Ways To Make Cybersecurity Education/Opportunities More Accessible in the Philippine Public School System

Joshua Oania
Old Dominion University

Ways To Make Cybersecurity Education/Opportunities More Accessible in the Philippine Public School System

Joshua Raymond Oania

Old Dominion University

COVA CCI Cybersecurity Undergraduate Research

Dr. Leigh Armistead

December 1, 2023

ABSTRACT

This paper will examine how the Philippines can make cybersecurity education more accessible in their public school system. The solutions it proposes include making cybersecurity a part of the school curriculum, creating summer/internship programs for Junior and Senior High School students in multiple different areas within cybersecurity, and providing basic infrastructure and resources for students to meet their educational needs and aspirations.

Keywords: cybersecurity, technology, education, accessibility, opportunities

INTRODUCTION

Cybersecurity is an ever-growing field in the Republic of the Philippines. Job opportunities exist in many sectors, such as financial institutions, government agencies, and healthcare. With the recent creation of the Department of Information and Communication Technologies (DICT) under the Republic Act 10844 in 2016 (Official Gazette, 2016), even more cybersecurity opportunities have been created for Filipinos.

These jobs play a vital role in the daily lives of Filipinos. However, despite the many job opportunities, there is still a huge demand for cybersecurity professionals due to the ever-growing nature of the field. According to an article written by ABS-CBN News (2023), a popular Filipino news channel, about "180,000 cybersecurity professionals are needed to cover 10 percent of companies and critical infrastructures involved in healthcare, finance, BPO, and utilities such as water, electricity, and telecommunications."

Because of this gap in cybersecurity professionals, there also exists an increased risk of cyber attacks, with the Philippines being a "hotspot" for cybercrime (National Defense College of the Philippines, 2022, para. 22). Perhaps one of the most famous is the Love Bug, otherwise known as the ILOVEYOU virus (White, 2020). It was created by Filipino Onel de Guzman in the early 2000s in order to steal the internet access passwords of the local people around him. He could do this by sending an email with an attachment that, if opened, would steal passwords, overwrite existing files, and send copies of itself to all of the victim's Microsoft Outlook contacts by exploiting a flaw in the Windows OS. Not only did it affect the Philippines, it also affected the entire world, spreading as far as other major powers and here in the US.

Another more recent yet notable cyber attack happened before the elections. Around the end of March, a group called Anonymous Philippines hacked into the website of the Philippine

Commission on The Elections (Comelec), the governing body in the Philippines responsible for administering and supervising elections (Commission on Elections, 2023). They did it to highlight the vulnerabilities of the Comelec voting system and protest against its use, which was unfortunately brushed aside (Chi, 2016). Shortly after, a group with malicious intent, called LulzSec, managed to hack into the voter database and leaked the data of over 55 million registered voters (National Defense College of the Philippines, 2022, para. 24).

The increased risk of cybercrime highlights the need for cybersecurity professionals and the importance of cybersecurity education. Fortunately, there are educational opportunities at the university and in professional settings. Universities such as Mapua University and Asia Pacific College offer cybersecurity degrees and computer science degrees specializing in cybersecurity. However, these kinds of opportunities are less readily available at the primary and secondary levels in the public school system. Most of the focus has been on core subjects such as math, science, social studies, and reading/writing, as cybersecurity is not a part of the primary curriculum. Furthermore, even if these opportunities were readily available, there needed to be more infrastructure that could support the basic educational needs of students, making it difficult for them to meet their educational goals and needs.

This paper examines how cybersecurity education/opportunities can be more accessible in the Philippine public school system.

IMPLEMENTATION OF CYBERSECURITY IN THE PUBLIC SCHOOL SYSTEM CURRICULUM

In the Philippines, formal education is structured from grades K through 12, much like in the United States. However, there are some key differences to note. Unlike in the US, where high school is structured from grades 9 through 12, high school, or Senior High School, is

structured from grades 10 through 12 (DepEd, 2016). Middle school, or Junior High School, is structured from grades 6 through 10.

In an article written back in 2018, the Philippines Department of Education (DepEd) coordinated with the Department of Information and Communications Technology (DICT) to possibly implement a cybersecurity curriculum for Senior High School students (Umali, 2018). However, as it stands during the writing of this paper, cybersecurity is not officially recognized in the public school system's formal K-12 curriculum. According to DepEd (n.d.), the Applied Track is a pathway with courses students will take to prepare them for a given career field. There are four tracks: Academic Track, Sports Track, Arts and Design Track, and the Technical-Vocational Livelihood Track. Each track has its sub-tracks/strands. The Technical-Vocational Livelihood Track has an Information and Communication Technology Strand (Computer-Systems-Servicing-NC-II-CG, n.d., p. 5). Within this strand are courses that go over essential concepts in cybersecurity. One of these courses, Computer Systems Servicing, goes over things like "1) installing and configuring computer systems, 2.) setting up computer networks, 3) setting up computer servers, and 4) maintaining and repairing computer systems and networks" IT concepts which are essential to understand in the world of cybersecurity.

However, it does exist in the ALS curriculum, falling under the Digital Literacy strand (Department Of Education, 2017, p. 31). Under Content Standard: Digital Ethics, Learning Competency 4, students go over concepts such as cyber ethics, cyber safety, cyber wellness, and cybersecurity, allowing them to "Explain different terminologies in safe and responsible use of digital technology." The ALS, which stands for Alternative Learning System, is a "parallel learning system" that exists to serve those who do not have access to formal educational means, such as people who do not have access to schools within their communities (those who live in

remote areas of the Philippines) (Department Of Education, n.d.). It gives Filipinos the opportunity to get an education. ALS is established under the Governance Act for Basic Education (Republic Act 9155). Under Article XIV, Section 2, Paragraph (1), the Philippine Constitution recognizes and encourages using educational means outside the formal education system, such as self-learning, indigenous learning systems, and other seemingly unconventional ways of learning. The ALS system has six learning strands: Communication Skills, Scientific Literacy and Critical Thinking Skills, Mathematical and Problem Solving Skills, Life and Career Skills, Understanding the Self and Society, and Digital Literacy. The difference between the two systems is that trained professionals manage the formal system in an in-person classroom setting. Meanwhile, the ALS system is volunteer-based/managed by trained ALS professionals. It is conducted in several settings in person (community centers, libraries, volunteer homes, to name a few) and online (Zoom, Google Meet, or other video conferencing platforms). The ALS system is also much more flexible than the traditional formal system as it strives to make it as convenient for people as possible.

A solution is that the Department of Education create a cybersecurity strand under the Technical-Vocational Livelihood Track of the formal curriculum and merge it with the Information and Communications Technology strand (Computer-Systems-Servicing-NC-II-CG, n.d., p. 5). The DepEd can do this by adopting the same curriculum the ALS system utilizes, specifically, Content Standard: Digital Ethics, Learning Competency 4. Implementing the ALS curriculum into the formal curriculum exposes a broader and more diverse range of people to cybersecurity, thus fostering interest in the field and bridging the gap of professionals needed. Furthermore, close collaboration between the Department of Education and the Department of

Information and Communications Technology (DICT) in further developing this curriculum is substantial as the field and technologies continuously evolve.

CREATION OF SUMMER/INTERNSHIP PROGRAMS FOR STUDENTS

Government agencies and private companies must collaborate to make cyber education more accessible for students. As the US's Cybersecurity & Infrastructure Security Agency (CISA) states, "partnerships between the public and private sectors that foster trust and effective coordination are essential to maintaining critical infrastructure security and resilience" (Cybersecurity & Infrastructure Security Agency, 2016).

There are many ways they can go about this. A solution is that relevant government agencies (DepEd, DICT) and private companies allocate funding towards creating a summer/internship program aimed towards students in Junior and Senior High School. Multiple programs in different areas should be created, allowing students to explore what the field of cybersecurity offers. The differences in skill level should also be considered when creating these programs. Though education within the classroom is essential, one of the best ways to learn and gain exposure is through hands-on experience. Creating a summer/internship program would allow students to learn and explore a possible career choice of interest, network with skilled professionals, and land a job with the same people they learned from and worked with.

There are similar initiatives that exist that the Philippines can follow. For example, the CyberCorps: Scholarship for Service (SFS) program, which the US government created in collaboration with specific universities and private companies, provides scholarships to university students in exchange for their employment for however many years they received scholarships, given that they meet specific criteria (CyberCorps®: Scholarship for Service, n.d.).

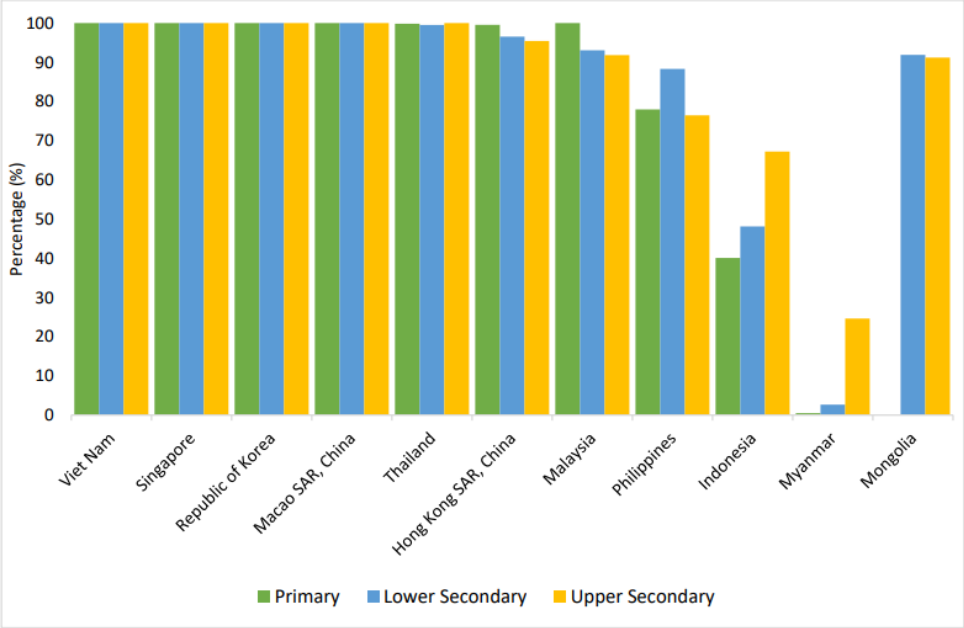
Another program in the US is that of the National Security Agency (NSA), the US equivalent of the DICT (*NSA student and internship programs*, n.d.). The NSA offers students both in high school and university summer/internship programs in many different fields of cybersecurity. Relevant government agencies in the Philippines, such as the DICT, do not offer such programs to students on these levels. Moreover, unlike the NSA, the DICT and other agencies do not have a dedicated section for student internships of all levels, making the accessibility to such programs much more difficult (DICT, n.d.).

Following the footsteps of these initiatives would prove beneficial in providing public school students the opportunities they need to flourish in the field of cybersecurity.

MORE FUNDING FOR BASIC EDUCATIONAL INFRASTRUCTURE AND RESOURCES

The government must allocate the necessary funds and resources to develop school infrastructure that will cater to the needs of students. Though a cybersecurity curriculum must be implemented in the public school curriculum, it will only be helpful if students have the basic infrastructure and resources to support their educational goals and needs. A study conducted by the Philippine Institute for Development Studies (PIDS) found that the quality of school infrastructure and access to resources in the Philippines compared to that of other Southeastern Asian countries was lacking (Navarro, p. 37). Though universal access to computers has already been achieved by schools in countries such as Vietnam, Singapore, and Korea in both the primary and secondary levels of education, the Philippines still needs to work on providing for this. Based on 2019 data collected from the UNESCO Institute of Statistics, 77.97% of students at the primary level, 88.30% at the lower secondary level, and 76.47% at the upper secondary level have computer access.

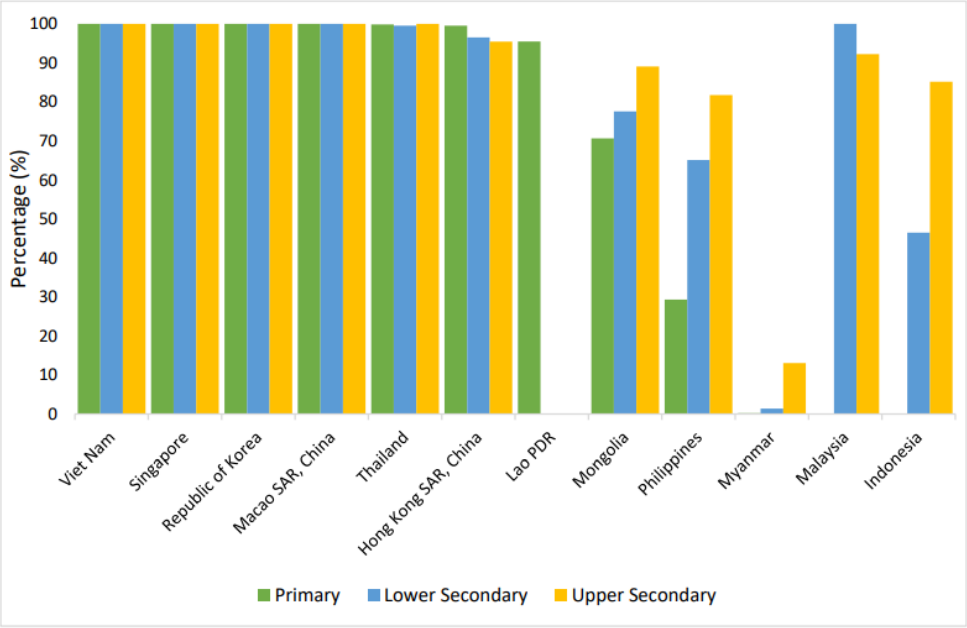
Figure 7. Schools' access to computers in Eastern and South-Eastern Asia (latest available data)



Notes: SAR = Special Administrative Region
2020 data - Viet Nam; Macao SAR, China; Thailand (primary and upper secondary); Hong Kong SAR, China
2019 data - Singapore; Thailand (lower secondary); Philippines
2018 data - Malaysia (lower secondary and upper secondary); Indonesia (primary and upper secondary); Myanmar
2017 data - Malaysia (primary); Indonesia (upper secondary)
2016 data - Republic of Korea; Mongolia

Similarly, schools in the Philippines have limited internet access, especially compared to those countries that have already achieved universal access to the internet. Based on data from 2019, 29.32% of schools in the primary levels, 65.09% have access to the lower secondary level, and 81.74% have access to the upper secondary level.

Figure 8. Schools' access to the Internet in Eastern and South-Eastern Asia (latest available data)



Notes: SAR = Special Administrative Region; Lao PDR = Lao People's Democratic Republic
2020 data - Viet Nam; Macao SAR, China; Thailand; Hong Kong SAR, China
2019 data - Singapore; Lao PDR (primary); Philippines; Malaysia (lower secondary and upper secondary)
2018 data - Myanmar; Indonesia (lower secondary and upper secondary)
2016 data - Republic of Korea; Mongolia

Source: UNESCO Institute for Statistics (2021)

By allocating more funding towards developing school infrastructure and distributing the necessary resources, it would enable students to reach their full potential.

CONCLUSION

Whether it is realized or not, cybersecurity plays an essential role in the daily lives of Filipinos. No matter what field they may be working in, whether it be in the medical field or the government, cybersecurity plays a considerable part of their roles. Given the increased risk of cybercrime in the Philippines, the government must focus on educating and empowering the youth by providing them with opportunities in and outside the classroom and the essential educational resources and infrastructure they need to reach their full potential.

REFERENCES

About Alternative Learning System | Department of Education. (n.d.). https://www.deped.gov.ph/k-to-12/inclusive-education/about-alternative-learning-system/

Chi, B. L. (2016, April 11). Philippines elections hack "leaks voter data." *BBC News*. https://www.bbc.com/news/technology-36013713

Commission on Elections. (2023, March 19). *About COMELEC.* Commission On Elections. https://www.dbm.gov.ph/wp-content/uploads/OPCCB/OPIF2010/COMELEC/COMELEC.pdf

CyberCorps®: Scholarship for Service | Cybersecurity Center | CSUSB. (n.d.). https://www.csusb.edu/cybersecurity/student-resources/cybersecurity-student-opportunities/cybercorpsr-scholarship-service#:~:text=About%20the%20Program&text=Sponsored%20by%20the%20National%20Science,the%20length%20of%20the%20scholarship

Department of Education. (2017). K to 12 basic education curriculum for the alternative learning system (ALS-K to 12). 31. https://www.deped.gov.ph/wp-content/uploads/2019/01/LS-6-Digital-Literacy.pdf

Department of Education. (n.d.). K to 12 basic education curriculum junior high school technology and livelihood track and senior high school - technical-vocational livelihood track information and communications technology - computer systems servicing (NC II) (640 hours) https://www.deped.gov.ph/wp-content/uploads/2019/01/Computer-Systems-Servicing-NC-II-CG.pdf

Department of Information and Communications Technology. (2018, November 9). DICT not stopping with a bachelor's degree in cybersecurity. https://dict.gov.ph/dict-not-stopping-with-a-bachelors-degree-in-cybersecurity/

K to 12 Basic Education Curriculum | Department of Education. (n.d.). https://www.deped.gov.ph/k-to-12/about/k-to-12-basic-education-curriculum/

Lady Vicencio, ABS-CBN News. (2023, September 19). PH needs 180,000 cybersecurity professionals: group. *ABS-CBN News*. https://news.abs-cbn.com/business/09/19/23/ph-needs-180000-cybersecurity-professionals-group#:~:text=MANILA%20(UPDATE)%20%2D%20More%20cybersecurity,the%20Philippines%20(NADPOP)%20said.

National Defense College of the Philippines. (2023, March 28). *PHILIPPINE CYBERSECURITY IN RETROSPECT (2016-2021) - NDCP*. NDCP. https://www.ndcp.edu.ph/philippine-cybersecurity-in-retrospect-2016-2021/

National Cybersecurity Alliance. (2023, October 16). *Cybersecurity Awareness Month*. https://staysafeonline.org/programs/cybersecurity-awareness-month/#:~:text=Cybersecurity%20Awareness%20Month%20was%20launched,Homeland%20Security%20in%20October%202004

Navarro, T. (2022, March 23). School infrastructure in the Philippines: Where are we now and where should we be heading?. *Philippine Institute for Development Studies*. 36, 39. https://pidswebs.pids.gov.ph/CDN/PUBLICATIONS/pidsdps2210.pdf

NSA student and internship programs. (n.d.). U.S. Intelligence Community Careers. https://www.intelligencecareers.gov/nsa/students-and-internships

Palatino, M. (2023, February 22). The Philippines' basic education crisis. *The Diplomat*. https://thediplomat.com/2023/02/the-philippines-basic-education-crisis/#:~:text=%E2%80%9CThe%20lack%20of%20school%20infrastructure,104%2C536%20are%20in%20good%20condition.

Partnerships and Collaboration | Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/partnerships-and-collaboration#:~:text=Through%20these%20partnerships%2C%20we%20facilitate,is%20quick%2C%20seamless%20and%20actionable

PIDS study reveals serious school infrastructure gaps in PH basic educ sector. (n.d.). https://www.pids.gov.ph/details/news/press-releases/pids-study-reveals-serious-school-infrastructure-gaps-in-ph-basic-educ-sector

Senior High School in the Philippines: Curriculum breakdown – Courses in the Philippines: college, TESDA, online, short courses. (n.d.). https://www.courses.com.ph/senior-high-school-in-the-philippines-curriculum-breakdown/

SFS. (n.d.). https://sfs.opm.gov/About/History

The Philippines National Cybersecurity Plan shaping a secure cyber landscape. (2023, May 29). OpenGov Asia. https://opengovasia.com/the-philippines-national-cybersecurity-plan-shaping-a-secure-cyber-landscape/#:~:text=Cyberthreat%20actors%20took%20use%20of,secure%2C%20and%20reliable%20online%20environment

Umali, T. (2018, November 12). *Cybersecurity in the Philippine academe to bridge skills gap*. (2018, November 11). OpenGov Asia. https://opengovasia.com/cybersecurity-in-the-philippine-academe-to-bridge-skills-gap/

What we do. (n.d.). https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

White, B. G. (2020, May 3). Love Bug's creator tracked down to repair shop in Manila. *BBC News*. https://www.bbc.com/news/technology-52458765