Education and Information Technologies
https://doi.org/10.1007/s10639-025-13336-8

Collaborative online international learning as a third space to improve students' awareness of cybersecurity

Alison Lui[1] · **Catharina Womack**[2] · **Penny Orton**[2]

Received: 1 July 2024 / Accepted: 3 January 2025

Abstract

This article critically evaluates the effects of the ACU Virtual Mobility (VM) Project Digital Information Security Course (DISC) programme on improving students' awareness of cyber security skills, pre and post the educational intervention. Our selected VM tool is Collaborative Online International Learning (COIL). Building on a conceptual framework of COIL as a Third Space for teaching students from different countries, we show that COIL has a positive effect on glocalising cybersecurity. This enabled students to share their local experiences but work towards global solutions, since cybersecurity threats are global concerns. A cross-sectional survey design was used, with data collected using online questionnaires. The research was conducted at the Durban University of Technology (DUT), South Africa and at Liverpool John Moores University (LJMU), United Kingdom. Census sampling identified programme participants from DUT and LJMU, registered at the respective universities in 2024. Data were analysed statistically using descriptive statistics, Chi-square test of independence, One sample t-test and independent samples t-test. Results indicated that students reported cyber security as a high priority. This study confirms that students who are aware of cyber bullying have a greater ability to ensure their cyber security. An interesting finding was the difference between DUT and LJMU students on collaboration skills ($M = 4.84$, $t = (48.301)\ 2.478$, $p = .017$). The major contribution is the use of COIL as an educational intervention to increase students' cyber security awareness and enrich their learning experiences. Educators should consider adopting COIL as a pedagogical tool to educate students on cybersecurity and AI. This project has policy impact on social mobility and educational policies of the UK. We provide evidence to the ongoing dialogue in South Africa regarding student mobility and a stronger emphasis on short-term virtual mobility exchanges. This study focused on students who participated in the ACU virtual mobility project, DISC; therefore, the results may not be generalised to other projects of a similar nature. This study does not consider the long-term effects of this intervention on increasing cyber security awareness because it was of a cross-sectional design.

Extended author information available on the last page of the article

Published online: 23 January 2025

Keywords Collaborative Online International Learning · Virtual mobility; digital information · Cyber security awareness · Higher education · Educational intervention

1 Introduction

The Association of Commonwealth Universities (ACU) Virtual Mobility (VM) Project, Digital Information Security Course (DISC) involved a VM programme between Liverpool John Moores University and Durban University of Technology, towards improving students' digital security skills. The focus was on skills in digital security for two reasons. First, according to the National Audit Office, fraud in the UK now accounts for 40% of all reported crime, where 54% is cyber-related. South Africa ranked sixth in the world with cybercrime density, rising from 11.8 cybercrime victims per 1 million internet users in 2016 to 14.1 victims per 1 million in 2019, and 50.8/1 million users in 2020 (Chetty, 2022). Secondly, digital literacy skills are critical to employees for the future workplace. According to the McKinsey Report of 2022 (McKinsey & Company, 2022), demand for technological skills will grow.

The project involved four weekly Master classes from employers and academic staff on cyber-security skills. We particularly wanted guest speakers from both South Africa and England so that there was a balance of contribution to cybersecurity knowledge from both countries. This is important for the co-creation of knowledge in this global south-north partnership. The topics included social media minefields; the dark web; artificial intelligence and cybersecurity; deep fakes; online financial scams; scams in higher education. Students worked in small groups on a campaign educating the public about online security, meeting weekly. In the fifth and final session, the students presented their campaign (in digital format) and produced a group presentation. The campaign can be in the form of a brief video, cartoon or poster. Employers, staff and students voted for the winning work and provided feedback to students.

Project DISC was conducted online via Microsoft Teams and Zoom. The project was made accessible to as many students as possible in several ways. First, the project crossed international boundaries and included one university from the Global South, namely DUT; a merged university, which included an historically disadvantaged university in the South African higher education landscape. Most students at this university are previously disadvantaged (Black) and first-time higher education students. The city of Liverpool is ranked fifth nationally, in the United Kingdom, in deprivation. LJMU recruits 43% of its students from the Liverpool City Region. Thus, a large percentage of students are from lower socio-economic backgrounds and first-generation university students. Secondly, students who agreed to participate in the project had access to computers and Wi-Fi internet connection on campus. In addition, LJMU provided free laptops on loan to their students. Internet connection off campus in South Africa can be intermittent, therefore, the project was timetabled during the working day, where possible, to minimise internet disruption. Finally, the project was advertised and promoted through a range of methods such as email, social media platforms, and student societies, to reach as many students as possible.

The overall aim of the COIL project was to devise and run a COIL Project to improve students' cyber-security awareness and global citizenship skills, and to evaluate the success thereof. Our study is original and innovative because as far as we are aware, this is the first study to date to teach students in South Africa and England on cybersecurity awareness (including artificial intelligence's impact on cybersecurity) using COIL at the time of writing. We also measured the students' cybersecurity skills before and after the COIL project to see the effects of the project. We extended Wimpenny et al's theoretical framework on COIL as a Third Space to *glocalise* cybersecurity and AI teaching between students in South Africa and England. We found the COIL project was particularly helpful in improving DUT and LJMU students' cybersecurity and collaboration skills.

2 Background

2.1 The cybercrime landscape in South Africa and the United Kingdom

INTERPOL's 2023 Africa Cyberthreat Assessment report found that South Africa leads the African continent in the number of identified cybersecurity threats with 230 million threat detections in 2022 (Modise, 2023a, b). Morocco was in second place with 71 million threat detections. Moreover, cybersecurity company Surfshark reported cybercrime in South Africa increased by 8% from 2021 to 2022, which places the country in fifth position globally with 56 victims per 1 million internet users (Surfshark, 2022). South Africa`s annual cost of cybercrime victimization for the public amounts to approximately ZAR 2.2 billion (Mphatheni & Maluleke, 2022). The United Kingdom was ranked first globally for cybercrime density in 2022 with 4 371 victims per 1 million internet users (Gandhi et al., 2011). This is despite an 8.6% drop compared to 2021. Another survey by AAG IT Services triangulates this by confirming that the UK had the highest number of cybercrime victims per million internet users at 4 783 in 2022 (AAG IT Services, 2024). According to Barlow (2023), South Africa is a primary target in Africa for cybercrime because of three reasons. First, there is a lack of cyber awareness; secondly, investment in cybersecurity infrastructure is poor and thirdly, the enforcement of cybercrime laws is weak.

In 2022 the five most common types of cybercrime crimes worldwide were: phishing scams (53.2%), personal data breaches (10.4%), and non-payment, non-delivery (9.2%), extortion (7.0%) and technical support (5.8%) (Zandt, 2023). Consequently, Gondwe (2022) contends that South Africa needs a sustained national public awareness campaign to inform and mobilise the public against a growing pandemic of cybercrime. In South Africa, current crime statistics identify underlying tensions, wealth inequality, organised crime and government's response to police reform and crime intelligence in South Africa (Panchia, 2023) as reasons for the country being a cybercrime hotspot. It has been established that established and well-known South African organisations are being subjected to increased cyber-attacks, such as the Development Bank of Southern Africa (Greig, 2023) and Transnet (Pieterse, 2021). Furthermore, Awan (2024) contends that the most common types of smart phone

hacks are malware, phishing, WIFI attacks, physical access and social engineering. The author further avers that the most common type of smart phones hacked are Samsung, iPhone, Xiaomi, Huwai and LG.

Data from the National Fraud Intelligence Bureau in the UK reveals that between 2023 and 24, the top three cybercrime offences against individuals are hacking (social media and emails); hacking (personal) and computer virus/malware (National Federation of Intelligence Bureau, 2024). Prümmer et al., (2024) contend that several cyberattacks can be ascribed to weaknesses related to humans working within organisations. Mohammed (2022) agrees that the majority of workers do not sufficiently follow the specific cyber security policies, rules and directives provided at work. Against businesses, the top cybercrime offence is still hacking (social media and emails); the second is hacking of servers and the third is hacking in the form of extortion (National Federation of Intelligence Bureau, 2024). The key enablers of hacking are phishing emails to initiate cyber-attacks and fraud, as well as weak passwords (Action Fraud, 2024). The goals in both hacking and phishing are the same, namely, to steal personal information and financial details from the victims. However, hacking occurs when the victims do not voluntarily disclose their personal information, whereas victims disclose personal information through phishing, because criminals pretend to be from a trusted source such as a bank. Hence, an informed and proactive approach to cybersecurity is necessary (Taherdoost, 2024). In addition, Aliyu et al. (2010) aver, due to their frequent use of technology, being careless and sometimes even reckless in their computer usage, students are considered the most vulnerable with regard to cyber-attacks. Lepan (2017) further contends South African youth, as a result of the many challenges they face in the country, put themselves more at risk for online exploitation. Pramod and Raman (2014) reported students in higher education are aware of security concerns where their smartphones are concerned; however, they are not fully aware of all the risks and the security practices. Consequently, Yamin et al. (2020) contend being informed and prepared is the first defence against cyber threats and cybercrimes through, for example, information security training. The UK Action Fraud data show that young people between 20 and 39 years old are in the highest risk of being a cybercrime victim (Action Fraud, 2024). Action Fraud explain this result first that young people in this age category frequently use digital technology and secondly, they are more likely to report cybercrimes. The latter point is interesting, since our survey results show that a significant proportion of the LJMU respondents never reported phishing by hitting the spam or 'report phishing' buttons.

2.2 Weaknesses in enforcement and public awareness campaigns

Kavanagh (2021) contends the 'gap' in law enforcement cyber capabilities within and across regions needs to be addressed, as this gap is a key enabler for criminal opportunities, networks and infrastructure. The author further asserts this enables cyber-criminals to exploit borderless playing fields in the digital world, particularly where the law enforcement structure is limited to its national borders (Kavanagh, 2021). Moreover, INTERPOL's 2021 report

maintained prevention is key in the face of continuously growing cyber threats, as enforcement by itself is not a complete solution. INTERPOL'S, 2023 African Cyberthreat assessment report maintained that law enforcement agencies in the African region need robust and well-structured cybercrime and cybersecurity mechanisms to effectively combat cybercrime. The 2023 INTERPOL report, nevertheless, contends having policies, legislation and agencies in place can provide an appropriate level of response to the broad range of cyber threats and incidents countries are faced with globally. However, as technology is advancing, cybercriminals are also adapting, making it difficult for the average user to keep up with the criminals (Dipa, 2023). Whilst there is to date no single database showing the cross-national law enforcement actions against cybercriminals, there is both qualitative and quantitative data revealing that there is a significant cyber enforcement gap. In the United States of America for example, less than 1% of cyber incidents that occur annually in the United States of America resulted in an actual arrest (Eoyang et al., 2018). This is a significant lacuna in the current global cybersecurity law enforcement framework since cybercrimes are global.

The UK Cyber Aware Campaign website calls for stronger password protection and raises cybersecurity awareness on the website and the National Protective Security Authority has developed several cybersecurity awareness campaigns. Nevertheless, an academic study in 2020 (van Steen et al., 2020) shows that national cybersecurity awareness campaigns are often unsuccessful because they try to provide a one-size-fits-all programme. Their research reviews the national cybersecurity awareness campaigns of 17 governments, including the UK and South Africa. Ticket scams are different to investment scams or ransomware attacks, so national campaigns should be more tailored and targeted to specific sectors of society. Awareness does not necessarily translate into change in human behaviour, but van Steen et al. (2020) argue that many government campaigns rely on the assumption that by raising public awareness on cybersecurity risks, the public will change their behaviour. Often, education of why we should take certain steps are necessary to see a change in human behaviour. So, when dealing with cybersecurity, knowledge alone will not be of significance unless it is used to influence outcomes and to encourage behaviours (Chaudhary, 2024). Most importantly, campaigns should teach the public to have the right skills and increase confidence to deal with cybersecurity threats.

2.3 Virtual mobility as a delivery method of cybersecurity awareness in higher education

A plethora of methods is available to teach cybersecurity awareness offline and online in higher education. The offline mode of teaching in a classroom is often top-down, utilising experts such as instructors to impart knowledge with the students. A classroom style is helpful to illicit non-verbal cues from students and interact with them. The main disadvantage of a classroom-style delivery is that it can be a "static solution for a fluid problem" (Valentine, 2006). Cybersecurity is constantly evolving but a conventional classroom-based delivery model can lack participatory opportunities. Much depends on

the instructor's ability to engage and sustain the learners' attention and interest to avoid a static learning situation. Therefore, instructors need to build in discussions, group work and exercises to stimulate the learning process in classroom-based learning (Abawajy, 2014).

Online delivery modes include blogs, emails, animations, online synchronous and asynchronous discussions, multimedia (Abawajy, 2014). In an educational context, there are also simulation and game-based learning. These types of learning are interactive and engaging (Cone et al., 2007), although often, licences need to be purchased for game-based learning. CyberCIEGE is an example of teaching cybersecurity awareness using game-based learning. When teaching cybersecurity to students from different cultures however, the effectiveness of game-based learning should take into account of language. For example, Fung et al. (2008) compared the delivery of cybersecurity awareness between a traditional class-based environment and game-based learning. Interestingly, 75% students who learnt about cybersecurity in a classroom environment improved their cybersecurity awareness compared to 60% who learnt via games. The authors explained a possible reason for this is that students in the classroom setting learnt in Thai, their mother tongue, although the teaching materials were in English. In the game-based setting, students learnt entirely in English.

Online learning has made learning more internationalised because the internet is relatively borderless, in that many people have internet access these days. Nonetheless, digital poverty, exclusion, power cuts are obstacles to internet access in some global south countries. South Africa for example, implements a load shedding schedule to avoid power blackouts. Another criticism of online learning is that knowledge remains predominantly western based (Wimpenny et al., 2022). To remedy this, Montgomery (2019) calls for co-creation of new 'Global Southern' knowledge through collaborative online learning between South-North or South-South countries. One way of achieving this is through Collaborative Online International Learning (COIL). It is a type of virtual mobility where students from different countries learning together on a mutually agreed topic using digital technology. COIL improves students' global citizenship skills, inter-cultural awareness and soft skills such as teamwork and leadership. They learn about contemporary topics which affect professional globally. COIL is most often used in language training and cultural training at higher education institutions (Lewis & O'Dowd, 2016), but it is still an emerging pedagogical method in other areas such as Law and cybersecurity.

2.4 Aim of the study

The aim of this study was to critically evaluate the ACU DISC COIL programme's influence in improving student awareness of cybersecurity.

2.5 Theoretical model

We build on existing scholars' models of COIL as a Third Space of co-teaching and co-learning in higher education, developing students into global citizens through COIL on the topic of cybersecurity awareness, which includes artificial intelligence.

The concept of a Third Space means that COIL is seen as "a symbolic in-between space, enabled through cultural difference and offering generative potential beyond the 'either/or' limits of dualities" (Zhou & Pilcher, 2018). For several scholars (Bhabha, 1994; Lorde, 2012), COIL is an alternative space to create dialogues and discussions for students representing different perspectives at an international level. Discourses can arise (Moje et al., 2004) but since COIL promotes mutual respect and understanding, it is capable of generating new knowledge and perspectives without dismissing speakers' experiences (Wimpenny et al., 2022). COIL has been used in projects to foster diversity and inclusivity successfully. As such, we have considered the extant literature in this area by Wimpenny and Orsini-Jones (Wimpenny & Orsini-Jones, 2020); Le Grange (2016). In particular, Wimpenny and Orsini-Jones view COIL as an important teaching platform to g/localise the learning experience. COIL students share their local experiences and context on global challenges via COIL, thus providing a *glocalised* discussions and solutions (Fig. 1).

In our COIL project between DUT and LJMU, we adopt Wimpenny et al's conceptual framework of Third Space COIL exchange in the context of improving students' cybersecurity awareness and skills. As a South-North COIL project, we share the authors' views of incorporating key values and capital concepts into COIL. These are important to promote open, honest and authentic discussions online, which help to foster trust between the students. The capital concepts address some of the common problems arising from COIL namely three gaps identified by Stallivieri. First, the linguistic gap in the learning environment because many students in COIL projects speak English as their second language. Secondly, the digitisation gap due to technological challenges to access the internet. Thirdly, structural gap in

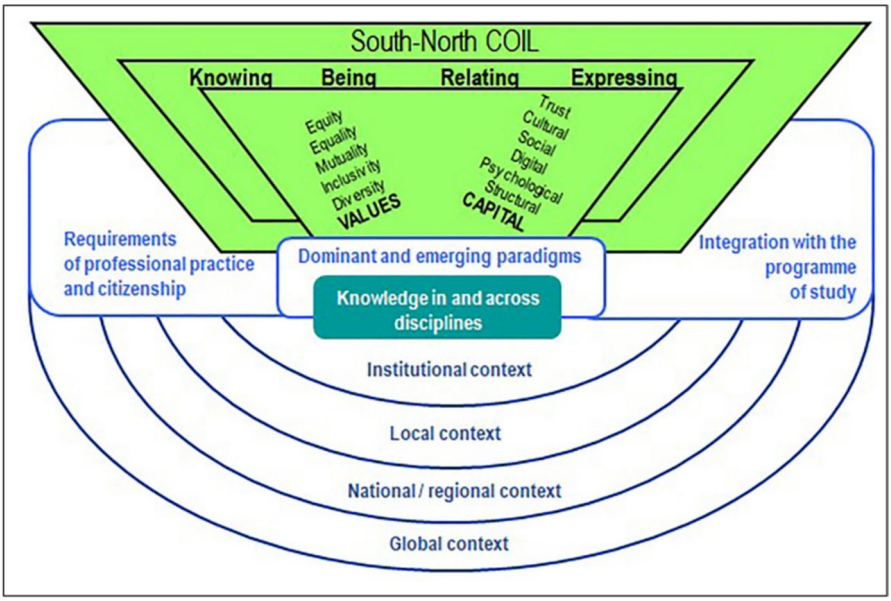

Fig. 1 A conceptual framework on Third Space COIL exchange model by Wimpenny et al. (2022)

higher education in the sense of challenges arising from timetabling and flexibility in the curriculum to incorporate COIL.

In our project, we addressed the three gaps by the following steps. The linguistic gap was not a big challenge, since DUT students, albeit from many ethnic groups, speak very good English. They have to meet a minimum requirement to gain a place at DUT. When there are instances of words or terms which are unfamiliar to certain students, we tried to find alternative ways to explain. We addressed the digital gap by scheduling the COIL classes during the working day in South Africa, so that students can have access to computers and laptops on campus. Wi-Fi on campus was also more reliable than off-campus. For students who missed the classes, we recorded the classes. Finally, there was considerable flexibility in structuring the classes, since we designed the project as an extra-curricular activity. We designed learning objectives and outcomes just like a module, as well as a group task which was unassessed. We did not have to decide which module we had to embed the COIL project.

The different layers of contextual learning in the diagram are very useful to our project. We measured students' cybersecurity awareness before and after the COIL project through questionnaires. The first questionnaire was completed by students prior to commencement of the project. The questionnaire asked straightforward questions on students' awareness, knowledge and confidence of cyber security. Students' perceptions of their skills were measured using a Likert scale on declarative statements. In the final session, the students received a second questionnaire to complete. This was similar to the first questionnaire but included additional questions regarding how, if in any way, the project had increased their knowledge and confidence on cybersecurity. As revealed in the discussion section, the *glocalised* environment is really useful to try and understand the differences in some of the results in for example, DUT students' view of cybersecurity as a very high priority as opposed to high priority amongst LJMU students; DUT students being more concerned about cyberbullying, and they are keener to report scams than LJMU students. Our article is therefore original for two reasons. First, we show that COIL has been a particularly helpful pedagogy in improving DUT students' cybersecurity and collaboration skills. Secondly, we have adapted Wimpenny et al's conceptual framework of COIL as a Third Space of teaching students from different countries. We show that COIL has a positive effect on glocalising cybersecurity. This enables students to share their local experiences but work towards global solutions, since cybersecurity threats are global concerns.

2.6 Research methods

A quantitative cross-sectional survey design was used for this research (Polit & Beck, 2012). This was appropriate for the variables under review; a COIL programme educating students on cyber security, within a real-life, contemporary setting. The research was conducted in Durban, KwaZulu Natal, South Africa and Liverpool, United Kingdom. The Durban University of Technology (DUT) has approximately 33,000 registered students, of which 807 are registered in the Faculty

of Management Sciences. KwaZulu Natal is one of nine provinces in South Africa and the second most populous, with a population of 11.10 million. This province comprises a multi-ethnic society, comprising Black Africans, predominantly Zulu speaking, Asians and both English and Afrikaans speaking Coloured and Caucasian people.

Ranked fifth nationally in poverty, LJMU recruits 43% of its students from the Liverpool City Region Combined Authority. Thus, a large student percentage is from lower socio-economic backgrounds and first-generation university students. LJMU was founded in 1823 as the Liverpool Mechanics' School of Arts. It became a university in 1992 and has roughly 27,000 students from more than 100 countries world-wide, 2,400 staff and 250 degree courses.

The target population for this study comprised DUT PhD, Masters, Postgraduate and Advanced Diploma Management Sciences, and Business Law students and LJMU Faculty of Business and Law students, registered at the respective universities in 2024. All selected students participated in the ACU COIL Project DISC programme between LJMU and DUT, to improve students' digital security skills. Potential participants were approached, informed regarding the study, and asked whether they would be interested in participating. Those who expressed an interest were provided a letter of information to read further.

The census method for sampling was employed as the target population of 100 was considered small. The census method was deemed appropriate, as it is reliable and accurate, results collected are less biased, diverse characteristics can be studied, and all items collected are examined, with the information gathered being thorough and widespread. The target population size of 100 (50 from DUT and 50 from LJMU) was sought for the questionnaire. A final sample realisation of 55% (55 respondents) was recruited for the pre-intervention survey, while only 30% (30 respondents) completed the post-intervention survey questionnaire. The post intervention sample was impacted by a non-response bias which was thought to be due to student`s lack of interest in participating following the end of the intervention and many competing demands on their time. The end of the project coincided with the Spring holiday and many students who were also preparing for assessments and movement towards examinations and semester end. They did not receive any incentive to participate, and the researchers relied on the voluntary participation of the students. This non return bias was despite several reminders to students to participate and that it was online and therefore available at a convenient time for completion. Participants who agreed to participate in this study may have a more positive attitude towards cyber security and its role in being victims of cyber-crime and potentially influencing results. The potential impact of this could be a sampling bias which means the results are not generalizable.

Permission to conduct this study was granted by the Durban University of Technology University Research Ethics Committee (IREC 218/23). Gatekeeper permission to access students at DUT was received from the Deputy Vice Chancellor for Research, Innovation and Engagement at DUT. At LJMU, the Principal Investigator completed the University Research Ethics Committee (UREC) Minimal Risk Registration Form and obtained relevant ethical approval from the UREC (23/LAW/004). The principle of autonomy was observed, with all

participants provided information on the study and the freedom to choose to participate without fear or favour, while written informed consent was also sought. Participants experienced no harm through their participation. There were no foreseeable risks for the students. No sensitive questions were posed and those who participated were not in a vulnerable population group. All electronic data are held on a password protected computer, only accessible by the two principal investigators. All electronic data will be deleted from the computers after five years (end of 2029).

Data were collected pre- and post-intervention using anonymised questionnaires developed by one of the researchers following a literature review, and from her personal experience as a scholar in the field. Survey data were collected via Google Forms, having sent the participants a link to access the questionnaire. The questionnaire included five (5) sections with a total of 15 questions. The sections included demographic data, engagement and capabilities, risks and consequences, responsibility and reliance and artificial intelligence and cyber security. The first questionnaire was completed by students prior to commencement of the COIL project. The questionnaire asked straightforward questions on students' awareness, knowledge and confidence of cyber security. Students' perceptions of their skills were measured using a Likert scale on declarative statements with options ranging between strongly agree to strongly disagree. In the final session, the students received a second questionnaire (Evaluation Survey) to complete. This was like the first questionnaire but included additional questions regarding how, if in any way, the project had increased their knowledge and confidence on cyber security awareness.

Quantitative data were analysed statistically on IBM SPSS (v. 27) and the following tests applied:

- Descriptive statistics, including means and standard deviations, where applicable.
- Chi-square test of independence: used on cross-tabulations to determine whether a significant relationship existed between the two variables represented in the cross-tabulation. When conditions were not met, Fisher's exact test was used.
- One sample t-test: Tested whether the mean score was significantly different from the scalar value.
- Independent samples t-test: used to compare two independent groups of cases.

The survey questionnaire was assessed for clarity, unambiguous language and ease of understanding the language, through piloting with ten students (five from DUT and five from LJMU), following ethical approval from the respective universities. This data was not included in the final data set.

The students benefited from the project, as it increased their awareness of cybersecurity. This study will be of value to future students through the sustainability of the project, as evidenced by student recommendations to continue offering the project.

3 Results

The questionnaires were administered to participants pre- and post-intervention. The results are reported in that order, with a comparative analysis at the end.

3.1 Pre-intervention results

A sample realisation of 55% ($N=55$) was achieved, of which $n=30$ were from LJMU and $n=25$ from DUT. Those sampled were predominantly female (65%, $n=36$), with males only constituting a little over a third of those sampled (35%, $n=19$). DUT female respondents made up 76% ($n=19$) of the DUT cohort. The respondents tended to be between the ages of 18 to 28 years (85%, $n=47$).

Pre-intervention, the question "how much would you say you know about how best to protect yourself from harmful cyber activity?", indicated a significant relationship between knowledge on how to protect oneself from harmful cyber activity and the university students were registered at, Fisher's exact = 7.713, $p=.025$, Cramer`s V 0.377. A significant proportion of those from DUT (44.0%) indicated they know *"not very much"*, while a significant proportion of student participants from LJMU (73.3%) indicated they know "*a fair amount*". Respondents were asked to rate their agreement that "most information on how to be secure online is confusing". The scale used is 1 = strongly disagree to 5 = strongly agree. Across both universities, the average agreement score is 3.15, which is not significantly different from the neutral score of '3' ($p=.280$, 95% CI [−0.114, 0.417]). Thus, neither significant agreement nor significant disagreement were found for this statement. Respondents from DUT agreed significantly more (M = 3.52) than those from LJMU (M = 2.83) that most information on how to be secure online is confusing, t (53) = −2.710, $p=.009$, 95% CI [0.189, 1.286]. When asked "How high or low a priority is cyber security to you?", respondents were found to rate cyber-security as a high priority (M = 4.11, t (54) = 8.604, p = < 0.001, 95% CI [0.819, 1.503]. DUT respondents (M = 4.48) gave this a significantly higher priority than LJMU (M = 3.80), t= (53) 2.787, $p=.007$, 95% CI [0.205, 1.304]. Compared to DUT respondents, a significant proportion of respondents from LJMU 'never' report phishing by hitting the spam or 'report phishing' buttons, Fisher's = 9.513, $p=.045$, Cramer`s V 0.424.

The question, "to what extent, if at all, do you think about protecting your own privacy?", elicited a response from 46.7% (n = 14) LJMU students that, *"I think about it sometimes"*. However, the DUT students responded "*I think about it a lot"* n = 25 (100%), Fisher`s = 20.582, p = < .001, Cramer`s V.585. When asked "to what extent, if at all, do you think about avoiding losing photos ", 36.7% (n = 11) LJMU students, on the one hand, responded *"I think about it sometimes"*. The DUT students, on the other hand, responded "*I think about it a lot"* n = 19 (76%), Fisher`s = 6.978, p = .028, Cramer`s V .363.

In response to the question, "to what extent, if at all, do you think about avoiding any potential wider impact on other people and organisations?", 26.7% (n = 8) LJMU students responded, "*I never think about it*". The DUT students, however,

responded "*I think about it a lot"* n = 18 (72%), Fisher`s = 14.219, p = < .001, Cramer`s V .502. When asked "to what extent, if at all, do you think about avoiding being bullied online?", LJMU students responded "*I never think about it"*, n = 8, 29.6% and "*I think about it sometimes"* n = 13, 48.1% .The DUT students responded "*I think about it a lot"* n = 20 (80%), Fisher`s = 17.724, p = < .001, Cramer`s V .583.

The question, "How reliant, if at all, are you on other people for checking the security settings on your devices?" elicited a response from 45.8% ($n = 11$) DUT students that stated they are "*partly reliant on others"* and 12.5%, $n = 3$ responded they were "*fully reliant on others"*. Furthermore, LJMU students reported "*not being reliant at all"* ($n = 24$, 80%), Fisher`s 9.176, $p = .006$, Cramer`s V.424. DUT students were more reliant on others to help create their online accounts. Seven (28%) students reported being "*partly reliant on others"* to help create their online accounts and 12%, $n = 3$ responded they were "*fully reliant on others"*, Fisher`s 11.009, p = .002, Cramer`s V 0.459.

In response to the question, "how much would you say you know about facial recognition?", eight (26.7%) LJMU students admitted "*not very much"*, while $n = 14$ (56%) DUT students suggested "*a great deal"*, Fisher`s 6.819, p = .034, Cramer`s V 0.637. When asked whether they "would like to learn more about the role of artificial intelligence in cyber security?", DUT students agreed significantly more than those from LJMU (n = 25, M = 4.96, t= (42.537) 2.193, p = .034, 95% CI [0.009, 1.091]).

3.2 Post-intervention results

A post-intervention sample realisation of 30% ($N = 30$) was achieved, of which $n = 12$ were from LJMU and $n = 18$ from DUT. Those sampled were predominantly female (80%, $n = 24$), with males only constituting a third of those sampled (20%, $n = 6$). A little more than half the respondents were between the ages of 18 to 28 years (53%, $n = 16$); six (20%) were between 29 and 39 years of age; four (13%) were aged 40 to 50 years and four (13%) from DUT were 51 plus years of age.

Post-intervention there was no significant relationship between students' knowledge on how to protect themselves from harmful cyber activity and the university they were attending. There was disagreement between LJMU respondents (M = 2.83, SD 1.193) with the statement "most information on how to be secure online is confusing…" and DUT respondents (M = 3.67, SD 1.029), who tended to agree with the statement, despite the intervention. When asked "How high or low a priority is cyber security to you?" respondents were found to rate cyber-security as a high priority (M = 4.67, t (29) = 16.699, p = < 0.001. The mean indicates a marginal increase on the pre-intervention score. There was no significant difference in this across universities. To the question "how much would you say you know about deep fakes", slightly more than half ($n = 7$; 58.3%) LJMU students sampled responded "*a great deal"*, while 44.4% ($n = 8$) DUT students responded, "*not very much"*, Fisher`s 11.914, p = .004.

In summary, DUT students showed significantly more agreement than LJMU respondents when asked "to what extent, if at all, do you agree or disagree with

this statement? This project improved student's collaboration skills." (M = 4.84, t= (48.301) 2.478, p = .017, 95% CI [−0.962, 0.503]).

3.3 Comparative results

Engagement and capability As illustrated, DUT respondents tended to agree information on how to be secure online was confusing, 95% CI [−0.079, 0.651] (Fig. 2).

For both pre- and post-intervention, a significantly high priority was assigned to cyber security, $p < .001$, 95% CI [2.202, 3.904] and 95% CI [0.819, 1.503] in each case. There was significant agreement pre- and post-intervention that losing money or personal details over the internet these days has become unavoidable: Pre-intervention t=(54) 2.548, $p = .014$, 95% CI [0.072, 0.616] and post-intervention t=(29) 2.186, $p = .037$, 95% CI [0.027, 0.771]. There was no significant difference across the two universities. Respondents indicated significant disagreement to the statement "I rely on friends and family for help on cyber security" both at pre-intervention testing ($n = 55$, M = 2.62, SD 1.063, t= (54) −2.665, $p = .010$, 95% CI [−0.630, −0.085]) and post-intervention ($n = 30$, M = 2.50, SD 1.137, t=(29) −2.408, $p = .023$, 95% CI [−0.815, −0.065]). There were no significant differences across the two universities.

When asked to respond to the statements "I am aware of the role of artificial intelligence in cyber security" and "I would like to learn more about the role of artificial intelligence in cyber security", there was significant agreement both pre- and post-intervention. Analysis of the first statement responses indicated $N = 55$,

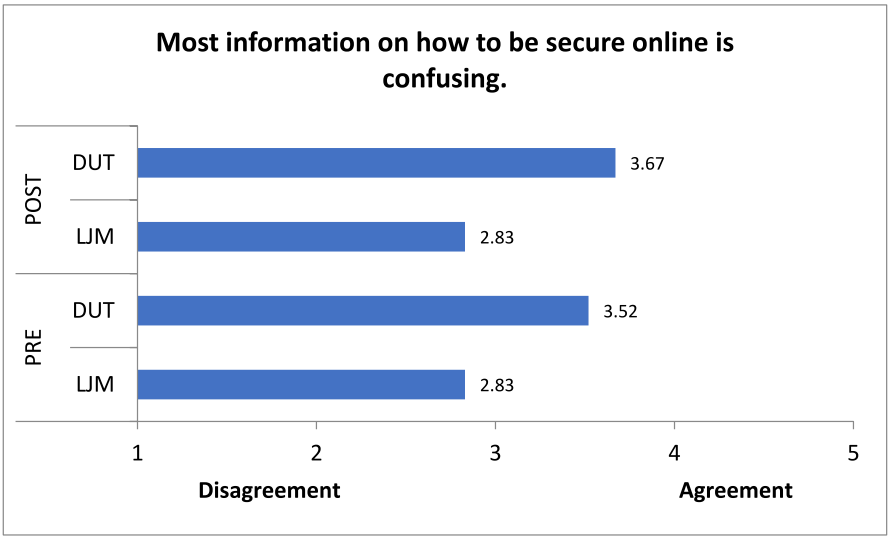

Fig. 2 Responses to the survey question "Information on online security is confusing"

M = 3.56, t=(54) 4.886, p = < 0.001, 95% CI [1.277,2.464] and 95% CI [0.363, 0.945] and to the statement "I would like to learn more …" $N = 30$, M = 4.47, t=(29) 9.337, p = < 0.001 95% CI [1.148, 2.271] and 95% CI [4.190, 6.203].

4 Discussion

Access to the internet is fundamental to contemporary life; however, with this comes increased security risks. The results of this study support findings by Pramod and Raman (2014), who reported students in higher education are aware of security concerns regarding their smartphones, nonetheless, they are not fully aware of all the risks and security practices. The current study found students reported cybersecurity was a high priority, with DUT students according this a significantly higher priority than those from LJMU. This result was corroborated by Huraj et al. (2023), who showed students not only recognize but also care about the importance of cybersecurity. Prior to the awareness project, a significant proportion of DUT students indicated they did not know much regarding how to protect themselves from harmful cyber activity, whereas a significant proportion of LJMU students indicated they knew a fair amount. LJMU had an active cybersecurity campaign during 2022–2023, and students were encouraged to complete a free self-learning module on cybersecurity. As such, this may explain why more DUT students felt that they did not know much about how to protect themselves from harmful cyber activity in comparison to LJMU students.

A study of Nigerian university students reported they did not have basic knowledge of cyber security and there was a need to introduce cyber security awareness training (Garba et al., 2020). The DUT students agreed significantly more than LJMU students that most information on how to be secure online is confusing. A number of studies have narrated this theme of cyber security information being confusing (Kolouch et al., 2023; Reeves et al., 2021; Thompson et al., 2018). In addition, the DUT respondents rated cyber-security as a significantly higher priority than the LJMU respondents. This finding was consistent for both pre- and post-intervention, with a significantly high priority assigned to cyber security. This is supported by the finding that DUT students frequently thought about protecting their own privacy, in contrast to LJMU students, who only sometimes thought about it.

A further finding of interest, is that the DUT students were far more concerned with avoiding being bullied online, which they frequently thought of. This is in contrast to the LJMU students only sometimes thought about it. Cyberbullying is prevalent worldwide but students who are aware of cyberbullying have a greater ability to ensure their personal cybersecurity. Students' reasons for using the internet reportedly impact their awareness of cyberbullying (Zorlu, 2023). Students who use the internet for educational purposes have significantly higher awareness of cyberbullying than those who use it for entertainment (Zorlu, 2023; Odacı & Çelik, 2017). Our results are consistent with a study by Zwilling et al. (2022) who revealed that there was a connection between the respondent's country of residence, awareness, knowledge and behaviours in cybersecurity. Comparing results between respondents in Turkey, Poland and Israel, Zwilling et al. (2022) found that Turkish respondents

perceive cybersecurity as very threatening. Israelis and Poles showed less concern. This can be explained by cultural differences, in that Israel is very advanced in cybersecurity innovation (Tabansky, 2013). According to the MIT Technology Review Cyber Defence Index 2022/23, Poland is ranked sixth as the most resilient to cyberattacks according to the country's cybersecurity policies, organisational capabilities and cybersecurity assets. This also explains why the Poles were less concerned than the Turkish respondents. The UK is ranked seventh in the world. South Africa does not feature in the top 20 places of the MIT Technology Review Cyber Defence Index. From our comparative results above regarding DUT students being far more concerned with cyber bullying and online security then LJMU students, this may be explained by Zwilling et al's study that the UK is ranked higher than South Africa nationally for cyber resilience, and thus UK students perceive cyber bullying as less threatening than DUT students. Individuals' knowledge, understanding and perception of cybersecurity threats depend on other factors such as the role of media and social media. Manwaring and Holloway's (2023) research on cyber-enabled foreign interference in Australia reveals that Australians' threat perceptions of cyber operations are informed by media reports of similar attacks in other countries. This means that many Australians might have poor knowledge of what actual risk Australia faces, and the source of such threats, through what means and for what purposes. The policy recommendation arising from this is that Manwaring and Holloway (2023) advise that a more inclusive approach of understanding citizens' concerns would lead to a more informed and enriched cyber defence strategy. The UK's cyber strategy is led by the government but states that individuals have personal responsibility to take all reasonable steps to safeguard both hardware and software. The UK government will provide timely support but there does not appear to be any inclusion of citizens' voices or expressions of concerns. Similarly, the South African National Cybersecurity Policy Framework (South Africa, State Security Agency, 2015) outlines in Sect. 18 the role and responsibility of the civil society. Citizens should keep hardware and software secure, as well as reporting security incidents to the relevant authorities. A policy recommendation arising from our research is thus to call for citizens' voices and concerns to be included in the UK and South African cyber security frameworks. These concerns would shape better suited actions to reduce cyber security threats.

The strong positions of Israel, Poland and the UK have led to the situation where many of their citizens are under the false impression that they have sufficient knowledge or tools to deal with cyber threats (Zwilling et al., 2022). The more nervous disposition of many Turkish respondents in Zwilling et al's study and DUT's students in our study can be explained by the fact that Turkey and South Africa are not as strong as the UK in cyber defence. South Africa has limited skilled human capital with organisations and government failing to manage cybersecurity with cybercrime victimization as evidence of the country`s under preparation to manage cybercrime (Chigada, 2023). This behaviour is aligned with Fishbein and Ajzen's Theory of Planned Behaviour (Fishbein & Ajzen, 2011). According to this theory, people are motivated to change their behaviour, such as taking cybersecurity precautions, if they are knowledgeable about the risks and thus wish to protect themselves. Zwilling et al. acknowledged that the relationship is more complicated when an action

requires a higher level of specialised knowledge. In this situation, people might be aware of the risks and intend to protect their devices, but they do not feel confident in taking the relevant steps. This would then reduce their motivation to change. Cybersecurity awareness programmes are thus crucial to motivate people to be more proactive in preventing cyber threats (Zwilling et al., 2022).

A noteworthy finding is the greater the level of concern from DUT students in avoiding any potential wider impact on other people and organisations, whereas the LJMU students never thought about it. This is further supported by the finding that a significant proportion of the LJMU respondents never reported phishing by hitting the spam or 'report phishing' buttons. Chandarman and van Niekerk (2017) determined shortcomings in the cyber-security awareness of many university students. In addition, a dissonance was found between knowledge of cyber-security and behaviour (Chandarman & van Niekerk, 2017), which might be evident in the LJMU students, who appear to know a fair amount on the subject of how to protect themselves but do not ever report phishing emails.

Pre-intervention, it was found DUT students are reliant on others to check the security settings on their devices, whereas the LJMU students do not rely on others at all. It was further found DUT students were also more dependent on others to help create online accounts. However, pre- and post-intervention there was significant disagreement amongst respondents regarding their reliance on friends and family for cyber security assistance. Redmiles et al. (2016) reported this as a common finding in their research. In addition, they reported that this did not have anything to do with the family or friend being an expert in information technology but rather perceiving the family member or friend as being "a bit of a techie" (Redmiles et al., 2016).

Another interesting finding pre-intervention was the LJMU students' admittance to not knowing much regarding facial recognition, whereas the DUT students suggested they knew a great deal. This could account for why the DUT students were far more concerned about avoiding losing photos, which they thought a lot about, as opposed to the LJMU students who only thought about it sometimes. This supports findings by Huraj et al. (2023), with regard to Computer Science students' wariness in putting their personal information on social networks. Although it was interesting to note that post-intervention, the LJMU students knew a great deal regarding deep fakes, whereas the DUT students did not know much of deep fakes. There was also significant agreement pre- and post-intervention that losing money or personal details over the internet is unavoidable these days.

The results of this study further support (Yamin et al., 2020), who contend being informed and prepared is the first defence against cyber threats and cybercrimes. The DUT students indicated significantly more agreement than the LJMU students that they would like to learn more regarding the role of AI in cyber security. There was significant agreement both pre- and post-intervention with student awareness of the AI role in cyber security and wanting to learn more regarding the role of AI in cyber security. It was found DUT students agreed significantly more than LJMU students that the ACU project improved student's collaboration skills.

Not only does our study extend the conceptual framework of Wimpenny et al. (2022) on COIL as a Third Space in teaching cybersecurity awareness and *glocalising* knowledge creation, our results also show that COIL is a useful learning tool

and providing an international experience for students. Outbound student mobility is challenging for many students, especially from low socio-economic backgrounds. Between 2015 and 16, the participation rate is 2.5% for students from higher socio-economic backgrounds in the UK compared to 1.5% for students from lower socio-economic backgrounds (Universities UK, 2022). Yet, it is well known that students who participate in mobility schemes are more likely to gain a better degree classification and more likely to obtain a graduate level job (Universities UK, 2022). The results are more pronounced for students from lower socioeconomic backgrounds. Graduates from such backgrounds who were mobile during their degree earned 6.1% more, and those in work were more likely to be in a graduate level job (80.2% compared to 74.7%) than their non-mobile peers (Universities UK, 2022). COIL is a useful tool to provide an international experience to students who cannot participate in physical student mobility. Thus, our research contributes to the government's social mobility and educational policies of the UK. Similar statistics in South Africa have been difficult to obtain. Nevertheless, online resources reveal that few South African students participate in outbound student mobility due to lack of confidence and insufficient funding (Anstey, 2023b). Some schemes such as the French South Africa Scholarship and Erasmus Plus are very popular, but others had poor or no participation (Anstey, 2023a). At the 7th Biennial Research and Innovation Dialogue in South Africa in 2023, there was a discussion about rethinking the traditional physical student mobility model, which can be inflexible and damaging to the climate (Anstey, 2023b). Thus, we are providing evidenced research to this ongoing dialogue in South Africa regarding student mobility and a stronger emphasis on short-term virtual mobility exchanges. Globally, educators should consider COIL as a vehicle for enriching students' learning experiences. Cybersecurity problems require global leaders to solve, and COIL is a good way of raising students' global citizenship and collaboration skills.

4.1 Limitations of the study

We are aware that the sample utilised in this study is small. We have tried very hard to obtain more responses for the post-intervention questionnaire, but many students were on their Spring break or started assessments at LJMU. However, our methodology and analysis process are very rigorous. We have used a pilot study to test the questionnaires; used a Chi-square test of independence; one sample t-test and independent samples t-test to compare two independent groups of cases. The small sample size, inconsistencies in responses and potential biases in self-reported data may affect the reliability of the study findings.

This study is focused solely on students who participated in the ACU virtual mobility project, DISC; therefore, the results may not be generalised to other projects of a similar nature. This study does not consider the long-term effects of this intervention on increasing cyber security awareness because it was of a cross-sectional design. The researchers acknowledge that the narrow focus of the questionnaires. Students' awareness, knowledge, and confidence regarding cybersecurity may have caused other important factors to be overlooked. This study was exploratory,

and these factors could be further explored in a subsequent study. Future research would benefit from a larger sample of students and given the students' appetite for more learning of AI and cybersecurity. Since university students generally study for a maximum for three years, a longitudinal study is possible if we start from the first year and repeat the study in their final year.

5 Conclusion

Our project tested whether our DISC programme improved students from DUT and LJMU in terms of cybersecurity awareness and AI. We adopted a cross-sectional survey design, with data collected using online questionnaires. Census sampling identified programme participants from DUT and LJMU, registered at the respective universities in 2024. Data were analysed statistically using descriptive statistics, Chi-square test of independence, One sample t-test and independent samples t-test. Results indicated that students reported cyber security as a high priority. This study confirms that students who are aware of cyber bullying have a greater ability to ensure their cyber security. An interesting finding was the difference between DUT and LJMU students on collaboration skills.

There is agreement that COIL improved digital security, cyber security awareness and knowledge amongst both DUT and LJMU students. Significantly, more DUT students found the COIL project helpful to improve their collaboration skills. This is in line with the study by Wimpenny et al. (2022), in that "COIL can have a positive transformational effect on the learner". By extending Wimpenny et al's COIL conceptual framework to teaching cybersecurity awareness, we see the importance of *glocalising* the learning environment online in the context of DUT students' heightened concerns over cyberbullying and cybersecurity due to the lower position of South Africa in protecting its netizens from cybersecurity threats. Further, many students on the project would recommend this pedagogy to be offered. We acknowledge that the sample size is small, the study was focused on the students on this specific COIL project and so the results cannot be generalised. Future research would benefit from a larger sample of students and given the students' appetite, for more learning of AI and cybersecurity.

Our study is original and has policy impact on social mobility and educational policies of the UK. We are providing evidenced research to the ongoing dialogue in South Africa regarding student mobility and a stronger emphasis on short-term virtual mobility exchanges. Educators should consider adopting COIL as a pedagogical tool to educate students on cybersecurity and AI. In our project, many students felt that COIL has improved a range of soft skills and the knowledge on cybersecurity and AI. We also provide policy recommendation to both the UK and South African governments on cybersecurity strategy. Individuals' knowledge, understanding and perception of cybersecurity threats depend on other factors such as the role of media and social media. We propose a more inclusive approach of understanding citizens' cybersecurity concerns, which would lead to a more informed and enriched cyber defence strategy.

Acknowledgements The authors would like to thank Ms SL Naidoo, Durban University of Technology, Faculty of Management Sciences, for her contributions towards the preparation of this article.

Funding The authors received funding for this project from the Association of Commonwealth Universities.

Data availability The authors have no financial or proprietary interests in any material discussed in this article.

Declarations

Ethical approval All authors certify that they have no affiliations with or involvement in any organisation or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

Competing interest The authors have no competing interests to declare that are relevant to the content of this article.

Disclosure The authors have no relevant financial or non-financial interests to disclose.

References

AAG IT Services. (2024). The latest 2024 cyber crime statistics (updated May 2024). With an average of 97 leaked every second in 2022. https://aag-it.com/the-latest-cybercrime-statistics/#:~:text=. Accessed 22 Oct 2024.

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Action Fraud (2024). *Fraud and cyber crime national statistics*. https://www.actionfraud.police.uk/data. Accessed 5 Dec 2024.

Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer Security and Ethics awareness among IIUM Students: An Empirical Study. In *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010* (pp. A52-A56). IEEE. https://doi.org/10.1109/ICT4M.2010.5971884

Anstey, G. (2023a). Academic mobility is about a lot more than students travelling between countries. Universities South Africa. https://usaf.ac.za/academicmobility-is-about-a-lot-more-than-students-travelling-between-countries/. Accessed 22 Oct 2024.

Anstey, G. (2023b). Student mobility was a hot topic at USAf's Research and Innovation Dialogue. Universities South Africa. https://usaf.ac.za/student-mobility-was-a-hot-topic-at-usafs-research-and-innovation-dialogue/

Awan, H. (2024). Top 5 most hacked phone brands - what you need to know. https://www.efani.com/blog/most-hacked-phone-brands-to-ditch. Accessed 5 Dec 2024.

Barlow, E. (2023). *What makes south africa a target for cyber crime, and what actions can be taken?* https://www.securityhq.com/blog/what-makes-south-africa-a-target-for-cyber-crime-and-what-actions-can-be-taken/. Accessed 9 Sept 2023.

Bhabha, H. (1994). The Location of Culture. Routledge. https://doi.org/10.4324/9780203820551

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication (AJIC)*, 20, 133–155. https://doi.org/10.23962/10539/23572

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security*, 142, 103858, https://doi.org/10.1016/j.cose.2024.103858

Chetty, R. C. (2022). *SA ranked sixth in the world as country most impacted by cybercrimes*. https://www.thesouthafrican.com/news/south-africa-top-ten-countries-impacted-most-cybercrimes-world-cyber security-surfshark/. Accessed 5 Oct 2023.

Chigada, J. (2023). *Towards an aligned South African national cybersecurity policy framework*. https://hdl.handle.net/11427/38253. Accessed 5 Dec 2024.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63–72. https://doi.org/10.1016/j.cose.2006.10.005

Dipa, K. (2023). The World's online privacy and cybersecurity awareness is declining. https://www.iol.co.za/saturday-star/news/study-the-worlds-online-privacy-and-cybersecurity-awareness-is-declining-e9db66b4-1789-43c6-b749-abe8936aba04. Accessed 8 Oct 2023.

Eoyang, M., Peters, A., Mehta, I., & B, G. (2018). *Third way to catch a hacker: toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors*. https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors?stream=technology. Accessed 22 Oct 2024.

Fishbein, M., & Ajzen, I. (2011). Predicting and changing behaviour: The reasoned action approach. New York: Psychology Press. https://doi.org/10.4324/9780203838020

Fung, C., Khera, V., & Boonbrahm, P. (2008). Raising information security awareness in digital ecosystem with games – a pilot study in Thailand. *2nd IEEE International Conference on Digital Ecosystems and Technologies*, 375–380. https://doi.org/10.1109/DEST.2008.4635145

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyberattacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine, 30*(1), 28–38.

Garba, A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. *Science Proceedings Series*, 2(1), 82–86. https://doi.org/10.31580/sps.v2i1.1320

Gondwe, M. (2022). The public sector needs to do more against cybercrime. *Business Day.* https://www.businesslive.co.za/bd/opinion/2022-10-24-moss-gondwe-the-public-sector-needs-to-do-more-against-cybercrime/. *Accessed 9 Sept 2023.*

Greig, J. (2023). State-owned bank in South Africa confirms Akira ransomware attack. *The Record*. https://therecord.media/development-bank-of-southern-africa-akira-ransomware-attack. Accessed 9 Sept 2023.

Huraj, L., Lengyelfalusy, T., Hurajová, A., & Lajčin, D. (2023). Measuring cyber security awareness: A comparison between computer science and media science students. *TEM Journal, 12*(2), a623–633. https://www.temjournal.com/content/122/TEMJournalMay2023_623_633.pdf. Accessed 9 Sept 2024.

INTERPOL. (2021). Innovation to beat cybercrime acceleration the theme of 2021 Europol-INTERPOL cybercrime conference. https://www.interpol.int/en/News-and-Events/News/2021/Innovation-to-beat-cybercrime-acceleration-the-theme-of-2021-Europol-INTERPOL-Cybercrime-Conference. Accessed 5 Dec 2024.

INTERPOL (2023). *African cyberthreat assessment report cyberthreat trends*. African Cybercrime Operations Desk. https://www.interpol.int/content/downloa/19174/file/2023_03%20CYBER_African%20Cyberthreat%20Assessment%20Report%202022_EN.pdf. Accessed 8 Oct 2023.

Kavanagh, S. (2021). Contribution to the elaboration of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf. Accessed 8 Oct 2023.

Kolouch, J., Tovarňák, D., Plesník, T., & Javorník, M. (2023). Cybersecurity: Notorious, but often misused and confused terms. *Masaryk University Journal of Law and Technology, 17*(2), 281–305.

Le Grange, L. (2016). What is (post)qualitative research? *South African Journal of Higher Education*, *32*(5), 1–14. https://doi.org/10.20853/32-5-3161

Lepan, C. (2017). *Analysis of a South African cyber-security awareness campaign for schools using interdisciplinary communications frameworks*. Master's Dissertation. Nelson Mandela Metropolitan University. Gqebera. https://core.ac.uk/download/pdf/159469489.pdf. Accessed 8 Oct 2023.

Lewis, T., & O'Dowd, R. (2016). *Online intercultural exchange: Policy, Pedagogy and Practice*. Routledge.

Lorde, A. (2012). Imperialism, history, writing and theory. *Research and indigenous peoples* (pp. 9–14). Zed Books.

Manwaring, R. & Holloway, J. (2023). Resilience to cyber-enabled foreign interference: Citizen understanding and threat perceptions. *Defence Studies, 23*(2). https://doi.org/10.1080/14702436.2022.2138349.

McKinsey Report (2022). Technology trends outlook . https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20top%20trends%20in%20tech%202022/mckinsey-tech-trends-outlook-2022-full-report.pdf. Accessed 11 Oct 2023.

Modise, E. (2023a). South Africa is the cybercrime hub of Africa, according to INTERPOL. *TechCabal*. https://techcabal.com/2023/04/19/south-africa-interpol-cybercrime/. Accessed 9 Sept 2023.

Modise, E. (2023b). Remote working responsible for surge in cybersecurity threats in Africa, according to INTERPOL. *TechCabal*. https://techcabal.com/2023/07/04/remote-working-cybersecurity-africa/. Accessed 9 Sept 2023.

Mohammed, A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*. 2022.12. 2589. https://doi.org/10.3390/app12052589

Moje, E., Ciechanowski, K., Kramer, K., Carrillo, R., & Collazo, T. (2004). Working toward third space in content area literacy: An examination of everyday funds of knowledge and discourse. *Reading Research Quarterly*, *39*(1), 38–70. https://doi.org/10.1598/RRQ.39.1.4

Montgomery, C. (2019). Surfacing southern perspectives on student engagement with internationalization: doctoral theses as alternative forms of knowledge. *Journal of Studies in International Education*, *23*(1), 123–138. https://doi.org/10.1177/1028315318803743

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business and Social Science, 11*(4), 384–396. https://doi.org/10.20525/ijrbs.v11i4.1714

National Federation of Intelligence Bureau (2024). NFIB fraud and cyber crime dashboard – 13 months of data. https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46. Accessed 22 Oct 2024.

Odacı, H., & Çelik, Ç. B. (2017). Internet dependence in an Undergraduate Population: The roles of coping with stress, self-efficacy beliefs, and sex role orientation. *Journal of Educational Computing Research, 55*(3), 395–409. https://doi.org/10.1177/0735633116668644

Panchia, Y. (2023). Spiralling out of control: Recent stats reveal South Africa's crime conundrum. *Forbes*. https://www.forbesafrica.com/current-affairs/2023/06/02/spiraling-out-of-control-recent-stats-reveal-south-africas-crime-conundrum/. Accessed 9 Sept 2023.

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication (AJIC)*, 28, 1–21. https://doi.org/10.23962/10539/32213

Polit, D. F., & Beck, C. T. (2012). *Nursing Research Generating and Assessing Evidence for Nursing Practice* (9th ed.). Wolters Kluwer Health I Lippincott Williams & Wilkins.

Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security. *International Journal of Applied Engineering Research, 9*(23), 19133–19144. https://ssrn.com/abstract=2543737. Accessed 8 Oct 2023.

Prümmer, J., van Steen, T., & Bibi van den Berg (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136.* https://doi.org/10.1016/j.cose.2023.103585. Accessed 22 Oct 2024.

Redmiles, E. M., Malone, A. R., & Mazurek, M. (2016). L. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 272–288). IEEE. https://doi.org/10.1109/SP.2016.24

Reeves, A., Calic, D., & Delfabbro, P. (2021). Get a red-hot poker and open up my eyes, it's so boring 1: Employee perceptions of cybersecurity training. *Computers & security, 106,* 102281. https://doi.org/10.1016/j.cose.2021.102281

South Africa, State Security Agency. (2015). *The national cybersecurity policy framework (NCPF)*. https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf. Accessed 5 Dec 2024.

Surfshark (2022). *Cybercrime statistics*. https://surfshark.com/research/data-breach-impact/statistics. Accessed 22 Oct 2024.

Tabansky, L. (2013). Critical infrastructure protection policy: The Israeli experience. *Journal of Information Warfare, 12*(2), 78–86.

Taherdoost, H. (2024). Towards an innovative model for cybersecurity awareness training. *Information, 15*(9), 512. https://doi.org/10.3390/info15090512. Accessed 5 Dec 2024.

Thompson, J. D., Herman, G. L., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., Phatak, D., & Patsourakos, K. (2018). Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice, 2018*(1), 5. https://doi.org/10.62915/2472-2707.1030, https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/5. Accessed 28 May 2024.

Universities, U. K. (2022). *Widening participation in UK outward student mobility a picture of participation*. https://www.universitiesuk.ac.uk/sites/default/files/uploads/UUKireports/widening-participation-in-uk-outward-student-mobility.pdf. Accessed 5 Dec 2024.

Valentine, J. (2006). Enhancing the employee security awareness model. *Computer Fraud and Security*, *6*, 17–19. https://doi.org/10.1016/S1361-3723(06)70370-0

van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa019

Wimpenny, K., & Orsini-Jones, M. (2020). Innovation in collaborative online international learning: A holistic blend. *Radical Solutions and eLearning: Practical innovations and online Educational Technology* (pp. 1–25). Springer.

Wimpenny, K., Finardi, K. R., Orsini-Jones, M., & Jacobs, L. (2022). Knowing, being, relating and expressing through Third Space Global South-North COIL: Digital Inclusion and Equity in International Higher Education. *Journal of Studies in International Education*, *26*(2), 279–296. https://doi.org/10.1177/10283153221094085

Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: scenarios, functions, tools and architecture. *Computers & Security, 88*. https://www.sciencedirect.com/science/article/pii/S0167404819301804. Accessed 8 Oct 2023.

Zandt, F. (2023). *The most prevalent forms of cyber crime*. https://www.statista.com/chart/30870/share-of-worldwide-cyber-attacks-by-type/. Accessed 22 Oct 2024.

Zhou, V., & Pilcher, N. (2018). Tapping the thirdness in the intercultural space of dialogue. *Language and Intercultural Communication*, *19*(1), 23–37. https://doi.org/10.1080/14708477.2018.1545025

Zorlu, E. (2023). An examination of the relationship between College Students' cyberbullying awareness and ability to ensure their personal cybersecurity. *Journal of Learning and Teaching in Digital Age, 8*(1), 55–70. https://dergipark.org.tr/en/pub/joltida/issue/75090

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behaviour: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Authors and Affiliations

Alison Lui[1] · Catharina Womack[2] · Penny Orton[2]

✉ Alison Lui
A.Lui@ljmu.ac.uk

Catharina Womack
catharinaw@dut.ac.za

Penny Orton
pennyo@dut.ac.za

[1] School of Law, Liverpool John Moores University, Redmonds Building, Brownlow Hill, Liverpool L3 5UG, UK

[2] Faculty of Management Sciences, Durban University of Technology, 41-43 ML Sultan Road, Durban, South Africa