Nyinkeu, N. D., Anye, D., Kwedeu, L., & Buttler, W. (2018). Cyber Education Outside the Cyberspace: The Case of the Catholic University Institute of Buea. *International Journal of Technology in Teaching and Learning, 14*(2), 90-101.

Cyber Education outside the Cyberspace: The case of the Catholic University Institute of Buea

Ngatchu Damen Nyinkeu
Catholic University Institute of Buea, Cameroon

Divine Anye
Capitol Technology University, USA

Leonnel Kwedeu
Catholic University Institute of Buea, Cameroon

William Buttler
Capitol Technology University, USA

In this era of technological abundance, it is difficult to imagine cyber education outside the cyberspace. The purpose of this paper is to extend the growing body of research on cyber education, by reporting the experiences of a Cybersecurity department cut-off from Internet access. The value of Cyber education is expressed even beyond the cyberspace. This qualitative exploratory study uses semi-structured interviews and content analysis to collect a wide variety of rich data in order to demonstrate the need and possibility of cyber education, even without Internet access. Willingness to learn and the hope of a fulfilled career were found to be the most significant factors for students' continual motivation. The presence of an eminent "force majeure" was seen more as an opportunity for novel explorations. In contrast to customary thinking, the constructs of information security and assurance were fully fledged outside the cyberspace.

Keywords: Cyber Education, Information Assurance, Cybersecurity, Sub Saharan Africa, Cyberspace

INTRODUCTION

The multi-faceted issue plaguing the North-West and South-West regions of Cameroon has seen the implementation of an unusual cyber policy in these regions. The Geo-

---

This article is based on continuous collaboration between the Catholic University Institute of Buea (CUIB) and Capitol Technology University (Capitol) in the development of a Bachelor's degree program in the former university. Ngatchu Damen Nyinkeu can be reached at ngatchu@cuib-cameroon.net.

https://doi.org/10.37120/ijttl.2018.14.2.04

Linguistic constellations of the regions has led to the adoption of the name "Anglophone – Crisis". The details of the crisis is anthropological, social, political, judicial and educational in nature. The background to the "Anglophone – Crisis" is rooted in the history of the nation. Originating from a British and French trusted territories, Cameroon as a nation strives to integrate the political, judicial and educational inheritance from the British and the French. With the French part of the country occupying about 80% of the national territory, English Cameroonian constantly feel marginalized and time and again they look for avenues to express their feelings. Information exchange remains the most critical factor guiding the strike and is predominantly carried out via whatsapp and Facebook. Through these social media tools, Cameroonians at home and abroad, especially those of the English regions, began to vent their frustrations about the current government. In a bid to manage the information risk, on Tuesday, 17th January 2017, the government ordered a shutdown of Internet access from both regions.

The consequences of this government action has led to a change in views and behaviors among inhabitants of the affected regions particularly towards Internet usage. For students, and particularly information technology students, they could see a change in attitude towards communicating with resource persons and lecturers, as well as the difficulties with researching even very basic concepts. Their knowledge of certain concepts in information assurance and Cybersecurity is operationalized and presented to them as a real-life experience. The influence of such occurrences and what students make of them are the primary concern of this research. This paper investigates cyber education in a two-year old department of Cybersecurity at a seven-year old Catholic University in Cameroon, which has been cut-off from the Cyberspace, due to the strike action.

The primary of objectives of this study are as follows:

1. Evaluate the influence of no Internet access on Information Technology students.
2. Evaluate methods to reinforce Cybersecurity concepts in students in a situation of no Internet access
3. Evaluate specific Cybersecurity concepts students gained in a situation of no Internet access

LITERATURE REVIEW

As the world continue to age in the information era, the need to maintain a growing scholarly literature in cyber education remain paramount, in-as-much as this literature captures the diversity and profundity of the complex pedagogic issues. As expressed in the introduction, the issue of cyber education outside the Cyberspace cuts across every aspect of educational science. Our literature review focuses on the Educational systems and pedagogic approaches, since these are most relevant in the context of this study.

EDUCATIONAL SYSTEMS

The overall objective of any educational system is to build and maintain a required level of consciousness in learners. Across academic disciplines in different educational systems, curricular are designed based on an expected level of awareness, set by a reference body. In cyber security, it is required that students have the right skill set and master appropriate toolkits (Wescott and Clark, 2017) as well as have a proper ethical disposition (Rawal, 2017). With the current technological climate in today's educational environment, Misawa (2017) investigates cyber-mobbullying as a malicious social issue. He affirms that "*the more technology is utilized, the more cyber-mobbullying seems to occur*." In this regard, awareness remains a fundamental aim of curricular and both students and faculty are expected to convey a certain level of security awareness with respect to the Cyberspace. Ekstrom et al., (2017) address a way in which the joint ACM/IEEE task force strives to

develop and articulating cybersecurity as a new meta-discipline, primarily for the American Educational System and for Centers of Academic Excellence (Wang et al., 2018). In Australia, the skills crisis in cyber security is a key policy issue and Henry, (2017) suggests a purpose-driven and mission-specific cyber security education as a focus of new initiatives in cyber security education. Nevertheless, Curricular are evaluated based on how well they meet the expectations of the stakeholders and thus the evaluation of any educational system.

With respect to main stream computing education and computational sciences, Information Assurance and Cybersecurity training is a relatively young discipline. Cyber education curricular are designed and proposed (Raj et al., 2011) as base training for today's students to improve their awareness of the computing, data, and privacy/security issues involved the technology age. Other researchers (Wang and North, 2008) view the infusion of information security into computing curriculum as an innovative way to restructuring computing curriculum. In well established computing contexts, such proposals are logical and they obviously create and add value to the educational agenda of information assurance and Cybersecurity. On the other hand, in contexts of low computational awareness, and where computing curricular are being established, an organic and integrative approach is more relevant. It creates and enforces an inherent link between the the learner's context, the content of the curriculum and the learning process.

Paramount to the learning process in cyber education is users' awareness. Besides educating students on the ethical, safety and security issues relating to the use of cyber space, students are expected to be able to educate others as well. Descriptive finding have been presented from an exploration (Pruitt-Mentle, 2011) of the nature of Cyberethics, Cybersafety and Cybersecurity (C3) educational awareness policies, initiatives, curriculum and practices in the U.S. public and private K-12 educational settings. Whether the findings are transferable and applicable in other parts of the world remains a subject for research. In Ukraine, for instance, (Voskoboinicov and Melnyk, 2018) continuous professional development is suggested as the national pedagogy mechanism for training of future cyber security specialists. Sobiesk et al., (2015) on the other hand, proposes a cyber education that collectively integrates foundational cyber knowledge, skills, and abilities through general education program, cyber-related electives, cyber threads, cyber minors, cyber-related majors, and cyber enrichment opportunities. The context of this project offers a unique experience for the exploration of Cybersecurity concepts viz-a-viz students' experience and proffers new insights to status quo and existing texts.

Centers of Academic Excellence (CEA) serve as reference for evaluation by mapping curriculum to government's standards (Livermore and Salter, 2011) and the role of faculty, organizational structure, scholarship, and commitment to developing a rigorous program cannot be undermined in this process. Establishing a Cybersecurity department is a strategic move which comes with obvious challenges (Goel et al., 2008) and demands careful planning. Experiences from contemporary, peers and similar projects are highly priced (Caelli and Smith, 2008) as they broaden the view of actors on curricular and implementation mechanisms as well as guidelines (Gorka et al., 2011) for evaluation.

In a nutshell, the relationship between curricular and the awareness of ethics, safety and security in the Cyberspace are partly constructed by the conscious efforts of the educational system. Strategies, policies and procedures, set by referencing bodies determine the majority of the content to which students are exposed. However, at the core of the strategies, policies and procedures of every educational system is the pedagogic approach. Although the pedagogic approach depends on the educational system, it dictates and determines how knowledge is generated and transmitted by shaping the student-teacher interaction.

PEDAGOGIC APPROACH

Various pedagogic approaches have been employed in cyber education, inducing online learning, competence based approach, scenario and game-based approach. These have been used in response to the desire to achieve expected learning outcomes; chiefly to deepen students' experience of the Cyberspace and thus improve program quality.

The need for students to understand the practical application of their knowledge, plays a vital and complementary role in their cyber education. Compared to traditional classroom learning, Online learning offers the possibility of reaching a broad audience, spread over wider locations. Ensuring high quality programs via online learning (Bier et al., 2011) required a keen eye on the learning process and a rigorous implementation of learning platform to ensure that learners acquire the right competences.

Success stories of implementing competency based approach in cyber education (Perez, 2011) reveal suitability of the approach in the discipline. However, its pedagogic success depends on the scenarios used for assessing students' competence. Project-based Learning (PBL) is an excellent execution of academic concepts in the real-world. Powell et al (2017) applied PBL in a cyber business law and they believe that it helps students to become better equipped in facing cyber business law challenges. However, they cautioned that, even though PBL produces consistent scores within a class, each class may have unique characteristics, strengths, and weaknesses that contribute to significant score differences when compared to another class. This indicates that course instructors need to pay attention to context while delivering content.

Scenario based training has proven to be more pedagogically apt (Poulios, 2011) for cyber education, since the instructor can tweak the environment to direct learning outcomes. Different infrastructural settings, such as traditional labs, competitions, virtual labs, and simulated web labs have been proposed to provide students with diverse scenarios and hands-on experience in security education (Fulton and Schweitzer, 2011). The choice of which setting to use depend on the complexity of the concept being taught, as well as the availability of the equipment.

Game-based learning (Ryoo et al., 2011) offers an interactive, scenario-driven educational framework which is more flexible for training. Jin et al (2018) presents a study in which four cybersecurity computer games were developed to educate high school students on social engineering, secure online behaviors as well as some first principles of cybersecurity such as attack types (DDoS, Phishing, Ransomware, Sniffer, Spyware, Trojan and Virus) and defense towers (Antivirus, Encryption, Firewall, Password, System Update and Secure Cyber Behavior). Their findings suggest that game based learning for cybersecurity education was very effective in cybersecurity awareness training. An evaluation of learning platforms and different learning styles for cyber-security courses (Biswas and Muthukkumarasamy, 2017) reveal that practice-based learning is the most effective learning method for cyber-security courses.

Matching scenario to infrastructural setting, to create a learning experience is a talent of the instructor. Students gain insights differently, based on the scenario-infrastructure configuration and this creates the learning experience for the particularly student. The experiences of students, who participated in cyber defense competitions, appears to increase their motivation and engagement in learning. They gain a perspective of the limits of their current knowledge, the benefits of a more extensive understanding of technical concepts, and the significance of integrating content from a number of areas (Hoag, and Tanko, 2011). Furthermore, capstone course are designed to be integrative, broadly focused, and demanding on the student (Livermore, 2008) to allow the student demonstrate their knowledge of project management techniques and a mastery of the skills taught across their program. All in an effort to provide experience.

Learning from experience creates lasting memories and allows students to claim ownership of the knowledge they build from these experiences. Although such experiences can be constructed in labs and simulation environments, their real-life occurrences produce vivid memories and allow for more insightful explorations. Experiences such as the one considered in this study are unique and spontaneous and cannot be formally integrated in curricular. However, they are a pedagogic jewel for examples, motivations and diction for cyber concepts. Below is a list of research questions guiding this study.

RESEARCH QUESTIONS

In tandem with other researchers, this study seeks an exploratory understanding of cyber education outside the Cyberspace from students' perspective. The "learner-centered" approach to higher education as well as the wide spread acceptance and use of Cyberspace in higher education motivated the following research questions:

1. What is the influence of no Internet access to technology students?
2. What Cybersecurity concepts are reinforced in students, during a situation of no Internet access?
3. How do students carry-on with Cyber education outside the Cyberspace?

METHOD

This paper reports the experiences of sophomore students of the department of Cybersecurity, who have been coalesced, with a significant fraction of a national territory to experience life without Internet access. In this section, we describe the participants, the research procedure as well as present and interpret the data.

PARTICIPANTS

The participants constituted sophomore students in the school of information technology, who were taking a course in Cyber Law. Six students (three girls and three boys) were purposefully selected to participate in a one-on-one interview, dues to their diversity in background experience relating to the Cyber space and gender balance. One of the girls already has a degree in political science and one of the boys holds a degree in mathematics, with a minor in Computer Science. The selection was based on the voluntariness of the students to share their experiences and their level of immersion in cyber education. Furthermore, Nineteen students of the sophomore class took part in a group discussion relating to the issue under investigation. In total, six girls participated in the study, despite the low intake of female students in science, technology, engineering and mathematics (STEM) disciplines. The choice of sophomore students was based on the desire to capture how students build understanding of Cybersecurity concepts earlier in the academic life.

PROCEDURES

Through an informal gathering of students from the school of information technology, contact numbers were collected and an initial invitation message was sent via short messaging service (SMS). The message required students to confirm their willingness and availability to participate in a one-on-one interview regarding their educational experiences without Internet access. Unstructured interviews were scheduled at the convenience of the participants and a class discussion was organized. Ethical clearance was obtained from the Research Ethics Committee of the institution where the research was carried out and an embedded analysis of the rich qualitative data was performed following guidelines from Yin (2003).

DATA AND FINDINGS

Data analysis and interpretation was done concurrently to maintain a close relation between the analytic discuss and the inferences drawn from these analysis. The findings have been tallied around the three research questions stated above, based on their appropriateness to the question and also to facilitate interpretation.

RQ1 *What is the influence of no Internet access on information technology students?*

On a general note, Information technology students develop mixed feelings when there is no access to the Internet. Some feel terrified, angry, frustrated, down-casted and discouraged. Others are able to identify the positive aspects of no Internet access and feel good about it. They related their frustration to the government's monopolization of Internet access in Cameroon and engaged in thinking about alternatives. Nevertheless, some students realized that the absence of Internet access enabled them to think independently and avoid "copy-paste", while doing assignments; to associate more with those physically around them; to be more focused and avoid distractions from Whatsapp, Facebook and other social media sites. Students have become more appreciative of other communication technologies like the short messaging service (SMS) and are more mindful of how much money and time they spend on Internet access.

One of the most disheartening recounts was the experience from a student, was the story of an attack by armed rubbers, who ambushed her sister while on a trip out of town to complete a financial transaction. Most participants traveled to neighboring towns and cities to gain access to the Cyberspace, even for rudimentary activities like sending an email or going a google search. Besides social consequences of such conditions, students raised more technical influences, which the circumstance had on them. It was intriguing to find students citing the shutdown of Internet access as a prelude for indulging in network hacking and cracking activities, in order to gain access to the Internet. They began digging on the web for methods to bridge mobile networks and bypass network securities. One student discovered the possibility of accessing specific antenna of a telecommunications network, with Internet access, from specific locations.

The influence of no Internet access for information technology students, had a social and a technical dimension. Students used the social challenge imposed the Internet access shutdown, to build critical thinking based on their technical competence. Although the shutdown lasted for a period three months, it permitted students to engage their thinking without the opportunity to implement some of their thoughts. Once connection was re-established, students returned to previous use patterns.

RQ2 *What Cybersecurity concepts are reinforced in students, during a situation of no Internet access?*

The findings reveal that three Cybersecurity concepts are reinforced in students due to the current "Anglophone – Crisis". Chiefly the need to be more responsible in using the Internet; a clear distinction between information security and network security as well as network isolation as a protective mechanism on the Cyberspace. The excerpt below is from a student who feels passionate about the spread of wrong information.

> *"I have learned that as IT people we should be using the Internet with some responsibility because over the holidays, I got very angry … because they were sharing, these are people who are educated and should be able to know what is misinformation. Each time I logged into the forum, those messages were circulating … I'm sure they were thinking that it was harmless … we should know the kind of messages we forward and the kind of things we talk about."*

His view was supported by another student who said

"Technology has aggravated the situation. In the sense that with the help of technology, people were spreading the information, mismanagement of information. … "

Some students where able to relate the information security risk with section and articles of Cameroon's Cyber law as well as recognize the efforts of the government in trying to educate the public about this law via SMS.

"… because they [the government] were sending threats to people on phones, that if you post this, you will have that … At least, they were not suppose to send it in a threatening manner, because that's actually part of the Cyber law, that if you use the social media to spread false propaganda, you risk five years imprisonment or five million [FCFA] … When I read the message I was annoyed … the message [came during a difficult political] climate "

Most of the students were able to distinguish between information security and network security, as well as a link between the two security concerns within the context of the "Anglophone – Crisis". One student said

"It was an information security problem; People were being mislead and the government did not know how to counter it, and they were taken aback [and they felt that cutting the Internet was a better solution … a more appropriate solution would have been to] really engage in those social media and immediately as those false information comes out, they [the government] also circulate their own information … so that people can be informed. … They should find ways to use the technology to their advantage, rather than fight it."

Another student expressed that they government, but shutting down Internet access was trying to reduce the about of false rumor that was being propagated. Others were able to relate the spread of the rumor to the existence of high Internet connectivity in Cameroon. Such clear distinctions in the experiences of the students creates a common language for further probing and exploration of these concepts.

The reflection from one student, presented in italics below, depicts the notion of network isolation as a protective mechanism.

"*From the way I feel about this whole thing … its positive and negative. Positive in the sense that, … a hacker would not be able to hack into someones network since there is no Internet. [Also, with respect to Internet blackmailing, one can] take a picture, … But will not be able to send it through the Internet because there is no connection, like to blaspheme. … for the flow of information, if there was Internet connection, people will be forwarding messages that are not true … [since there is no connection,] there will not be any forwarding of useless messages, messages to threaten others…* "

Although the view does not consider the mobility of peoples, and the consequences of this mobility, it portrays a picture of network isolation and how it can preserve the confidentiality and integrity of data which resides in the articulated section of the network.

In a nutshell, by engaging students in this research, they constructed a link between their socio-political circumstance and technical knowledge of their discipline. Three Cybersecurity concepts: (1) responsible use of the Internet; (2) distinction between information security and network security; and (3) network isolation as a protective mechanism on the Cyberspace; are clearly reinforced in students and they can always relate these concepts to the experience of no Internet Access.

RQ3 *How do students carry-on with Cyber education outside the Cyberspace?*

Students carried on with their education through the use of textbooks and video tutorials, which had been previously downloaded. One students feels the limitation of what can be known about Cybersecurity and says:

" reading from books, watching videos, although some of the book and videos are some how limited … the main limitations are … certain things that the books don't actually explain well, so you have to go to online forums to find out if someone has solved or done a similar problem before or if some one has a similar problem so that you could join heads together and solve but now … the inability to access forums and online chats has been a major handicap."

Another student said

"pre-downlaoded material could have helped but not for so long, because you'd eventually exhaust the material."

On the contrary, one student indicated that he changed his focus to non-academic activities and got involved in constructions work, while another said got engage in driving lessons. Traveling to Douala – the economic capital of Cameroon, which is about an hour drive, was the default means of Internet access for most students. Acknowledging the importance of Internet access to their education, most students recounted the interesting episodes of their trips to Douala for the sake of an assignment that required them to read beyond pre-downloaded materials. A true call for concern would be copy-right violation, with the spread of pre-downloaded material and other researcher could focus on this with respect to open and organically grown content.

Despite the challenge of no Internet access, students remain hopeful and value their pursuit of a degree in cyber security even more. Some extracts from the data include:

"[the current situation] encourages [one] even more because when you see a problem [like the current crisis], it pushes to think otherwise, … to try and bring your own solution"

"It makes me value my studies more … for security purpose, to secure myself and my network, the people I see that need security ,".

Others reclined to watching TV and listening to Radio, as sources of information and knowledge. Educational institutions could leverage from such media even as a complement to Internet content. The creation of a "richer" internal network would be a valuable solution to address some of the needs raised by the students.

Summary of findings

1. The shutdown of Internet access encourages students to think independently and critically and to be more focused.
2. The termination of Internet access is a prelude for indulging in network hacking and cracking activities, by cyber security students.
3. Without Internet access, students become more appreciative of alternative communication technologies and pre-downloaded educational content.
4. Three cyber security concepts are re-enforced by the shutdown of Internet access: (1) The need to be more responsible on the cyberspace; (2) A clear distinction between network security and information security; (3) Network isolation can be a protective mechanism in the cyberspace.

LIMITATIONS, IMPLICATIONS, CONCLUSION AND RECOMMENDATIONS

LIMITATIONS

The study is limited by its context and methodological approach and as such generalizations would be per-mature. The study was carried out in Cameroon – Africa,

during the sole period when the government decided to shutdown Internet access in two out of ten regions in the country. It focuses on the first two cohorts of students from a private university, in a Bachelor's Degree program in Cyber Security. However, it offers a unique experience from with other researchers and educators could draw inspiration. The impending limitation of small sample and uniqueness, informs the methodological stand for the study.

IMPLICATIONS FOR QUALITATIVE RESEARCH

Qualitative research is rear in technology studies (Lee et al., 2003; William et al., 2015) and research relating to use of technologies. Proponents of determinism argue that it lacks generalizability and reliability and thus could hardly be replicated, reproduced and or verified. Nevertheless, advocates of qualitative research hold that "i*nterpretive positions provide a pervasive lens or perspective on all aspects of a qualitative research project. The participants in these interpretive projects represent underrepresented or marginalized groups, whether those differences take the form of gender, race, ...*" (Creswell 2007:p24). Such inspirational thoughts inspire us to see beyond a generalization agenda of cyber education and spur us to ask deeper questions such as:

(1) How can we improve users' awareness of responsibility within and outside the Cyberspace?

(2) What practical analogies and or experiences could be used to explain Cybersecurity concepts so that students build lasting understanding of these concepts?

(3) How are (can) Cybersecurity concepts (be) implemented in other spheres of information flow.

These questions shift the pedagogic discuss towards creating experiences for students and leveraging from current or lived scenarios to reinforce taught concepts. The above questions are possible directions for future research; Yet they tell of the unique opportunity, which qualitative research brings to the technology studies.

THEORETICAL IMPLICATIONS

The findings evince practical and contextual application of the concepts of information security and assurance, which could be used by instructors to offer an insightful picture of these concepts. They suggest out-of-classroom approaches and offline activities which could be integrated into Cyber education courses, and even beyond, to engage students at a different level. The study not based on any particular theoretical odel, but can be used to induce one.

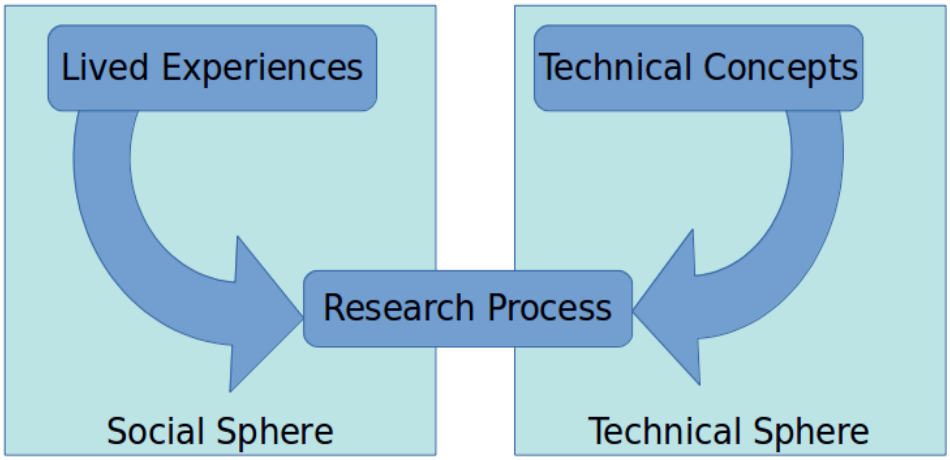

Figure 1 – Research Framework

Charmaz (2006:p126) proposes that an "*Interpretive theory calls for the imaginative understanding of the studied phenomenon. This type of theory assumes emergent, multiple realities; indeterminacy; facts and values as linked; truth as provisional; and social life as processual*". Figure 1 shows and inductive theoretical framework that emerged from this study. The framework is built based on extensive engagement with students, the Cybersecurity body of knowledge relating and the scientific research methodology.

The Cybersecurity body of knowledge envelops a wide range of concepts. Whether it is possible to map each of these concepts to lived experiences is a question to ponder. The study realized that students were successful in mapping the "no Internet access" experience to relevant technical concepts through their participation in the research, particularly during the interview process. The interviewer created a friendly conversational environment and encouraged the students to ask questions and facilitated the establishment of links between concepts and experiences.

The influence of the research methodology was very significant and limited the framework to generic categories of "Lived experiences" and "Technical concepts". Structured and formal interviews and or multiple focus group discussions are credible alternative to expound on these categories. Furthermore, the collected data and analytical machinery are not rigorous enough to ground a theory; yet this is a fruitful start. In conclusion, One can say that the research process is the conner stone for cyber education out side the cyber space. Whether as a participant (interviewee) or as a researcher (interviewer), student construct new knowledge and reinforce taught concepts through research.

RECOMMENDATIONS

The cyberspace has come to stay and threatens to be an indispensable part of human activity in our world tomorrow. Consequently, cyber education needs to be viewed from a more comprehensive and broader perspective and we recommend the following directions for further studies

1. Focus on ethical education as an integral part of cyber education. The tools and skill set for white and black hat hackers are the same. What makes the difference is their conscience.
2. A comprehensive view on the field of cyber security, inspired by an organic development of cyber education. Partnerships between government, educational institutions and organizations is critical for this to happen.
3. Use "live-audience" pedagogic approaches, in a manner similar to education by apprenticeship.

REFERENCES

Bier, N., Lovett, M., & Seacord, R. (2011). An online learning approach to information systems security education. In *Proceedings of the 15th Colloquium for Information Systems Security Education.*

Biswas, K., & Muthukkumarasamy, V. (2017). Quantitative research design to evaluate learning platforms and learning methods for cyber-security courses. In *28th Annual Conference of the Australasian Association for Engineering Education (AAEE 2017)* (p. 793). Australasian Association for Engineering Education.

Caelli, B., McNair, N., & Smith, L. (2008). Information assurance education in a specialist defence environment. *Proceedings of the 12th Colloquium for Information Systems Security Education*. University of Texas, Dallas, TX June 2 - 4, 2008

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage. ISBN-10 0-7619-7352-4

Creswell, J. W. (2007). Qualitative inquiry and research design: Choosing among five approaches (ed.). *US: Sage*. ISBN 978-1-4129-1606-6

Creswell, J. W. (2011). Controversies in mixed methods research. *The Sage handbook of qualitative research*, *4*, 269-284.

Dittrich, D. (2008, June). On Developing Tomorrow's" Cyber Warriors. In *Proceedings of the 12th Colloquium for Information Systems Security Education* (pp. 2-4).

Ekstrom, J. J., Lunt, B. M., Parrish, A., Raj, R. K., & Sobiesk, E. (2017, September). Information Technology as a Cyber Science. In *Proceedings of the 18th Annual Conference on Information Technology Education* (pp. 33-37). ACM.

Fulton, S., & Schwietzer, D. (2011). A concept focused security lab environment. In *Proceedings of the 15th Colloquium for Information Systems Security Education* (pp. 126-131).

Goel, R., Mobolurin, A. & Rustagi, N. (2008) Challenges Of Establishing Centers Of Excellence In Information Assurance At An HBCU: A Case Study. *Proceedings of the 12th Colloquium for Information Systems Security Education*. University of Texas, Dallas, TX June 2 - 4, 2008

Gorka, S., Miller, J. & Yoas, D. (2011) A Tool for IAS Curriculum Development, Management, and Accreditation. *Proceedings of the 15th Colloquium for Information Systems Security Education*. Fairborn, Ohio June 13-15, 2011.

Henry, A. P. (2017). Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements. ACCS Discussion paper NO. 4, August 2017

Hoag, J., & Tanko, Z. (2011). The Impact of Cyber Defense Competitions on Student Motivation, Engagement, and Curriculum at Champlain College. In *Proceedings of the 15th Colloquium for Information Systems Security Education (CISSE), Dearborn, Ohio*.

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning*, *12*(1), 150-158.

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for information systems*, *12*(1), 50.

Lincke, S. J. (2011). Service-learning in Security. In *Proceedings of the 15th Colloquium for Information Systems Security Education* (pp. 63-68).

Livermore, J., & Poulios, N. (2008). Integrating a capstone course into an information assurance program. In *Proceedings of the Twelfth Colloquium for Information Systems Security Education. Dallas, TX*.

Livermore, J & Salter, A. (2011) What is the Student Recruitment Value of the CAE Designation? *Proceedings of the 15 th Colloquium for Information Systems Security Education*. Fairborn, Ohio June 13-15, 2011

Misawa, M. (2017). Investigating Technology Usage and Perceptions on Cyber-Mobbullying in Higher Education in the United States among College-Age Youth: A Correlational Study at a Research Institution. *Annali online della Didattica e della Formazione Docente*, *9*(13), 279-299.

Perez, T. J. (2011). Information Security Education: A Competency Based Approach and Exemplification. In *Proceedings of the 15th Colloquium for Information Systems Security Education Fairborn, Ohio June 13-15, 2011*.

Poulios, N. S. (2011) Scenario Based Exercises in IA Courses. *Proceedings of the 15th Colloquium for Information Systems Security Education*. Fairborn, Ohio June 13-15, 2011

Powell, J., Parker, C., & Kilcoyne, M. (2017). Cyber Business Law and Project-Based Learning. *International Journal for Innovation Education and Research*, *5*(11), 62-73.

Pruitt-Mentle, D. (2011) National C3 Baseline Study: State of Cyber Ethics, Safety and Security Awareness in US Schools. *Proceedings of the 15th Colloquium for Information Systems Security Education.* Fairborn, Ohio June 13-15, 2011.

Raj, R. K., Mishra, S., Howles, T., & Romanowski, C. (2011). Cybersecurity as General Education. In *Proceedings of 15th Colloquium for Information Systems Security Education (CISSE'11)*.

Rawal, B. G. D. R. (2017). Exploration of Cognitive Skills in Kids through Cyber Crime Ethics Education: A Prevention Method. National Conference on Latest Trends in Networking and Cyber Security, International Journal for Innovative Research in Science & Technology, March 2017, 121-124.

Republic of Cameroon (2010a). Law No 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon, Republic of Cameroon, Yaounde.

Ryoo, J., Techatassanasoontorn, A., Lee, D., & Lothian, J. (2011, June). Game-based infoSec education using OpenSim. In *Proceedings of the 15th Colloquium for Information systems security Education* (pp. 101-106).

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015, September). Cyber education: a multi-level, multi-discipline approach. In *Proceedings of the 16th Annual Conference on Information Technology Education* (pp. 43-47). ACM.

Voskoboinicov, S., & Melnyk, S. (2018). Cyber security in the modern sociation and improvement of preparation of future factors in the field of competent approach. *Social work and education*, *5*(1), 103-112.

Wang, J. A. (2008, June). Designing a Security Thread in Computing Curricula. In *Proceedings of the 12th Colloquium for Information Systems Security Education* (pp. 2-4).

Wang, P., Dawson, M., & Williams, K. L. (2018). Improving Cyber Defense Education through National Standard Alignment: Case Studies. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, *2*(1), 12-28.

Wescott, J., & Clark, U. (2017). Cyber Defense Education & A Linux Toolkit. In *Proceedings of the EDSIG Conference ISSN* (Vol. 2473, p. 3857).

Williams, M. D., Rana, N. P., & Dwivedi, Y. K. (2015). The unified theory of acceptance and use of technology (UTAUT): a literature review. *Journal of Enterprise Information Management*, *28*(3), 443-488.

Yin, R. K. (2003). Case study research design and methods third edition. *Applied social research methods series*, *5*.