7 Commonly Used Social Media Platform

The most common social media platform among the respondents is Facebook, followed by YouTube, Instagram, Twitter, and LinkedIn. Google, Viber, Telegram, and TikTok are almost in the same range but are less used than the former platforms.

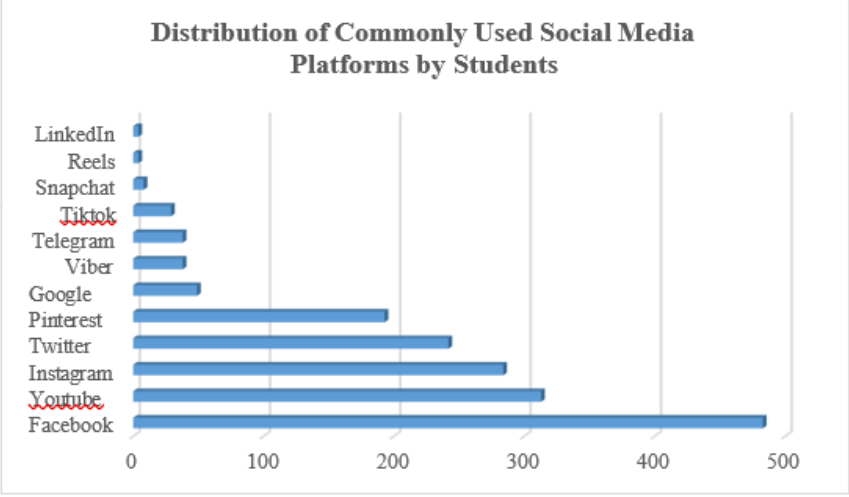

Figure 8: Distribution of Commonly Used Social Media Platforms by Students

5.2 Factors of Institutional Safety Nets for Students' Protection in Social Media Recruitment to Terrorism

5.2.1 Sampling Adequacy Requirement

Analyzing the result of Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity provided a result of 0.970, chi-square value of 7121.480, and significance value set at 0.000. This is an indication that the sampling adequacy is marvellous.

In relation, Bartlett's test of sphericity is used to assess the suitability of the sample. According to the result as presented in the same table below, the value of Bartlett's test is 0.000, less than the significance value of 0.001 (Field, 2013), thus confirming that the sample is suitable to be utilized in the study and factor analysis is an appropriate treatment for the study.

Table 1: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.970
Bartlett's Test of Sphericity	**Approx. Chi-Square**	7121.480
	df	190
	Sig.	.000

5.2.2 Factor 1: Institutional Safeguarding Frameworks for Heightened Awareness and Information Sensitivity

The first factor determined based on the result of Exploratory Factor Analysis is comprised of nine (9) statements and are as follows: being a student, safety measures are existing in SUCs regarding the guidelines of the students' handbook particularly protection in social media to terrorism (0.681); being a student, safety measures are provided by the SUCs administration for students' protection in social media to terrorism (0.797); being a student, safety measures are well-informed to students by their respective SUCs especially on the importance of privacy settings and the risks of sharing sensitive information online (0.695); being a student, safety measures are developed by the management of SUCs to guide and protect students on responsible and secure use of social media platforms (0.702); being a student, safety measures are put in place for students' protection in social media to terrorism (0.709); being a student, safety measures are discovered initiatives that focus on improving students' digital literacy (0.605); being a student, safety measures are introduced to students to critical thinking skills in order to revolve and react to social media responsibly (0.623); being a student, safety measures are explored for the development and effectiveness of monitoring systems within the educational institutions to detect signs of terrorization and provide timely intervention (0.622); and being a student, safety measures are taught to students for its use of technological tools and platforms to monitor cases relative to students' protection in social media to terrorism (0.599).

This factor underscores the need to educate students on the use of privacy settings and the risks associated with sharing sensitive information on social media. There is a

need to reevaluate SUCs' efforts on heightening awareness about online privacy, to encourage students to adopt protective behaviors that might expose them to terrorist recruitment and radicalization.

In addition, there is also a need to consider the idea of adding safety measures in student handbooks, particularly regarding social media protection against terrorism. Comprehensive guidelines established by SUCs to regulate student behavior online and provide clear protocols for maintaining safety and security within digital environments are necessary.

Heightened awareness among students about cyberattacks is identified as the most favorable factor influencing an organization's cyber-resilience strategy. The cyber capabilities of an organization are seen to advance alongside the comprehension of cyber risks by other pertinent stakeholders and their recognition of their personal roles and responsibilities in mitigating these risks (as outlined in a Cybersecurity Outlook Insight Report, 2023). These capabilities include a focus on addressing the impact on students' mental health along with sensory perception and cognition aspects, which, according to Gross *et al.* (2017), is frequently disregarded.

Table 2: Dimension 1: Institutional Safeguarding Frameworks for Heightened Awareness and Information Sensitivity

No	Statement	Score
1	Being a student, safety measures exist in SUCs regarding the guidelines of the students' handbook, particularly **protection in social media to terrorism**.	0.681
2	Being a student, safety measures are **provided by the SUCs administration for students' protection** from terrorism on social media to terrorism.	0.797
3	Being a student, safety measures are well-informed to students by their respective SUCs, especially on the **importance of privacy settings and the risks of sharing sensitive information** online.	0.695
4	Being a student, safety measures are **developed by the management of SUCs** to guide and protect students in the responsible and secure use of social media platforms.	0.702
5	Being a student, safety measures are put in place for students' **protection in social media** to terrorism.	0.709
6	Being a student, safety measures are **discovered initiatives** that focus on improving students' digital literacy.	0.605
7	Being a student, safety measures are introduced to students to develop **critical thinking skills** in order to respond to social media responsibly.	0.623
8	Being a student, safety measures are explored for the **development and effectiveness of monitoring systems** within educational institutions to detect signs of terrorization and provide timely intervention.	0.622
9	Being a student, safety measures are taught to students for the use of technological devices, tools and platforms to **monitor cases related to students' protection** in social media and terrorism.	0.599

The second factor determined based on the results has a corresponding eleven (11) statements and are as follows: being a student, safety measures are used to reduce the risk and impact of online recruitment to terrorism (0.704); being a student, safety

measures are studied and analyzed programs that enhance students' awareness to online threats and potential terrorization (0.667); being a student, safety measures are offered insights into effective educational policies realistic to students' protection in social media to terrorism (0.591); being a student, safety measures are regarded for the role of counselling services in addressing students' vulnerabilities and promoting mental health, reducing the risk of terrorization (0.567); being a student, safety measures are established by the global efforts and best practices in countering online terrorization (0.626); being a student, safety measures are informed policies to students' protection in social media to terrorism that can be adapted to the local context (0.697); being a student, safety measures are reflected in the evaluation methodologies to assess the effectiveness of safety net mechanisms (0.670); being a student, safety measures are looked at as strong partnerships between educational institutions and law enforcement agencies (0.652); being a student, safety measures are reinforced preventive nets against online recruitment to terrorism (0.748); being a student, safety measures are put in place of having an existing office and assigned personnel for students' protection in social media to terrorism (0.776); and, being a student, safety measures are held accountable by supervising and managing for development and administration on students' protection in social media to terrorism (0.782).

This factor emphasizes the adoption of comprehensive risk reduction strategies by aligning with international safety protocols. It highlights the importance of utilizing recognized frameworks from around the world to diminish the risk and impact of online recruitment by terrorist organizations, thereby reinforcing the resilience of students against extremist threats.

According to Adap (2023), terrorist groups can establish a cyber-battlefield to expand their sphere of influence within the realm of ideas because of their adoption of new models and partnerships in technological innovation. Moreover, these groups leverage advanced technology as a strategic vantage point, integrating social media platforms into their communication systems and strategies.

That is why, by leveraging insights from international best practices, it will contribute to refining educational policies that protect students who are not immune to these cyber terrorism threats. In addition, synthesizing global knowledge on preventive measures will enhance students' awareness and preparedness against the multifaceted nature and modern era of social media-based terrorism.

Table 3: Dimension 2: Global Knowledge Synthesis for Holistic Risk Mitigation

No	Statement	Score
10	Being a student, safety measures are used to **reduce the risk and impact of online recruitment** to terrorism.	0.704
11	Being a student, safety measures are studied and analyzed programs that **enhance students' awareness** to online threats and potential terrorization.	0.667
12	Being a student, safety measures offer **insights into effective educational policies relevant** to students' protection in social media to terrorism.	0.591
13	Being a student, safety measures are regarded as a **role of counselling services** in addressing students' vulnerabilities and promoting mental health, reducing the risk of terrorization.	0.567
14	Being a student, safety measures are **established by the global efforts and best practices** in countering online terrorization.	0.626
15	Being a student, safety measures are **informed policies for students' protection in social media** to terrorism that can be adapted to the local context.	0.697
16	Being a student, safety measures are reflected in the **evaluation methodologies** to assess the effectiveness of safety net mechanisms.	0.670
17	Being a student, safety measures are looked at as **strong partnerships** between educational institutions and law enforcement agencies.	0.652
18	Being a student, safety measures are **reinforced, such as preventive nets** against online recruitment to terrorism.	0.748
19	Being a student, safety measures are put in place to protect students from existing office and assigned personnel for students' protection in social media to terrorism.	0.776
20	Being a student, safety measures are held accountable by supervising and managing for the development and administration of students' protection in social media to terrorism.	0.782

Significant difference between the identified dimensions for students' protection in social media recruitment to terrorism when grouped according to socio demographic profile.

5.2.3 Age

In terms of age, the results showed that there is no statistically significant difference between the mean scale scores of the dimensions (p1<0.368; p2<0.345). This can be interpreted as the respondents having the same viewpoint when it comes to the importance of institutional safety nets for the protection of students in social media recruitment to terrorism.

Table 4: ANOVA Results for Age

		Sum of Squares	df	Mean Square	F	Sig.
Dimension1	Between Groups	.797	3	.266	1.054	.368
	Within Groups	124.946	496	.252		
	Total	**125.742**	**499**			
Dimension2	Between Groups	.891	3	.297	1.109	.345
	Within Groups	132.858	496	.268		
	Total	**133.749**	**499**			

5.2.4 Gender

According to the results of the one-way ANOVA presented below, there is a statistically significant difference in terms of gender when it comes to the mean scale scores for both dimensions used in the study (p1<0.000; p2<0.001). Upon using the Tukey post hoc test, it is revealed that female respondents have higher mean scale scores compared to the other genders. Additionally, there is a significant difference between the mean scale scores of female and male respondents (p<0.000), while no statistically significant difference for the rest of the respondents with different genders.

Table 5: ANOVA Results for Gender

		Sum of Squares	df	Mean Square	F	Sig.
Dimension 1	Between Groups	4.880	3	1.627	6.675	.000
	Within Groups	120.863	496	.244		
	Total	**125.742**	**499**			
Dimension 2	Between Groups	4.640	3	1.547	5.942	.001
	Within Groups	129.109	496	.260		
	Total	**133.749**	**499**			

5.2.5 Year Level

There is a statistically significant difference in the mean scale scores of respondents for both dimensions identified in the study when it comes to year level (p1<0.027; p2<0.007). A closer look using the Tukey post hoc test showed that there is a difference in the responses between first- and third-year respondents, while it is the opposite for the rest of the year levels included in the analysis. In addition, respondents who are in their first year of university have higher mean scale scores compared to the rest of the respondents.

Table 6: ANOVA Results for Year Level

		Sum of Squares	df	Mean Square	F	Sig.
Dimension 1	Between Groups	2.304	3	.768	3.086	.027
	Within Groups	123.438	496	.249		
	Total	**125.742**	**499**			
Dimension 2	Between Groups	3.193	3	1.064	4.044	.007
	Within Groups	130.556	496	.263		
	Total	**133.749**	**499**			

5.2.6 Membership in Organizations

According to the result of the independent samples t-test, there is no significant difference in the mean scale scores for both dimensions in terms of the respondents' membership to organizations (p1<0.347; p2<0.145). However, it can be noted that respondents who are members of the university have higher mean scale scores compared to those who are not.

Table 7: T-test Results for Membership in Organization

		Levene's Test for Equality of Variances		t-test for Equality of Means			
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference
Dimension 1	Equal variances assumed	.886	.347	.195	498	.846	.00877
	Equal variances not assumed			.194	481.116	.846	.00877
Dimension 2	Equal variances assumed	2.132	.145	.069	498	.945	.00322
	Equal variances not assumed			.069	475.384	.945	.00322

5.2.7 Geographical Location

At a 0.05 significance level, there is no significant difference in the mean scale scores of respondents according to geographical location. This indicates that the students, whether they are from rural or urban areas, have the same disposition when it comes to the importance of safety nets on social media against terrorism.

Table 8: T-test Results for Geographical Location

		Levene's Test for Equality of Variances		t-test for Equality of Means			
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference
Dimension 1	Equal variances assumed	.007	.931	-.994	498	.321	-.04533
	Equal variances not assumed			-.997	445.920	.319	-.04533
Dimension 2	Equal variances assumed	2.773	.097	-1.370	498	.171	-.06440
	Equal variances not assumed			-1.357	426.193	.175	-.06440

5.2.8 Gadgets Used

For this socio-demographic profile, while there is a statistically significant difference for the mean scale scores of the first dimension in terms of gadgets used by the respondents, it is the contrary for the second dimension ($p1<0.005$; $p2<0.265$). In relation, the variable 'laptop without internet' has the lowest mean scale scores among the rest of the options for gadgets used in the study.

Table 9: ANOVA Results for Gadgets Used

		Sum of Squares	df	Mean Square	F	Sig.
Dimension1	Between Groups	3.754	4	.938	3.808	.005
	Within Groups	121.989	495	.246		
	Total	125.742	499			
Dimension2	Between Groups	1.400	4	.350	1.309	.265
	Within Groups	132.349	495	.267		
	Total	133.749	499			

6. Conclusions

Based on the analysis of the results from the previous section, the researcher came up with the following conclusions: Two dimensions, namely **Institutional Safeguarding Frameworks for Heightened Awareness** and **Information Sensitivity** and **Global Knowledge Synthesis for Holistic Risk Mitigation** were identified, focusing on the exigency for endemic safety nets for students' protections against social media recruitment for terrorism, as well as anchoring on globalized safety protocols.

The urgency for an institutional safeguarding framework in state universities and colleges is paramount for the students to have heightened awareness against cyber-attacks and recruitment of terrorism on social media. As mentioned in the previous section, an organization and its stakeholders, in this case, the students, need to have heightened awareness in terms of cyber risks and the role they play in mitigating these risks and vulnerabilities.

In relation, SUCs have to emphasize the necessity to adopt global risk reduction strategies against terrorism on social media. With the abrupt change in the way students use the internet after the COVID-19 pandemic, there is a necessity to have educational policies for students to be protected against cyber threats. These strategies may be leveraged from international best practices focused on reinforcing and reinventing student resiliency against extremist threats.

In terms of socio-demographic profile, the test of difference showed that while there is a statistically significant difference among components of gender, year level, and the gadgets used by students, it is the opposite for age, membership to organization, and the geographical address of the students. Regardless, a closer look indicated that female students, those who are in their first year, and are members of school organizations agree more with the statements relative to students' protection against social media recruitment for terrorism, compared to their counterparts.

7. Recommendation

Students from state universities and colleges, which constitute a large chunk of the youth demographic in the Philippines, play a huge role in addressing the challenge of cybersecurity. Their accessibility with social media, which brings them closer to the allure

of recruitment by terrorists, can be instead used to address this challenge. With this, and based on the conclusions defined above, the researcher was able to formulate this recommendation for the study:

- The revaluation of the Cybercrime Prevention Act of 2012 and the National Action Plan for Countering Violent Extremism, with the intent of incorporating institutional safety nets focused on addressing extremist activities on social media platforms. The policy reframing may consider the participation of state universities and colleges towards heightened awareness of students, as well as global benchmarking on best holistic practices against cyber terrorism.
- Establish a mandatory, regular cybersecurity and information sensitivity training program for all employees, contractors, and stakeholders. This training program should focus on identifying security threats (e.g., phishing, malware), proper data handling practices, and the use of secure communication channels.
- Create a formal policy for continuously synthesizing global knowledge and research in the cybersecurity domain, ensuring the institution remains aware of, and adapts to, evolving international security challenges. Establish a dedicated global risk monitoring team or working group responsible for integrating global best practices, emerging threats, and international regulatory requirements into the institution's safeguarding framework.
- For future researchers, it may help for further evidence and result-based and proactive policy reframing that there will be more studies on the same topic of institutional safety nets by SUCs against cyber terrorism, but with a different scope or locality in the country.

Conflict of Interest Statement
The authors declare no conflicts of interest.

About the Author(s)

Rommel V. Recla (PhD), Associate Professor, College of Development Management
University of Southeastern Philippines (USeP) – Mintal Campus.

- **Academic Background**
  - Licensed Professional Teacher
  - Over 20 years of experience in academia and professional practice
  - Teaches undergraduate and graduate courses in logic, ethics, applied social ethics, administrative ethics, and public service ethics
- **Current Roles**
  - **Associate Professor II**, College of Development Management, USeP (2014–present)
    - Faculty member involved in instruction, research, and extension programs focused on public safety and security, rural and urban development
  - **Coordinator, National Service Training Program (NSTP)**, USeP Mintal Campus (2024–2025)
  - **Research Adviser**, Public Safety Officers Senior Executive Course (PSOSEC), National Police College–Davao Campus (2017–present)
  - Former **Coordinator, Mintal Campus Student Council (MinCSC), Office of Student Affairs and Services**, and **Graduate School Head and Program Head**, College of Development Management, USeP (2014–2020)
- **Research Interests**
  - Public safety and security
  - Cybersecurity and digital governance
  - Rural and urban development
  - Peacebuilding and conflict-sensitive development
  - Ethics in public administration and governance
- **Selected Achievements**
  - Best Action Research Paper: *Development of Outcome-Based Framework of Executive Order No. 70 Series of 2018: The Case of Davao Occidental*
  - Best Oral Presenter: *Dimensions of Compliance of Local Government Units with the Clean Water Act in the Region of Davao*
  - Best Action Research Paper: *Development of Violent Extremism Governance Model in Conflict Context*
- **Professional Contributions**
  - Mentors senior law enforcement professionals in research and policy studies
  - Designed and enhanced graduate-level curricula in Development Management
  - Led initiatives to strengthen student support services, expand community outreach, and foster research culture at USeP

- **Academic Profiles**
  - ORCID: https://orcid.org/0000-0003-2209-0812
  - Academia.edu: https://usep.academia.edu/rommelrecla
  - ResearchGate: https://www.researchgate.net/profile/Rommel-Recla?ev=hdr_xprf
- **Contact:**

Email: rommel.recla@usep.edu.ph

References

Adap, Johanna S. (2023). The Cyber Battleground: An Analysis of the Use of Social Media for Terrorist Recruitment. Retrieved from https://ndcp.edu.ph/the-cyber-battleground-an-analysis-on-the-use-ofsocial-media-for-terrorist-recruitment/

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of COVID-19: A survey. *Journal of King Saud University Computer and Information Sciences, 34*(10), 8176-8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333. https://doi.org/10.3390/electronics12061333

Brangetto, P., & Veenendaal, M. A. (2016, May). Influence cyber operations: The use of cyberattacks in support of influence operations. In 2016, the 8th International Conference on Cyber Conflict (CyCon) (pp. 113-126). IEEE. Retrieved from https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf

Burke, P. (2016). It is Time to Shine a Light on the Islamic State's Hidden Executions. War on the Rocks, 20. Retrieved from https://warontherocks.com/2016/09/it-is-time-to-shine-a-light-on-the-islamic-states-hidden-executions/

Carcary, M., Doherty, E., & Conway, G. (2019, July). A framework for managing cybersecurity effectiveness in the digital context. In European Conference on Cyber Warfare and Security (pp. 78–86). Academic Conferences International Limited. Retrieved from https://mic.elsevierpure.com/en/publications/a-framework-for-managing-cybersecurity-effectiveness-in-the-digit

Data Reportal (2019). Digital 2019: Global Digital Overview. Retrieved from https://datareportal.com/reports/digital-2019-global-digital-overview.

de Bruijn, H. and Janssen, M. (2017). Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies. *Government Information Quarterly, 34*, 1-7. https://doi.org/10.1016/j.giq.2017.02.007

Fortiss (2020). AI Engineering: Progressing towards Robust and Trustworthy AI Systems. Retrieved from

https://www.fortiss.org/fileadmin/user_upload/06_Ergebnisse/Studien_und_Roadmaps/fortiss_report_AI_Engineering_en_web.pdf.

Froment, F., García González, A. J., & Bohórquez, M. R. (2017). The Use of Social Networks as a Communication Tool between Teachers and Students: A Literature Review. *Turkish Online Journal of Educational Technology-TOJET, 16*(4), 126-144. Retrieved from https://files.eric.ed.gov/fulltext/EJ1160610.pdf

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity, 3*(1), 49-58. https://doi.org/10.1093/cybsec/tyw018

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16). https://doi.org/10.3390/s23167273

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. *Sensors, 23*(8). https://doi.org/10.3390/s23084117

The Asia Foundation (2022). Cybersecurity in the Philippines: Global Context and Local Challenges. Retrieved from https://asiafoundation.org/publication/cybersecurity-in-thephilippines-global-context-and-local-challenges/.

Zeiger, S., & Gyte, J. (2020). Prevention of radicalization on social media and the internet. International Centre for Counterterrorism (ICCT). Retrieved from https://icct.nl/sites/default/files/2023-01/Chapter-12-Handbook_0.pdf