Journal of Information Systems and Informatics
Vol. 6, No. 1, March 2024 e-ISSN: **2656-4882** p-ISSN: **2656-5935**
DOI: 10.51519/journalisi.v6i1.676 Published By DRPM-UBD

The Cyber Kill Chain Model and Its Applicability on The Protection of Students Academic Information Systems (SAIS) in Tanzanian HEIs

George Matto

ICT Department, Moshi Co-operative University, Tanzania
Email: george.matto@mocu.ac.tz

Abstract

Security threats are constantly evolving in various computerized systems. As in many other systems, security threats and attacks have been directed to Students Academic Information System (SAIS) in Higher Education Institutions (HEIs). The seven steps cyber kill chain model offers preventive defense against such security threats. Little is known, however, on how well the model is applicable in the protection of SAIS. This study was therefore carried out to investigate the applicability of the cyber kill chain model on the protection of SAIS. The study was qualitative in which empirical evidence from literature was employed to gather data which were then analysed thematically through content analysis. Results showed that the cyber kill chain model is very relevant and applicable in the protection of SAIS. Each of the seven steps of the model practically applies differently in SAIS which entails for distinct protective measures as detailed in the paper. The study calls upon HEIs stakeholders to leverage the proposed preventive measures against security threats in SAIS.

Keywords: Cyber kill chain, Students Academic Information System, HEIs, Tanzania.

1. INTRODUCTION

Information and Communication Technologies (ICTs) have been playing an important role as a strong agent for change in the education sector through optimizing and streamlining classroom, campus and institutional operations [1]. In Tanzania, like in many other countries, almost all institutions (especially those of higher education) have adopted the use of ICTs to facilitate operations. A study by [2], for example, reported that Tanzania introduced the use of ICT-based systems to admit students to Higher Education Institutions (HEIs). In addition to admitting students, ICT systems are used by HEIs to register admitted students and consequently store and provide access to student-related information such as demographics, courses and instructors details, class schedule, students class attendance, grading, as well as billing and payments [1]. Likewise, [3] indicated that these systems provide capabilities for students to register courses, document examination results and other assessment scores, generate transcripts, build schedules and track students' academic progress.

The ICT-based systems for managing students' information have been given different names across institutions. According to [3] globally these systems have been named as Students' Information Systems (SIS), Students' Management Information Systems (SMIS), Students' Data Systems (SDS), Students' Data Warehouse (SDW) and Students' Information Management Systems (SIMS). In Tanzania, individual HEIs decide on the names of such systems. For example, the University of Dar es Salaam (UDSM) names the system for managing students' information as Academic Record Information System (ARIS) [4], the University of Dodoma (UDOM) names it as Students Records Management System (SRMS) [5], and the Open University of Tanzania (OUT) names it as Academic Register Management Information System (ARMIS) [6]. Other HEIs decided to name such systems to coin with the names of their institutions. For instance, the Moshi Co-operative University (MoCU) names such a system as MoCU Students Academic Registration Information System (MUSARIS) [7] and the Sokoine University of Agriculture (SUA) names it as SUA Students Information System (SUASIS) [8]. In the context of this study, these systems are regarded collectively as Students Academic Information System (SAIS). The core function of SAIS, as described by [9], is to keep all students' details in a systematic manner for easy archival and retrieval. SAIS are, therefore, very crucial systems in supporting both academic and administrative operations of HEIs.

In today's world, threats in various computerized systems are constantly evolving. As posed to other systems, security treats are posed also to SAIS. Research by [3] indicated that the problem of many HEIs with regard to the use of SAIS is on how to use them smoothly and safely so that they continue keeping their vital data and information, and protecting them from increasing malicious threats and attacks. Unfortunately, as the threats increase, it becomes difficult to address every occurrence and alert in SAIS. Thus, robust incident response is required to confront the security threats posed to SAIS.

It is suggested by [10] that the best approach to deal with security threats is to catch threat actors within their environments before they cause harm and become even greater threats. This require institutions to focus on being proactive rather than reactive. Studies (see for example [11] and [12]) have indicated that the cyber kill chain model offers preventive defense against security threats to networks and systems. Although the model has been used in various application areas, little is known on how well it can be suitable for the protection of SAIS. It was on these grounds that this study was carried out to investigate the applicability of the cyber kill chain model on the protection of SAIS.

The reminder of this paper is organized as follows. Section 2 explains more about the cyber kill chain model and its processes. Section 3 describes the methodological underpinnings of the study. Section 4 presents results and discussions, and section 5 concludes the study and puts forward recommendations.

2. METHODS

2.1 The Cyber Kill Chain Model

The cyber kill chain model is based on the 'kill chain' concept used by the military [13]. [14] describes the kill chain as the shorthand term for the "find, fix, track, target, engage, and assess" (F2T2EA) process necessary to achieve desired battlefield effects. [15] added that it is actually a systematic process to target and engage an enemy before the enemy creates desired effects. The authors expounded the kill chain process as *find* enemy targets suitable for engagement; *fix* their location; *track* and observe; *target* with suitable weapon to create appropriate effects; *engage* the enemy; and *assess* effects.

The military's kill chain concept was employed by Lockheed Martin in 2011 to come up with the 'cyber kill chain' model [13] and [16]. As explained by [17], the cyber kill chain model is a cybersecurity framework used to describe and track steps of a cyberattack. The model consists of a chain of seven steps that are required to be achieved for an attacker to successfully carry out the cyber attack. [18] descried that each step in the chain presents a specific goal along the attacker's path posing a risk that must be mitigated before it can happen. The seven steps of the cyber kill chain model, as presented by [17], are reconnaissance, weaponization, delivery, exploitation, installation, command and control and actions on objectives as summarized in Figure 1 as follows:

1) Step 1: Reconnaissance – in this step attacker gathers information about the target before the real attack starts. Information gathering could be achieved through looking for openly accessible information via the internet or on other sources.
2) Step 2: Weaponization – attacker uses information gathered during reconnaissance step to prepare a malicious payload that will be sent to the victim. This step happens at the attacker's side, without any contact with the victim.
3) Step 3: Delivery – in this step attacker delivers the prepared malicious payload to the victim using email or other means.
4) Step 4: Exploitation – involves the actual execution of the exploit.
5) Step 5: Installation – in this step prepared attacking tools are installed on the infected environment.
6) Step 6: Command and control – during this step attacker create a command-and-control channel in order to continue to operate his delivered attacking tools from a distance.
7) Step 7: Actions on objectives – in this step attacker collects and disengage information or other actions considered necessary to undertake actions against the target.

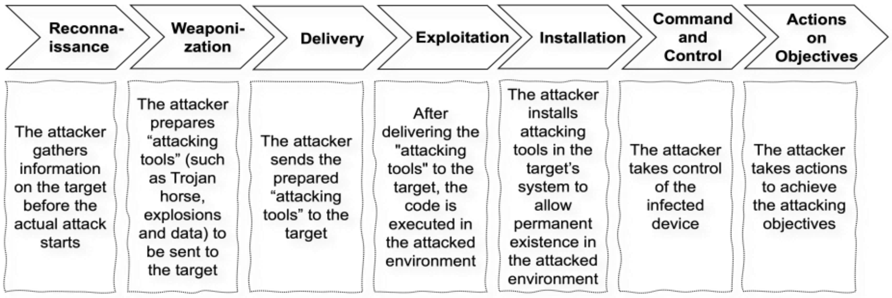
Reconna-issance
Weaponi-zation
Delivery
Exploitation
Installation
Command and Control
Actions on Objectives
The attacker gathers information on the target before the actual attack starts
The attacker prepares "attacking tools" (such as Trojan horse, explosions and data) to be sent to the target
The attacker sends the prepared "attacking tools" to the target
After delivering the "attacking tools" to the target, the code is executed in the attacked environment
The attacker installs attacking tools in the target's system to allow permanent existence in the attacked environment
The attacker takes control of the infected device
The attacker takes actions to achieve the attacking objectives

Figure 1. Steps of the cyber kill chain Model (Constructed from [18], [19] and [17])

The cyber kill chain is not a security system but rather a framework that enables security teams to anticipate how attackers will act so they can stop them as quickly as possible or intercept them if the attack has already transpired [13]. In other words, the model enhances visibility into an attack and enhances apprehension of the attacker's tactics, techniques and procedures. The cyber kill chain has, thus, become a model for actionable intelligence when organizations align defensive capabilities against attackers [15].

Like many other models, the cyber kill chain has received criticisms (see for example [20] and [21]. One of its major critiques posed by scholars is that attacks in the first two phases of the model (i.e. reconnaissance and weaponization) appear to occur outside the target network which makes it difficult for organizations to understand or defend against internal actions occurring during these phases. In other words, critiques contends that the model sounds not well suitable for insider threats. Consequently, similar models such as Unified Kill Chain [21] and the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework [22] were introduced. These models extended the concept of the cyber kill chain by, among others, adding more steps (18 for the Unified Kill Chain and 10 for the MITRE ATT&CK) to try addressing the weak points of the cyber kill chain. In addition, the ATT&CK model goes beyond describing the steps of an attack, and instead models specific attacker actions and motivations [22].

Despite the presented criticisms, [11] affirm that organizations can still use the cyber kill chain model in defining their cybersecurity strategy as part of preparing for the existing and future cyberattacks. In addition, through its seven steps, the model offers organizations a layered approach of administrative, technical and security measures. On the other hand, [12] posits that the cyber kill chain model should not be thrown out, it can be very useful when doing threat modeling. Questions like "how will the attacker find information about organization systems? how will they compromise information they got? and, how will they get the data out of the system? can be well addressed with help of the cyber kill chain model. It was on these grounds that the study was based on the cyber kill chain model.

2.2 Research Procedure

This study was essentially qualitative in which empirical evidence from literature was employed to gather data that was used to establish the applicability of the cyber kill chain model in the protection of SAIS. Four steps were involved to accomplish the study. The first step was broad literature search. In this step the study searched various literature related to the focus of this study. In particular, various electronic databases of peer-reviewed scholarly articles and informational websites regarding SAIS attacks and the cyber kill chain model were searched. The explored literature include; books, journal articles, conference proceedings, theses and informational websites.

The second step involved in the study was selection of particular thematic literature in which relevance of literature, currency, credibility, clarity, and accessibility were considered during selection of specific thematic literature. The third step was analysis of selected thematic literature in which selected thematic literature was analyzed using the content analysis approach and then classified into themes as per the seven steps of the cyber kill chain model. And the fourth and last step was organization of the paper in which analysis results were then organized to meet the study objectives as presented in the results and discussion section.

3. RESULTS AND DISCUSSION

3.1 Cyber-attacks incidents on SAIS in Tanzania

As cyber-attacks happen in HEIs elsewhere in the world (see for example [23], [24], [25] and [26]), they have also been reported to happen in Tanzanian HEIs. The primary target being altering results, generating transcripts, changing fees payment status and disrupting HEIs services. For instance, recently the University of Iringa (UoI) expelled more than 50 students studying Information Technology at the campus after they hacked the University's Student Management Information System (SAMIS) and committed payment fraud in the system [27]. Like other SAIS, SAMIS manages university academic data such as exam results, course registration, billing and fees management and timetabling [28]. [29] added that in connection to altering results and changing fees payment status, HEIs are also being targeted by attackers with the aim of the ransomware objectives as well as disruption of learning processes. A study by [30] revealed also existence of hacking incidences to many Information systems in the education sector in Tanzania. According to the author the incidences include hacking of the Open University of Tanzania website which hosts SARIS, hacking of the students' system at the University of Dar es Salaam, as well as hacking of the web-based information system of the Tanzania Commission for Universities (TCU).

In addition, [31] reported that there has been evidence of occurrence of incidents of cyber threats at University of Arusha and Tumaini University Makumira in which numerous students have been accused for breaching the security of university computer system in order to alter their grades. Presence of such cyber-attacks in HEIs' SAIS entails that SAIS are continuously targeted by attackers. This is supported by [32] who argued that students, administrators and faculty use SAIS to support a number of HEIs related activities and functions which makes the systems attractive target for attackers. Robust security measures are, thus, required to protect the systems.

3.2 The Cyber Kill Chain and SAIS protection

3.2.1 Reconnaissance

Reconnaissance is the first step in the cyber kill chain model. This step is applicable in SAIS in the sense that before delivering the actual attacks into SAIS, the attacker attempts to discover SAIS related information that can be exploited. That information is such as IP addresses of the SAIS server, the SAIS URL, information about the server's operating system as well as other information like address of the HEIs' mail or web server deemed necessary to the attacker. The attacker may also try to identify open ports on a network hosting SAIS. These can be achieved through actions like foot printing, port scans, DNS requests, and social engineering attempts to trick SAIS users (students, instructors and admins) to reveal sensitive information or download malicious software [33]. Reconnaissance can also be done through shoulder surfing and other physical attempts [34], [15].

In order to protect SAIS against reconnaissance, [35] suggests that HEIs must install firewalls to detect ongoing port scans and shut them down early enough. Moreover, according to [36] and [35], regular checking of HEIs' network systems through penetration testing and intrusion detection to determine existing weak points that could be exploited is another way to protect SAIS reconnaissance. In addition, [34] suggest the use of strong and unique passwords that are regularly changed and undertaking regular trainings to SAIS users (especially students and instructors) on how to be aware of the signs and tactics used by attackers.

3.2.2 Weaponization

Once reconnaissance is successful, the attacker undertakes weaponization. According to [19], reconnaissance activities play a significant role in the attacker's choice of attacking tool. During weaponization, attacking tools such as Trojan horse, exploitation and fake data are prepared and placed in infected files (PDFs, Microsoft Office files or web pages) that will then be sent to SAIS users or any user connected to a network hosting SAIS. Although, as said by [20] and [21], this step is difficult to protect as it happens to the attacker's side but effective protective mechanisms in the reconnaissance and delivery steps guarantee ineffective weaponization.

3.2.3 Delivery

Upon successful preparation of the attacking tools during weaponization, in the delivery step attackers attempt to deliver the prepared tools to SAIS users. Several approaches are used to deliver the tools. One of the common is through the use of email attachment in which attackers send fake email messages to SAIS users demanding them to open attached files such as PDFs, Microsoft Office files which are embedded with malicious software. In the case of HEIs students, for example, attackers may send emails with fake job advertisement, embedded with malware, demanding students to download attached job advert [11]. In 2017 for example, the Federal Bureau of Investigations (FBI) issued a public service announcement to University students in the US warning them against employment scam [37]. In line with email attachments, attackers have also been implanting malware in webpages in which links to those pages are sent to HEIs students and staff through emails or social media messages, demanding them to click on the links [38].

External storage media such as weaponized USB drives containing malware have also been used by attackers. The common approach by many attackers to deliver their tools to users is through dropping malicious USB drives within campus or in students' house of residence. Once a student picks the USB and try to open it to see what is inside, he gets the stored malicious software. In addition, attackers deliver malware to HEIs students through distributing free USB drives with hidden malware, or through USB phone chargers to smartphone users [39].

With all the existing means to deliver attacking tools, [40] pointed out that email has consistently been the number one entry point for threats, with 90% of breaches beginning with an email attack. Thus, to protect against delivery of attacking tools, HEIs must put in place strong protection mechanisms especially against email attacks. One way to achieve this is to use strong and effective email and web filtering tools with strong password policy [9]. In addition, [13] suggests the use of strong Antivirus tools. [32] recommend that for HEIs to be safe from attacks, system users need to undertake physical attempts such as verification of the identity and authenticity of any message or call that asks for personal or sensitive information, and not clicking on links or open attachments that are unexpected or suspicious. There must also be limited use of USB devices and blocking autoruns [9].

3.2.4 Exploitation

Exploitation follows after attackers have managed to deliver the "attacking tools" to SAIS user. During exploitation, the codes attached in the delivered malicious software are executed in the SAIS network [19]. Attackers may infiltrate further the SAIS network and learn of additional vulnerabilities that they were unaware of prior to entering. As explained by [13], the exploit will only work on outdated systems and most probably will not be picked up by traditional security tools, like antivirus or firewalls. Thus, to protect SAIS against exploitation step it is advised that HEIs use latest web application firewalls and use vulnerability scanning.

3.2.5 Installation

Upon a successful exploitation, attackers strive to gain control of the SAIS and thereafter navigates the network without any obstruction [19] and [10]. This is achieved through the installation step in which malware and other prepared attacking tools are installed. Through those tools, attackers gain access to various SAIS sensitive information. During this step, attackers may install additional attacking tools within the SAIS network so as to gain more control of the systems. They may also put in place open SAIS security credentials and alter system authorizations. In addition, they may create back doors into the SAIS or its hosting network so that they can continue accessing SAIS even if the original opening wedge is identified and closed.

3.2.6 Command and Control

During the command-and-control phase, attackers liaise with the attacking tools they have installed in the previous step and instruct them to undertake whatever they want. For example, attackers may shut down the SAIS server, seize resources or encumber the server with traffic. If this is achieved, SAIS users may experience system being down for several hours or even days and thus not be able to access SAIS. Attackers may use this attack with various motives, one of which (as reported by [41]) being demanding ransom to HEIs for them to bring back the service. Attackers in this step can be prevented through the use of strong firewalls, intrusion protection systems and proxy filters [19].

3.2.7 Actions on Objectives

In the final step of the cyber kill chain, attackers carry out their original objectives of attacking SAIS. In line with DoS as explained in the sixth step, attackers could have several other objectives of attacking. Most common ones are, as [9], [32] and [30] indicated, change of examination results, generate transcripts, and change of fee payment and other transactions details. They may also encrypt data so that whoever manages to access SAIS database will access only encrypted data, or steal the data for their own intents.

Attacks and their devastating effects at this step of the cyber kill chain model can be protected through a number of measures. Some of such measures are endpoint malware protection, periodic logs analysis, secure backups as well as putting in place plans for disaster recovery [36] and [18].

3.3 Discussions

The study has shown that SAIS are constantly targeted by attackers whose attacking intentions differ. There are those that attack SAIS for the aim of altering results, generating transcripts or changing fees payment status. Most of attackers in this category are ongoing HEIs students, HEIs graduands or hired professional attackers. In most cases, these attackers have some basic information with regard to respective SAIS. Another category of attackers consists of those that come from outside HEIs whose aims are disrupting HEIs services and learning processes or ransomware. Thus, HEIs ought to take proactive measures against potential attacking incidents to SAIS.

The results of this study have shown that the seven steps cyber kill chain model presents a framework that can enable HEIs to anticipate how attackers will act so they can stop them as quickly as possible. The first three steps of the cyber kill chain model (i.e. reconnaissance, weaponization and delivery) help HEIs to confront the attacker's malicious intent even before it happens. As revealed in the study, these can be achieved through a number of preventive measures some of which are use of strong firewalls, undertaking regular penetration testing and intrusion detection, enforcing the use of strong and unique passwords, as well as limiting the use of USB devices within the SAIS network. This will limit two possibilities of attackers. First, it will block easy discovery of sensitive SAIS information that can be exploited by attackers. And second, in case attackers have prepared attacking tools, it will prevent delivery of such tools to SAIS users.

In the event that attacking tools have been delivered to SAIS network (especially by those attackers who already have some SAIS information necessary for preparing attacking tools), the study has shown that the cyber kill chain model enlightens possible intercepts to limit the outcomes. The four last steps of the model (i.e. exploitation, installation, command and control, and action on objectives) suggest possible ways of limiting the effects. Measures such as use of proxy filters, web application firewalls and vulnerability scanning have been detailed by the study. In addition, it is important for HEIs to undertake endpoint malware protection, periodic logs analysis, secure backups as well as putting in place plans for disaster recovery.

4. CONCLUSION AND RECOMMENDATIONS

The study aimed at exploring the applicability of the cyber kill chain model on the protection of Students Academic Information System (SAIS). Undertaking of this study was motivated by a number of threats and attacks that have been directed to SAIS to cause devastating results. As it has been suggested by scholars, the best approach to respond to such situations is to catch threat actors within their environments before they become serious. The cyber kill chain model stands to offer guidance in which the needed preventive defense against security threats can be achieved. The study found out that each of the seven steps of the cyber kill chain model are applicable in SAIS. In line with provisions in the model, SAIS attackers will try to acquire information about SAIS through social engineering attempts (including and shoulder surfing) and other means. They will then prepare fake data and place them in infected files which are then delivered to SAIS through, among other means, fake email messages to SAIS users. Once users open the message the malicious software gets installed in SAIS server, in which the attackers will instruct them to undertake their malicious acts such as change of examination results, generate transcripts, and change of fee payment and other transactions details. Preventive measures, as provided in the cyber kill chain, are therefore necessary to be undertaken to protect SAIS from threats and attacks. The study recommends that HEIs stakeholders should consider leveraging the proposed preventive measures against security threats in SAIS.

ACKNOWLEDGEMENT

The author is grateful to his employer, Moshi Co-operative University, for giving him opportunity to undertake this study. The author is also grateful to the editors and reviewers whose constructive comments shaped this work.

REFERENCES

[1] G. Matto, “Big Data Analytics Framework for Effective Higher Education Institutions,” *Tanzan. J. Eng. Technol.*, vol. 41, no. 1, pp. 10–18, Jul. 2022, doi: 10.52339/tjet.vi.768.

[2] O. Tefurukwa, “The Central Admission System in Tanzania: The Best E-Government Service Tool?,” *J. Policy Leadersh. JPL*, vol. 9, no. 2, pp. 37–54, 2023.

[3] K. Kavuta and S. Nyamanga, “The Factors Affecting the Implementation of Students’ Records Management System to Higher Learning Institutions in Tanzania A Case of The Institute of Accountancy Arusha,” *Int. J. Sci. Technol. Res.*, vol. 7, no. 2, pp. 150–156, 2018.

[4] N. Obasi, E.O. Nwachukwu, and C. Ugwu, "A Novel Web-Based Student Academic Records Information System," *West African Journal of Industrial and Academic Research*, vol. 7, no. 1, pp. 31–47, 2013.

[5] A.E. Nwaomah, "Political factors’ influence on students’ records management effectiveness in the Nigerian university system," *European Journal of Research and Reflection in Management Sciences*, vol. 3, no. 2, pp. 29–41, 2015.

[6] J. A. O'brien and G.M. Marakas, Management information systems, vol. 6. New York, NY, *USA: McGraw-Hill Irwin*, 2006.

[7] Moshi Co-operative University, “MoCU Students Academic Registration Information System.” [Online]. Available:

https://musaris.mocu.ac.tz/auth

[8] Sokoine University of Agriculture, “SUA Students Information System.” [Online]. Available: https://suasis.sua.ac.tz/index.php/login

[9] A. Semlambo, N. Stanslaus, and G. Munguyatosha, “Factors Affecting the Security of Information Systems in Public Higher Learning Institutions in Tanzania,” *Inf. Technol. Int. J. Inf. Commun. Technol. ICT*, vol. 19, no. 2, pp. 43–65, 2022.

[10] F.A. Garba, S.B. Junaidu, I. Ahmad, and M. Tekanyi, "Proposed framework for effective detection and prediction of advanced persistent threats based on the cyber kill chain," Scientific and Practical Cyber Security Journal, vol. 3, no. 3, pp. 1–11, 2018.

[11] T. Yadav and A.M. Rao, "Technical aspects of cyber kill chain," in Security in Computing and Communications: *Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings*, vol. 3, pp. 438–452, Springer International Publishing, 2015.

[12] M. Korolov, “How attackers sidestep the cyber kill chain.” [Online]. Available: https://www.csoonline.com/article/572195/how-attackers-sidestep-the-cyber-kill-chain.html

[13] P.N. Bahrami, A. Dehghantanha, T. Dargahi, R.M. Parizi, K.K.R. Choo, and H.H. Javadi, "Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures," *Journal of Information Processing Systems*, vol. 15, no. 4, pp. 865–889, Aug. 2019, doi: 10.3745/JIPS.03.0126.

[14] National Research Council, Division on Engineering and Physical Sciences, Air Force Studies Board, and Committee on Future Air Force Needs for Survivability, Future Air Force Needs for Survivability. *National Academies Press*, 2006.

[15] E. Hutchins, M. Cloppert, and R. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” *Lead. Issues Inf. Warf. Secur. Res.*, vol. 1, no. 1, pp. 1–14, 2011.

[16] H. Penney, “Scale, Scope, Speed & Survivability: Winning the Kill Chain Competition,” *Mitchell Institute*, vol. 40, 2023.

[17] Y. Ahmed, A.T. Asyhari, and M.A. Rahman, "A cyber kill chain approach for detecting advanced persistent threats," Computers, Materials and Continua, vol. 67, no. 2, pp. 2497–2513, 2021.

[18] M. S. Khan, S. Siddiqui, and K. Ferens, “A Cognitive and Concurrent Cyber Kill Chain Model,” in *Computer and Network Security Essentials*, K. Daimi, Ed., Cham: Springer International Publishing, 2018, pp. 585–602. doi: 10.1007/978-3-319-58424-9_34.

[19] P. N. Bahrami, A. Dehghantanha, T. Dargahi, R. M. Parizi, K.-K. R. Choo, and H. H. S. Javadi, “Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures,” *J. Inf. Process. Syst.*, vol. 15, no. 4, pp. 865–889, Aug. 2019,

doi: 10.3745/JIPS.03.0126.

[20] H. Kim, H. Kwon, and K. K. Kim, "Modified cyber kill chain model for multimedia service environments," *Multimed. Tools Appl.*, vol. 78, no. 3, pp. 3153–3170, Feb. 2019, doi: 10.1007/s11042-018-5897-5.

[21] Pols, P., "The Unified Kill Chain–Raising Resilience against Advanced Cyber Attacks," *White Paper, The-Unified-Kill-Chain,* 2021.

[22] B. Strom, A. Applebaum, D. Miller, K. Nickels, A. Pennington, and C. Thomas, "Mitre att&ck: Design and philosophy. In Technical report," *He MITRE Corp.*, 2018.

[23] S. Gukurume, "Surveillance, spying and disciplining the university: deployment of state security agents on campus in Zimbabwe," *J. Asian Afr. Stud.*, vol. 54, no. 5, pp. 763-779, 2019.

[24] The Zimbabwean, "NUST System Hacked, Students De-registered, Results Deleted." [Online]. Available: https://www.thezimbabwean.co/2021/10/nust-system-hacked-students-de-registered-results-deleted/

[25] Y.A. Odugbesan, "Rebuilding the social fabric: challenging and transforming unwarranted influences in the educational institutions in Nigeria," *Doctoral Dissertation, Rutgers University-Graduate School-Newark*, 2017.

[26] The Herald, "Just In: CUT student hacks exam database, forges results." [Online]. Available: https://www.herald.co.zw/just-in-cut-student-hacks-exam-database-forges-results/

[27] The Citizen, "Iringa University IT students expelled after hacking campus online fee payment system." [Online]. Available: https://www.instagram.com/p/Css8c7YIEsh/

[28] J.A. Ampofo, "Challenges of student management information system (MIS) in Ghana: A case study of University for Development Studies, Wa Campus," *Int. J. of Management & Entrepreneurship Research*, vol. 2, no. 5, pp. 332-343, 2020.

[29] N. Fouad, "Securing higher education against cyberthreats: from an institutional risk to a national policy challenge," *J. Cyber Policy*, vol. 6, no. 2, pp. 137–154, 2021.

[30] M. Mshangi, "Enhancing Security of Information Systems in Tanzania: The Case of Education Sector," Doctoral dissertation, The Open University of Tanzania, 2020.

[31] E. Kundy and B. Lyimo, "Cyber Security Threats in Higher Learning Institutions in Tanzania, A Case of University of Arusha and Tumaini University Makumira," *Olva Acad. Res.*, vol. 2, no. 3, pp. 1–38, 2019.

[32] G. Rogers and T. Ashford, "Mitigating Higher Ed Cyber Attacks," *Assoc. Support. Comput. Users Educ.*, 2015.

[33] M. Bossetta, "The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy," *J. Int. Aff. Editor. Board*, vol. 71, no. 1.5, pp. 97–106, 2018.

[34] S. Zulkiffli, M. Zawawi, and F. Rahim, "Passive and active reconnaissance: a social engineering case study. In 2020 8th International Conference on Information Technology and Multimedia," pp. 138–143, 2020.

[35] M. Dabbagh, A.J. Ghandour, K. Fawaz, W. El Hajj, and H. Hajj, "Slow port scanning detection," *in Proc. 2011 7th International Conference on Information Assurance and Security (IAS)*, December 2011, pp. 228-233, IEEE.

[36] T. Hamed, R. Dara, and S. Kremer, *Intrusion detection in contemporary environments. In Computer and Information Security Handbook*. Morgan Kaufmann, 2017.

[37] Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B. and Ipsen, Y., 2018. Phishing and cybercrime risks in a university student community. *Available at SSRN 3176319*.

[38] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, 2021.

[39] Proofpoint, "State of the Phish: An in-depth look at user awareness, vulnerability and resilience," *2020 Annual Report*, 2020.

[40] N.S. Fouad, "Securing higher education against cyberthreats: from an institutional risk to a national policy challenge," *J. Cyber Policy*, vol. 6, no. 2, pp. 137-154, 2021.

[41] F. Aldauiji, O. Batarfi, and M. Bayousef, "Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art," *IEEE Access*, vol. 10, pp. 61695–61706, 2022, doi: 10.1109/ACCESS.2022.3181278.