Teaching Pentesting to Social Sciences Students Using Experiential Learning Techniques to Improve Attitudes towards Possible Cybersecurity Careers

Aleksandras Melnikovas[1], Ricardo G. Lugo[2,6], Kaie Maennel[3,5], Agnė Brilingaitė[4], Stefan Sütterlin[2,7] and Aušrius Juozapavičius[1]

[1] General Jonas Žemaitis Military Academy of Lithuania, Lithuania
[2] Faculty of Health, Welfare and Organisation, Østfold University College, Norway
[3] School of Information Technology, Tallinn University of Technology, Tallinn, Estonia
[4] Institute of Computer Science, Vilnius University, Vilnius, Lithuania
[5] School of Computer and Mathematical Sciences, The University of Adelaide, Adelaide, Australia
[6] Department of Information Security and Communication Technology, Norwegian University of Science and Technology,
[7] Faculty of Computer Science, Albstadt-Sigmaringen University, Sigmaringen, Germany

aleksandras.melnikovas@lka.lt
ricardo.g.lugo@hiof.no
kaie.maennel@taltech.ee
agne.brilingaite@mif.vu.lt
stefan.suetterlin@hs-albsig.de
ausrius.juozapavicius@lka.lt

Abstract: Labor market analysis shows that there is a significant shortage of experienced cybersecurity professionals, and this trend is expected to continue in the future. In addition, young people who are reluctant to choose STEM subjects in school typically do not see cybersecurity as a part of their future because they believe it demands exclusive technical knowledge that is beyond their reach. We aimed to change this perception among students of the social sciences, assuming that by providing social science students with the basics of cybersecurity, it would be possible to raise their awareness and encourage them to consider this field as a potential career option. Our team has designed a concise technical course based on Kolb's model that employs experiential learning to provide students with a basic knowledge of ethical intrusion (penetration testing). During the 32-hour subject, cadet officers with no prior IT education experienced all the steps of hacking both into a remotely accessible and physically accessible computer, including initial reconnaissance, vulnerability scanning, exploitation, and privilege escalation. A hands-on practical task of breaking into a highly vulnerable remote computer allowed for the evaluation of knowledge and skills as well as the reinforcement of learning experiences. In order to assess how the students' perceptions of the cybersecurity profession have changed based on the theory of planned behavior, they were asked to provide feedback immediately after the course and one year later. The results indicate that the short, technically challenging, but practical course based on experiential learning had a significant and positive effect on participants' attitudes: they were substantially more likely to consider cybersecurity as a future career, and some of them began participating in other cybersecurity courses or activities. It is reasonable to assume, therefore, that providing similar technical courses to social science students will encourage them to pursue cybersecurity-related careers in the future.

Keywords: military education, pentesting, Kolb's experiential learning cycle, cybersecurity, student attitude

1. Introduction

The number of cyber attacks is constantly rising and digitalization increases the attack surface constantly, giving. Due to the growing frequency and sophistication of cybersecurity threats, there is a shortage of professionals who would be capable of dealing with such threats. Scholarly literature clearly indicates that the demand for cybersecurity professionals is constantly increasing (Mogoane and Kabanda 2019; Helser 2019; Sohime et al. 2020). On a global level - currently more than 3,4 million cybersecurity related positions are unfulfilled worldwide and despite growing numbers of professionals, the gap has doubled within the past few years and is likely to maintain the same dynamics in the future ((ISC)2, 2022).

One of the main reasons for the shortage of cybersecurity specialists is that the field is constantly evolving, making it difficult for professionals to stay up-to-date with the latest threats and technologies. Additionally, the

rapid growth in technology and the increasing number of connected devices has led to a growing number of potential targets for cyber attacks, which further exacerbates the need for cybersecurity professionals. Another reason for the shortage of cybersecurity specialists is that the field is not well understood by many people. This can make it difficult to attract and retain talented individuals. The studies show that a lack of computer skills has a negative effect on students' self-efficacy in cybersecurity, and perceived barriers significantly decrease students' intentions to pursue a career in cybersecurity (Chai and Kim, 2012). Thus, non-IT students may not be aware of the opportunities available to them or may not have the necessary qualifications, which supports their attitude that a career in cybersecurity would demand exclusive technical knowledge that is beyond their reach.

Another essential aspect of cybersecurity is its connection to national security and defense. The military has increased its focus on cybersecurity - since 2010 cyberspace was proclaimed a military domain of equal importance as land, sea, air, and space (Vogel, 2016). The security sector and the public sector are both affected by the current lack of cybersecurity professionals, however, the military's lack of cybersecurity personnel can have a number of severe repercussions. For instance, the military may find it difficult to adequately defend against emerging cyber threats and create new cybersecurity technology if it does not have access to sufficient numbers of cybersecurity personnel. If this happens, important military data and operations may be compromised, and the military's capacity to function in the digital sphere may be hampered. The military's vital power, communication, transportation, and financial systems may potentially be at risk. As a result, the military could lose ground in a cyberwar, both tactically and strategically. To address these concerns, the paper introduces an approach to attracting non-IT students to the domain of cybersecurity through engaging in educational activities and experiential learning. We aimed to change the perception among officer cadets - who are also students of the social sciences (political and organizational sciences), assuming that by providing future officers with the basics of cybersecurity, it would be possible to raise their awareness and encourage them to consider this field as a potential career option.

We illustrate the application of Kolb's experiential learning methodology (Kolb and Kolb, 2017) to construction of a pentesting course for officer cadets with no prior IT experience. With this research, we address the question of what effect a short, technically challenging, but practical course based on experiential learning has on participants' attitudes towards cybersecurity in general and cybersecurity as a future career path in particular.

2. Literature review

Cybersecurity, including pentesting, is a complex subject matter, thus, the learners' motivation is very important to ensure success in cybersecurity learning, especially as learners may experience some difficulties to grasp the intricate concepts of cybersecurity (Kam et al., 2020). Game-based strategies are considered effective in increasing students' cybersecurity awareness and their decision to become cybersecurity professionals (Triplett, 2023). Specifically for the new talent attraction, cyber competitions or exercises (such as Capture the Flags (CTFs)) organized by universities or non-profit organizations are considered as effective ways. While the competitions positively influence future career intents, they are designed for targeting high schoolers and those undecided undergraduate and graduate students (Bashir et al., 2015). Recently, both high school and college level students have become increasingly interested in studying cybersecurity; therefore, educational institutions also design introductory courses and seminars to expand the students' knowledge of cybersecurity (Triplett, 2023). However, graduates, non-cybersecurity majors, or those already established in the career path with certain intentions, attracting them to competitions or traditional cybersecurity awareness courses may not work, and alternatives should be considered. The scholarly literature indicates that similar tendencies exist in the military sphere. Within the military domain, it is acknowledged that providing qualified cybersecurity personnel should be addressed in workforce strategy (Karamen et al., 2016). For example, the U.S. Army continues to develop personnel management initiatives that align with the Army People Strategy so that talented recruits can pursue and grow in an Army career, especially in cybersecurity areas (Bates and Rose, 2022). However, the initiatives are mostly aimed at persons who already have a positive predisposition towards IT subjects, while we investigate the behavior of students who had chosen a non-IT path for their careers.

Previous research indicates that educational models based on Kolb's experiential learning could be considered a rather effective alternative to the traditional methodology applied in cybersecurity education. Applied to the cybersecurity domain, experiential learning facilitates reaching higher learning outcomes, raising motivation to choose cybersecurity as a career path (Abdulwahed and Nagy, 2009), building self-efficacy (Towhidi and Pridmore, 2022) and providing an interesting and engaging learning experience (Konak, 2018). The hands-on and experiential learning is also emphasized in learning design for attracting non-IT talent. Giboney et al. (2019) use experiential learning principles (using playable case studies) and propose the Theory of Experiential Career

Exploration Technology, emphasizing the need to explicitly design technologies to support career pursuit decisions, understanding of career skills, and confidence in career skills. Our research uses a similar experiential learning approach, however, the authors use existing and open-source software to make it less costly and efficient to deploy.

Flow and task significance have powerful effects on motivation, which promotes learning persistence and performance (Kam et al., 2020). Therefore, in order to motivate and engage the various talent groups in cybersecurity learning, it is essential to employ the most effective and appropriate methods. Kam et al. (2018 and 2020) build upon Flow Theory and Self-Determination Theory, proposing a framework to attract individuals to cybersecurity and showing that perceived flow, relatedness, and learning autonomy, not the necessity to develop skill proficiency, drive self-determined motivation in cybersecurity learning (Kam et al., 2018). The authors suggest that this is because the participants had little knowledge of cybersecurity and therefore did not perceive high competency (Kam et al., 2018). This is very relevant for our research, as the non-IT personnel have low cybersecurity subject matter knowledge, and therefore, motivation is a key success factor and needs to be supported in the learning design. Our main intention was to convince the participants that even complicated tasks in cybersecurity are within their reach, and therefore we constructed sufficiently advanced scenarios that resemble real-life situations.

3. Methodology

A synthesized research approach informed by design research was used to develop the research methodology. Design research as a methodology allows for the collection of information on the learning preferences and needs of students, which can then be used to create engaging and empowering curricula and lessons. In this research, the goal of applying design research is to improve learning outcomes, explore new teaching methods and technologies by constructing a curriculum based on experiential learning, and determine the effectiveness of such curriculum in supporting students' positive attitudes towards career options in cybersecurity or related domains. Methodological procedures were adapted from Cole et al., (2005) and included four phases: *problem identification, intervention, evaluation, reflection and learning*.

3.1 Problem identification

As described above, we identified the problem as a lack of cybersecurity professionals in the military and civil domains. This research aims to introduce a penetration testing course for military cadets to increase their interest in a cybersecurity career.

Penetration testing identifies and assesses vulnerabilities that adversaries could exploit (NIST, 2020). Penetration testers are also called ethical hackers (ENISA, 2022), but their actions still might expose sensitive data or disturb systems. Therefore, these specialists should follow the rules of engagement, uncover vulnerabilities, perform security assessments, and prepare reports based on standard procedures. Thus, the penetration testing process requires high-level competences related to component integration, testing, and risk management, including offensive and defensive security procedures, testing tools, operating systems security, and computer network security (ENISA, 2022).

Existing research has presented a successfully executed semester-length penetration testing course for Bachelor students in Computing and shared experience on practice-oriented technical modules (Sufatrio, Vykopal and Chang, 2022; Wang, McCoey and Hu, 2020). According to world-known cybersecurity curricula (ACM et al., 2017), cybersecurity mainly relies on hard IT skills but also includes the knowledge area Societal Security focusing on various factors that impact society, such as cybercrime and ethical hacking. The latter topic integrates hacking principles, conditions, and differences in hacking types (ACM et al., 2017). Moreover, practical training positively impacts highly motivated students, increase their interest in the field, and encourages them to consider cybersecurity master's studies (Demetrio et al., 2019).

The national interests of smaller countries need broad-profile specialists instead of a workforce with dedicated cybersecurity specialist roles (Bukauskas et al., 2023). Thus, non-technical personnel can perform cybersecurity tasks, possessing knowledge in many related areas. As a practical approach in penetration testing training provides a broad overview of adversary actions and security perimeter factors, therefore, we chose this cybersecurity field to integrate into the social sciences cadet studies.

3.2 Intervention

As a means of intervention, we designed and delivered a concise, technically challenging, and practical course based on Kolb's experiential learning cycle (see below) to attract non-IT students to the domain of cybersecurity. By this intervention, we assume that by providing future officers with the basics of cybersecurity, it would be possible to raise their awareness and encourage them to consider this field a potential career option.

The course was designed utilizing an experiential learning paradigm. This paradigm is frequently applied in military training modules at the Lithuanian Military Academy, such as Leadership education and training, Education methodology course, Tactics, etc. Following this paradigm, the Cybersecurity module was designed using Kolb's learning cycle and the "teaching around the learning cycle" approach, which consists of four sequential stages: concrete experience, reflective observation, abstract conceptualization, and active experimentation (Kolb and Kolb, 2017). The architecture of the module allowed students to be guided sequentially through the experience of penetration testing in order to build cyber hygiene skills and raise cyber awareness. Students were directed through four stages of the learning cycle (see Figure 1). During each cycle, a new penetration testing method or tool was briefly demonstrated, and the students had to repeat the demonstration (usually in pairs), then read some extra material (tutorials) on their own or listen to a lecturer, discuss their findings and possible defense strategies among themselves, and then apply their newly acquired knowledge in a slightly different system (in groups of one to four students).

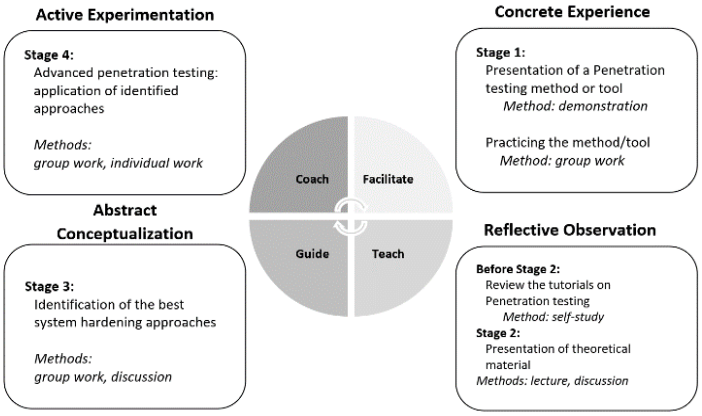

Figure 1: The stages of the Kolb's learning cycle adopted to the course

The course lasted for 2 weeks, with 2-4 contact hours per day (32 contact hours in total). It required extensive preparation of software and guidance for non-technical students. It started with hacking physically accessible computers. Each student had to obtain an Administrator's account and set up the machine for further lectures by installing virtualization software and downloading prepared images of virtual machines. The course covered the Linux command line, SSH protocol, basic network and vulnerability discovery tools, such as nmap and netcat, and hashed-password recovery tools and methods, e.g., brute-force and dictionary attacks with hashcat. Tools and commands enabled attacks on remote (virtualized) machines and privilege escalation by discovering sensitive information and service misconfigurations. Additionally, live social engineering attacks (smishing and phishing) employed selected command and control frameworks to demonstrate possible attacker's actions after taking full control of an infected computer. The CTF-based exam required penetrating a remote virtual machine and finding flags and some hints hidden along the way to the super-user account.

3.3 Evaluation

The results were evaluated measuring students' perceived quality of the course immediately after the delivered educational activities. About one year later, the students were asked to answer an additional questionnaire. The Theory of Planned Behavior (TPB; Figure 2) was applied in order to evaluate the long-term effect of the course on officer cadets' attitudes towards cybersecurity as a future career and participation in cybersecurity courses or activities. The TPB (Ajzen and Fishbein, 1977) incorporates attitudes, normative beliefs (NB) or subjective norms (social acceptance of a specific behavior), and perceived behavioral control (PBC) and these three variables predict behavior intentions (BI; Ajzen and Madden, 1986).

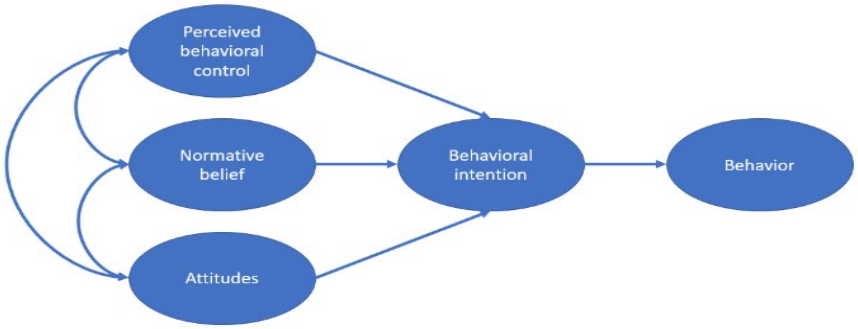

Figure 2: The model of the Theory of Planned Behavior

The TPB has been used in many studies and has been able to account for up to 50% of behavior (Armitage & Connor, 2001). A total of 6 questions (see Table 1) were used to gather quantitative data on the TPB aspects (2 questions for behavior intention, 1 question on attitudes, 1 question on normative beliefs, and 2 questions reflecting PBC). All questions had a scale of 1 to 7. One question asked participants about their current actions regarding the cybersecurity career path (if they had one).

Table 1: Questions of the delayed evaluation (approx. one year after the course)

	Where would you put yourself on a scale 1 (low) to 7 (high):		
Category of TPB	Question number		Scale
Perceived behavioral control	1	I have skills in cybersecurity:	
	pre	before the course (so a long time ago):	1-7
	post	today:	1-7
Attitude	2.	I think (today) that cybersecurity work positions are attractive.	1-7
Normative belief	3.	My friends/colleagues find cybersecurity an attractive area.	1-7
Behavioral intention	4.	I could consider a job position in cybersecurity if an opportunity came my way:	
	4A.	before the course:	1-7
	4B.	today:	1-7
A change in behavior	5.	Are you actually doing something cybersecurity related already? (Can you give an example?)	open

Phase four of the methodology procedure is *Reflection and learning.* The following section will report the results, provide reflections and lessons learned.

4. Results

We used written student feedback about the experience immediately after the course and applied a delayed evaluation in order to estimate students' perceptions of skills and attitudes towards cybersecurity. 14 students took the course in April 2021, and 17 students in April 2022. All the students were cadets from different military academies in Europe (with almost half of them local) except for one Italian civilian student. 18 of the 31 students gave feedback immediately after the course. Additionally, a delayed evaluation was carried out in December 2022. In total, only 11 of the 31 students replied to the delayed evaluation questions.

Course evaluation showed a significant difference (M_{diff}=.6, t=2.74, df=17, p=.014, d=.65) to the average score of all academy courses. On average, they gave 8.5 points on a scale of 10. In comparison, the average score of all courses given in the Academy during the year was 7.9.

However, not every student was happy about the substantial amount of new technical material they had to learn. The feedback revealed two groups of students: one group suggested having more theoretical lectures, while the other group praised the practical aspect of the course and the ability to work in groups. The former group also expressed concerns about the latter group having better basic knowledge, although no such differences existed. In retrospect, it is quite unrealistic to supply enough basic IT knowledge during such a short course, and the aim was not to create experts in penetration testing, but to prove to students that with effort this area is within their reach. Those who did not get discouraged during the first lectures continued to work hard and eventually succeeded in every task. The feedback was anonymous, and we cannot prove that those who believed in their abilities coincided with the group satisfied with the course, but perseverance and belief played an important role. In fact, the final task (the exam) was not limited in time, and those who spent the most time appeared most satisfied with themselves. They were also the ones who responded to the delayed evaluation questionnaire.

Descriptive statistics and correlations of behavioral factors (TPB) can be found in Table 2 and Figure 3. Items for the TPB were not normally distributed; therefore, non-parametric analyses were conducted.

Table 2: Descriptives and correlations (ρ) of behavioral factors (TPB)

	Mean	SD	1	2	3	4	5	6
1. PBC pre	1.636	0.809	—					
2. PBC post	3.818	0.874	.262	—				
3. Attitude	6.182	0.874	.016	.704*	—			
4. NB	4.273	1.679	-.241	.112	.289	—		
5. BI pre	1.818	1.25	.269	-0.11	-.327	.442	—	
6. BI post	5.409	1.2	.190	-.336	-.040	.170	.194	—

* p<.05, ** p<.01, *** p<.001

PBC: Perceived behavioral control; NB: Normative beliefs; BI: Behavioral intention

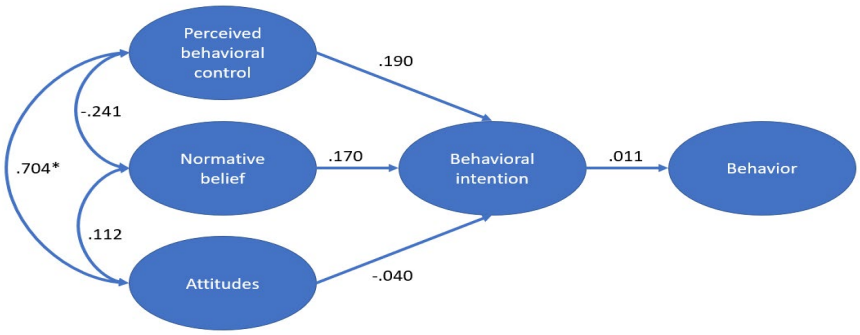

Figure 3: The model of the Theory of Planned Behavior with correlations of behavioral factors.

Wilcoxon paired sample t-tests were used to see if the course led to a significant increase in TPB behaviors (PBC & BI). Both PBC (z=2.93, p=.004, *RBC*=.328) and behavioral intentions (with identical parameters: z=2.93, p=.004, *RBC*=.328) had significant increases in reported behaviors (see Fig. 4 & 5). The students reported that their almost non-existing knowledge in cybersecurity (PBC pre: 1.6 on a scale 1 to 7) increased substantially (PBC post: 3.8). The change of their intention to enter the cybersecurity field was even larger: the average BI score went from 1.8 to 5.4 (on a scale of 1 to 7).

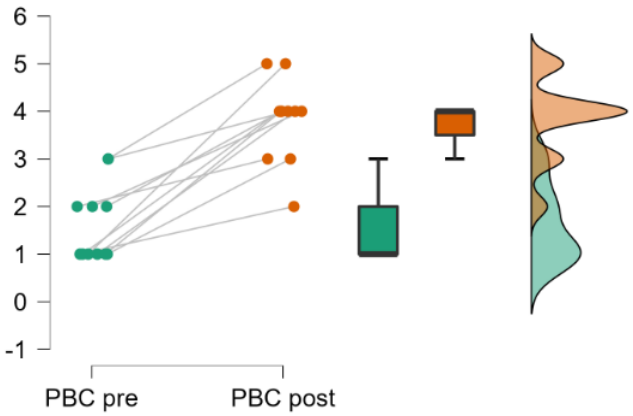

Figure 4: Change in perceived behavioral control (PBC)

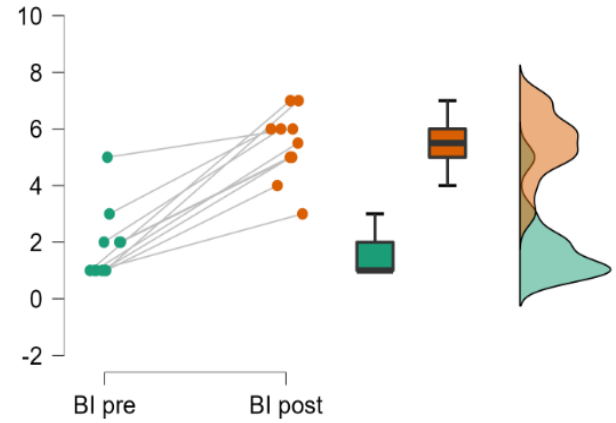

Figure 5: Change in behavioral intention (BI)

To test whether the behavioral factors (PBC, A, NB) could predict behavioral intention (BI), difference scores were calculated for perceived behavioral control and for the behavioral intention due to the participants assessing their PBC scores and assessing a career in CS before and after they had taken the course. Then, a stepwise regression analysis was performed to isolate the factors of the TPB that could predict a positive change in career intention. None of the TPB factors (PBC, NB, A) could predict behavioral intentions (R^2=.190, F=.547, p=.666).

Even though the TPB factors could not predict behavioral intentions of seeking CS careers, participants (6 responses; 43%) stated that they already were currently employed in CS or continuing CS education ("about to start MSc studies in cybersecurity", "got a position of a reconnaissance officer", "taking more courses in cybersecurity" and similar). Therefore, the course worked as a successful stepping stone towards a cybersecurity career for at least 19% (6 out of 31) of course participants. In our opinion, it is a substantial result, especially when considering the fact that cadets have rather limited control over their careers at this stage of their studies. Consequently, courses of similar design in other universities could be used as a tool to attract social science students to cybersecurity.

The pentesting course did significantly change perceptions of skill sets (PBC) and did predict a significant change in intentions in pursuing a career. Consequently, many participants did report that they went from 'not a career' in cybersecurity to having specific CS jobs or continuing their education in cybersecurity.

There are several factors that may explain the non-findings in the behavioral measures of the TPB. There was a limited number of participants, and not all participants completed the follow-up questions, so reported associations could reflect this.

5. Conclusions and Future Work

This study shows how the application of educational theories of motivation and learning can be implemented and possibly influence participants' decisions towards a line of work that is new and unfamiliar for many and generally considered to be demanding to learn. We showed that using Kolb's experiential learning approach to attract non-IT personnel to cybersecurity has a potential benefit for increasing interest in cybersecurity in populations that were previously not in touch with this field. The intentions and perceived skills of participants undergoing the introductory pentesting course significantly changed, indicating an effective intervention. The interindividual differences point at the possibility that the traits of perseverance and openness to experience could be relevant predictors. Numerous students reported actual activities in cybersecurity one year later. In combination with the lack of findings regarding attitude change, it is possible that the follow-up assessment one year after the course was too late to assess the details of the development of interest that potentially led to those decisions.

To the best of our knowledge, this study is the first to address social science students and assess long-term effects, and it is also the first to address the overall question of attitude and behavior change for increasing the recruitment of cyber specialists in the military sector. While short-term effects are easy to achieve in interventions based on short-term guided activities inducing positive affect, the sustainability of the achieved effects is much less clear.

It is beyond the scope of the time range of this study to investigate how many participating individuals' career paths are actually affected. However, it has to be considered that cybersecurity professionals do not work in isolation but need to interact with non-technical personnel in interdisciplinary teams or organizational structures requiring communication and problem-solving across disciplinary borders. A better mutual understanding - not in technical details but regarding the general nature of others' tasks - can contribute to lower thresholds for interactions and more efficient problem-solving in the presence of ambiguous threats.

Future research should replicate these findings in a larger sample. It is noteworthy, that the current results did not suffer from self-selection bias, the course content was the same for all. In order to improve the course content further, more insights are needed in regards to prepositions the participants come with - such as attitudes and personality traits such as openness to new experiences or a general IT-affinity.

The fact that nearly half of respondents chose a relevant career path indicates that future research should implement a more fine-grained follow-up assessment applying several shorter time windows. Due to the quasi-experimental design, we can not isolate clear causal relations. Further research potential may be in the investigation of personality traits as predictors of intention and behavior change.

Acknowledgements

The "Advancing Human Performance in Cybersecurity", ADVANCES, benefits from nearly €1 million grant from Iceland, Liechtenstein and Norway through the EEA Grants. The aim of the project is to advance the performance of cybersecurity specialists by personalizing the competence development path and risk assessment. Project contract with the Research Council of Lithuania (LMTLT) No is S-BMT-21-6 (LT08-2-LMT-K-01-051).

References

Abdulwahed, M., and Nagy, Z. K. (2009) "Applying Kolb's experiential learning cycle for laboratory education", *Journal of engineering education*, *98*(3), pp 283-294.

ACM, IEEE, AIS and IFIP. (2017) "*Cybersecurity Curricula 2017. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*", A Report in the Computing Curricula Series, Joint Task Force on Cybersecurity Education. Version 1.0, December.

Ajzen, I. and Madden, T.J. (1986) "Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control", *Journal of experimental social psychology*, *22*(5), pp 453-474.

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British journal of social psychology*, *40*(4), 471-499.

Bashir, M., Lambert, A., Guo, B., Memon, N., and Halevi, T. (2015) "Cybersecurity competitions: The human angle", *IEEE Security & Privacy*, 13(5), pp 74-79.

Bates, C. C., & Rose, M. C. (2022) "Leveraging Talent to Dominate in Cyber War—An Army Perspective", *The Great Power Competition Volume 3: Cyberspace: The Fifth Domain*, pp 319-346.

Bukauskas, L., Brilingaitė, A., Juozapavičius, A., Lepaitė, D., Ikamas, K. and Andrijauskaitė, R. (2023) "Remapping cybersecurity competences in a small nation state", *Heliyon*, e12808.

Chai, S. M., & Kim, M. K. (2012) "A road to retain cybersecurity professionals: An examination of career decisions among cybersecurity scholars", *Journal of the Korea Institute of Information Security & Cryptology*, *22*(2), pp 295-316.

Cole, R., Purao, S., Rossi, M., & Sein, M. (2005) "Being proactive: where action research meets design research", *ICIS 2005 proceedings*, 27.

Demetrio, L., Lagorio, G., Ribaudo, M., Russo, E. and Valenza, A. (2019) "ZenHackAdemy: Ethical Hacking@ DIBRIS" *In CSEDU (1),* pp 405-413.

ENISA. (2022) *European Cybersecurity Skills Framework (ECSF)*. European Union Agency for Cybersecurity. September. pp 27.

Fishbein, M. and Ajzen, I., (1977) "Belief, attitude, intention, and behavior: An introduction to theory and research", *Journal of Business Venturing*, Vol.5, pp 177.

Giboney, J., Hansen, D., Mcdonald, J., Jonathan, B., Tanner, J., Winters, D., and Bonsignore, E. (2019) Theory of Experiential Career Exploration Technology (TECET): Increasing cybersecurity career interest through playable case studies.

Helser, S. G. (2019) "Health services at risk: an unanticipated outcome of the need for cybersecurity", *Issues in Information Systems*, *20*(4).

(ISC)2. (2022) *Cybersecurity Workforce Study 2022. A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution.* Retrieved from: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx. Accessed on 03 Jan 2023.

Kam, H. J., Menard, P., Ormond, D., & Katerattanakul, P. (2018) "Ethical hacking: Addressing the critical shortage of cybersecurity talent", *In PACIS Proceedings*.

Kam, H. J., Menard, P., Ormond, D., & Crossler, R. E. (2020) "Cultivating cybersecurity learning: An integration of self-determination and flow", *Computers & Security*, *96*, 101875.

Karaman, M., Hayrettin, Ã., & Aybar, C. (2016) "Institutional cybersecurity from military perspective", *International Journal of Information Security Science*, *5*(1), pp 1-7.

Kolb, A. Y., and Kolb, D. A. (2017) "Experiential learning theory as a guide for experiential educators in higher education", *Experiential Learning & Teaching in Higher Education*, *1*(1), pp 7-44.

Konak, A. (2018) "Experiential learning builds cybersecurity self-efficacy in K-12 students", *Journal of Cybersecurity Education, Research and Practice*, *2018*(1), 6.

Mogoane, S. N., & Kabanda, S. (2019) "Challenges in Information and Cybersecurity program offering at Higher Education Institutions", In *ICICIS*, pp 202-212.

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations*. Joint Task Force. Special Publication 88-53. Revision 5, September.

Sohime, F. H., Ramli, R., Rahim, F. A., & Bakar, A. A. (2020) "Exploration study of skillsets needed in cybersecurity field", In *2020 8th International Conf. on Information Technology and Multimedia (ICIMU),* pp 68-72. IEEE.

Sufatrio, Vykopal, J. and Chang, E.C. (2022) "Collaborative Paradigm of Teaching Penetration Testing using Real-World University Applications", *In Australasian Computing Education Conference*, pp 114-122.

Towhidi, G., and Pridmore, J. (2022) "Increasing cybersecurity interest and self-efficacy through experiential labs", *Issues in Information Systems*, *23*(2).

Triplett, W. J. (2023) "Addressing Cybersecurity Challenges in Education", *International Journal of STEM Education for Sustainability*, *3*(1), pp 47-67.

Vogel, R. (2016) "Closing the cybersecurity skills gap", *Salus Journal*, *4*(2), pp 32-46.

Wang, Y., McCoey, M. and Hu, Q. (2020) "Developing an undergraduate course curriculum for ethical hacking". In *Proceedings of the 21st Annual Conference on Information Technology Education*, pp 330-335.