# Teaching Cyber-Security for Distance Learners: A Reflective Study

Ali Ahmed
*School of Engineering and Computer Science*
*Victoria University of Wellington*
Wellington, New Zealand
ali.ahmed@vuw.ac.nz

Karsten Lundqvist
*School of Engineering and Computer Science*
*Victoria University of Wellington*
Wellington, New Zealand
Karsten.Lundqvist@vuw.ac.nz

Craig Watterson
*School of Engineering and Computer Science*
*Victoria University of Wellington*
Wellington, New Zealand
Craig.Watterson@vuw.ac.nz

Nilufar Baghaei
*School of Natural & Computational Sciences*
Massey University
Auckland, New Zealand
N.Baghaei@massey.ac.nz

***Abstract*—The number of distance learning degrees has increased dramatically over the last decade. Yet, despite this increase, teaching computer security subjects for online students remains challenging. Online classes often need a special infrastructure such as devices with specific tools, or hardware requirements. It is also a challenge to design a course that is pedagogically sound, engaging and fun for students who may come from a wide spectrum of educational backgrounds. The quality of the education delivered also differs from one institution to another. To provide a sense of accreditation and regulation, the National Cyber-security Centre, which is a part of Government Communications Headquarters (GCHQ) in the United Kingdom (UK) has certified only two online (i.e. distance learning) cyber-security MSc degrees in the country.**

**This paper presents an innovative way of designing capstone projects (i.e. case studies) along with the impact of it on retention, completion, and success rates in a world-class distance learning degree at the University of Liverpool (UoL) over the last ten years. The Chartered Institute for IT (i.e. BSC) is the accreditation body of the degree program studied in this research [1].**

***Index Terms*—Distance Learning, Online Students, pedagogical, Teaching Cyber-security, Capstone Projects, case study-based projects, Student Satisfaction, peer assessment.**

## I. Introduction

With the proliferation of the Internet and the enormously connected devices come security concerns. Security attacks are inevitable and their widespread and severity reveal, with no doubts, the growing need for computer security professionals who can defend against such attacks [1], [2]. A study in 2017 by the Center for Cyber Safety and Education (ISC) suggests the need for about 1.5 million computer security professional to augment the gap in the market [3]. The lack of young people entering the profession is one of the main factors contributing to this shortage [1]. Universities, world-wide, have responded to the lack of computer security professionals and introduced cyber-security majors with many universities in the UK offering such a degree either at the undergraduate or the postgraduate level. However, as highlighted by Hentea and Dhillon (2006), "universities often fail to provide their graduates with skills demanded by employers" [4]. A reason for that is the quality of those degrees/programs, especially those offered in a purely online environment (i.e distance learning) [5]. There are quite few certified undergraduate and postgraduate degrees in cyber-security that are offered to online learners who can not physically attend a university. There are only two online (i.e. distance learning) cyber-security MSc degrees in the UK fully certified by the National Cyber-security Centre, which is a part of Government Communications Headquarters (GCHQ). It is worth noting that distance learning is instrumental in increasing the number of computer security professionals especially from those areas where face-to-face classes are challenging or not possible [6], [7]).

The variety of pedagogical models used in distance learning and the different policies of universities make it hard on students to choose and hard on the research community to compare those degree programs unless the teaching practices at those universities are published. For that reason, this reflective paper describes a world-class distance learning degree taught at the UoL during the last ten years as experienced by the first author as teaching staff. The paper discusses reflections on an innovative way of designing case study projects for online students studying cyber-security courses. The innovative way combines the advantages of peer assessment and capstone projects.

## II. Literature Survey

One of the major challenges in teaching cyber-security courses online is how to evaluate the student's mastery of both concepts and tools used in, for example, protecting digital assets. A small capstone project at the end of the course could be used for such a purpose where students are to work

[1]https://www.bcs.org/ accessed 08.04.2020

on a case study in groups or individually. Capstone projects in cyber-security pave the way to integrate the theories with the practices of cyber-security professionals and are used as a final component in many courses and degree programs. Industrial organisations and employers continue to recommend the utilisation of team-based projects as a means to assure graduate's quality and competitiveness in, for example, the software development industry [8]. Capstone projects enable the students to build a wide range of soft skills such as project management, teamwork, presentation, and communication [9], [10] where project-based learning is instrumental. A capstone project is usually a practical or research activity (i.e. project) that requires the final year students to plan, implement, and evaluate a solution to a specific problem (i.e. this our case a cyber-security problem). In many organisations, small capstone projects are designed per course for those students towards their graduation. Capstone projects have proven to be of good value for online degrees [11]. Online platforms such as Backboard and Moodle offer various tools to address the problem of social and academic isolation experienced by students in traditional one-on-one supervision [12]. In general, project-based learning is effective in distance-learning environments although curriculum might need to be changed to allow longer project's period [13]. Group projects are a fundamental instrument in teaching cyber-security courses and they are quite challenging when it comes to online environments due to many reasons such as dispersed geographical locations of the students [14], cultural perception of collaboration, academic integrity promotion and enforcement, project assessment especially for the required soft-skills, and infrastructure [15]. Not to mention the wide-spectrum of cyber-security projects that could be facilitated such as low-level programming activities, access control policy development, and digital forensics investigation. Group work in online education promotes higher student perceived learning than individual hands-on work [16]

Harnessing the cloud for teaching cyber-security is on the rise. Services such as Amazon Web Services (AWS) are used to facilitate the practical experience for online students [17]. Such services are used to build virtual labs allowing the students to attempt the practical part of cyber-security courses economically. Economically in the sense that an AWS instance could be configured and tested along with all the software tools required then the configuration is easily copied as many instances as the student's number. Cloud-based labs "can satisfy and alleviate most (if not all) of the requirements and problems introduced by classical lab settings" [18]. Most of the work in [15], [19]–[27] address the problem of how to set up virtual cyber-security labs that facilitate the practical cyber-security experiments. The main objectives of such models proposed by these authors are the platform or the tool itself, not how they are used to create cyber-security projects or used hands-on within education institutions. In other words, they focus on the technical design of the virtual laboratory overlooking things such as how to measure the intended learning objectives of a course using capstone projects. Unlike the work mentioned before, [16] puts the proposal of a new virtual computing laboratory in context to foster collaborative information security learning. The work uses a specially-designed virtual computer laboratory to asses its effect on student's learning and attitudes concerning laboratory assignments using group's and individual's work. The work reports on the Usefulness, Interaction, Competency, Interest, Reflection, and Challenge factors from a student perspective, not from a pedagogical perspective. For example, how academic integrity is enforced in such a virtual laboratory is missing. EDURange framework falls under the same research trend (i.e. using the cloud to teach cyber-security) [28]. The interesting aspect of this research is the design of the scenarios (i.e. activities, projects, or assignments) that are used to evaluate the framework. The main design objective here is that those scenarios, as supported by EDURange, are re-configurable; thus they can be deployed in multiple classes reducing the possibility of answers-copying (i.e. plagiarism) or easy to Google as said by the authors. The idea of a re-configurable exercise is interesting although, as highlighted by the authors, many exercises can not be easily modified! Unlike the re-configurable exercises in EDURange, the work in [29] reports on capstone projects for K-12 students including some activities on a vulnerable web server. Such activities are static and solutions for those vulnerable web servers could be easily found online such as that of WebGoat [2].

Case study-based cyber-security teaching is around for quite some time now and has been recommended for both instructors and students for effective teaching and learning [30]. Proposing a case study starts with a case learning objectives set that defines what to expect from the students. Then a case description is provided to the students to give the necessary background as well as the activities that took place in the case study. Finally, the resources needed to work on the case study needs to be provided. Consider an example of a digital forensics investigation case study; the objectives set needs to list what expect from the investigation (i.e. Identification of the pieces of evidence, maintaining a valid chain of custody). The case description provides the background of the case, such as the context in which the case study took place and the suspect's known activities. A disk image that is seized from a suspect's machine could be the resource provided to the students to start the investigation process. Such case studies could be used in capstone projects as well. The main concern in such case studies is the static nature of the study and the ability to simply Google an answer. One of the ideas to overcome those static case studies is to involve industrial partners [14], [31]. Our experience in using industrial partners is diverse. Industry partners' engagement and collaboration are fundamental to the success of those projects/case studies. However, when using industrial partners, it could often come with time constraints due to tight time schedules and proximity to the teaching facilities [32].

Meeting the deadline for summative assignment feedback

[2]https://github.com/WebGoat/WebGoat/wiki/(Almost)-Fully-Documented-Solution-(en) accessed 06.04.2020

is challenging in online education. Many factors contribute to this crucial element of teaching online such as limited time, number of students, number of teaching staff for a module, and the experience of the teaching staff. It is challenging to imagine a group project for a class of 8 groups that is due in three days. For such a reason, peer assessment is used in online education. Peer assessment is considered as a common strategy for evaluating open assignments, increasing learners' engagement with the educational content and/or for breaking the social isolation some learners might feel during their learning journey. Peer assessment refers to the process wherein students evaluate the quality of other students' learning outcomes [33]. A growing body of research underlines the value of peer assessment for the learning process and the benefits it offers [34]. The use of peer assessment strategies can foster community development, give students a chance to learn through critiquing other learners' work [35], improve their motivation and engagement [36], [37], and promote the learning process [38]. It encourages critical thinking [39] and the implementation of higher-order cognitive skills [33], [40]. Acquiring these skills can help improve students' understanding of the scientific topic and provide them with the opportunity to reflect on and improve their work. Despite the great potential that peer assessment can offer learners, there have been some studies showing some concerns around this process as well, if not done correctly. It can be time-consuming, not taken seriously by some students and whether students can evaluate each other work's reliability and assign valid grades [34]. It was found in [41] that peer graders are significantly harsher than instructor graders. The differences between peer and instructor grades can be explained by some students' lack of experience or excessive competitiveness [34], [42]. Most of those concerns can potentially be addressed by online instructors preparing clearly defined and effective grading rubrics for their courses. The rubrics explicit specification of target performance criteria and division of a large task into smaller sub-tasks will provide helpful scaffolding to novice evaluators [34]–[36]. For example, [36] examined the value of using a guided rubric on enhancing students' ability to provide quality feedback and producing more reliable assessments of their fellow students' work in a MOOC writing course. Although results were mixed, on average students who were provided with no rubric guidance in scoring writing samples were less likely to successfully differentiate between novice, intermediate, and advanced writing samples compared with those students who received rubric guidance. Rubric guidance was most beneficial for items "that were subjective, technically complex, and likely to be unfamiliar to the student. Items addressing relatively simple and objective constructs were less likely to be improved by rubric guidance" [36].

Reflective practices in education have been commonplace for some time now and are a significant part of the learning cycle [43]. Reflective analysis as an activity in distance learning has proven to be an effective and important teaching and learning tool (i.e. [44]–[48]). Reflection is a crucial mental activity that enables academics to engage in a meaningful way with the academic practices they employ [49]. The hermeneutic perspective of Van Manen (1977) is followed in this paper to cover technical, and practical reflections [50] to improve the quality of distance learning modules, particularly the cyber-security ones. The reflection methodology applied in this paper utilises four types of data: the students' feedback (i.e. responses to the end of the module satisfaction survey), self-generated feedback from the authors while teaching the cyber-security modules, feedback from course moderators, and feedback from the program director. As highlighted by Karsten et. al (2019), "For [the] formative purpose[s], such as improvement of courses over time, it is generally considered best practice to follow this method [i.e. reflective analysis] instead of using quantitative tools, such as students' questionnaires, which are better at assessing individual teacher performance than improving course quality over time" [31].

## III. Distance Learning Model: Background, Practices and Policies

The distance learning degree program at the UoL started in April 2000 as a partnership with K.I.T. eLearning that is a private entity that specialised in online education. This organisation has since sold the business to Laureate Online Education (LOE) that is a world-class education organisation focusing on online education. The program started back in 2000 without cyber-security degrees that started in 2014 with two degrees (i.e MSc in Computer and Information Security and MSc in Computer Security). In this paper, the focus is on the cyber-security related modules that the first author taught at the UoL/LOE, while other modules are out of scope. The modules discussed in this paper are CKIT-530: Cyber Crime Prevention and Protection, CKIT-511: Security Engineering and Compliance, and CKIT-519: Cyber Forensics.

The first author of this paper joined the program in December 2009 till now. Over the years, the program has evolved a couple of times keeping some of its fundamental foundations such as the week structure and the learning management system (LMS). The LMS used is Blackboard (BB) and each module is structured in 8-10 weeks cycles. For an intake module, it is ten weeks and for a regular module, it is 8 weeks. The different components of our online module are depicted in figure 1 which will be discussed throughout this paper.

It is worth noting that a week cycle starts on Thursday every week and ends on the next Wednesday, where there are mainly 3 assessment items. Firstly, the initial Discussion Question (DQ) answer, which is mainly a discussion question that is released before the beginning of the week where the students have to research a topic and compile an answer. The submission deadline of the initial DQ answer is on Sunday midnight. This simply means the students would have 4 days of studying the topic and going through the provided resources before compiling their initial DQ answers. Secondly, the Follow-ups which are posts students have to send in an online forum discussing ideas raised from the initial DQ answer. The required number of posts is 3 to 5 'substantial' posts in each DQ on at least 3 different days of the week cycle. This

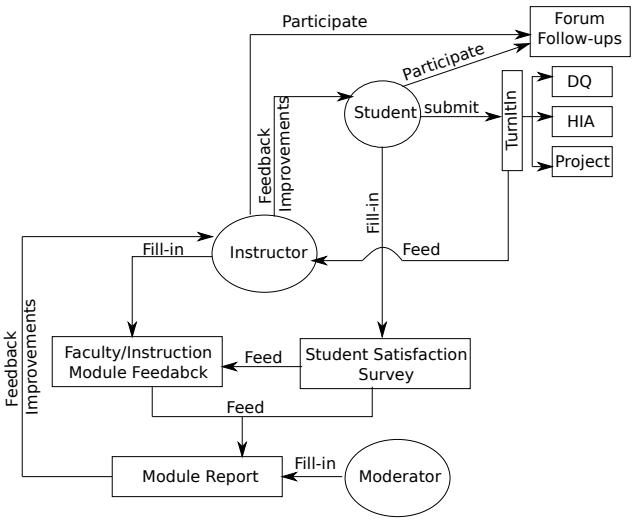


Fig. 1. A module Structure and Feedback Loop

TABLE I
CKIT-530: ASSESSMENT GRID

| **Week** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **Weight** |
|---|---|---|---|---|---|---|---|---|---|
| Initial DQs and Follow-ups | X 5% | X 5% | X 5% | X(2) 10% | X 5% | X(2) 10% | X 10% | X 5% | 50% |
| Individual Assignments | X 5% | X 10% | X 5% | - | - | - | - | X 10% | 30% |
| Group Project | - | - | | $\Rightarrow^*$ | X 10% | $\Rightarrow^*$ | X 10% | | 20% |
| Number of Assessments | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 16 %100 |

$\Rightarrow^*$: starts on the current week and is due the next one.

is the main attendance requirement of the module. Thirdly, the Hand in Assignment (HIA). There is another assessment item which replaces the HIA at the last week (i.e. or weeks) of the module, which is the end of the module project (i.e. sometimes called group project). It is worth noting that for an 8 weeks module, there are at most 18 assessment points that are distributed evenly, based on the complexity, not the number of submissions as one can see in the sample assessment grid for the Cyber Crime Prevention and Protection module in Table I.

Since this is a reflection paper and not a research project, no ethical approval is needed [31]. None of the students' feedback is quoted in this paper; however, as highlighted before, the students' feedback has impacted the authors' reflections. Each instructor is required to respond to a Faculty Feedback request that requires responses to the following academic items such as grades, class performance, and academic integrity incidents. As depicted in figure 1, after the end of the module, a senior faculty member carries out the moderation process which includes assessing the delivery of Learning Objectives, the application of Policies and Procedures, the maintenance of academic standards, Any issues identified in Student Feedback.

## IV. CASE-STUDY-BASED PROJECT: REFLECTIVE ANALYSIS

As discussed before, it is a challenging task to design case-study-based computer security projects for distance learners [51] especially when specific infrastructure is required such as virtual laboratories [2] for CKIT-530 and CKIT-519 which needs to fit certain learning scenarios as discussed by Haag et. al (2019) in [52]. Besides, the ability to evaluate the student's intended learning objectives fairly is overtly important. This encompasses the need for validation that previous students' work has not been leaked to the new cohort. The challenge is in designing case studies where their answers can not be easily shared online. Thus, data-sets such as those developed by NIST CFReDS ProjectNIST2019 do not fit summative assessment models. The solution sheet for an instructor created case study could be easily shared between different cohorts, making it hard to assess the actual students' technical ability. It is important to identify and act upon academic integrity breaches (i.e. identify whether an answer is genuine or copied from an old student's work) [53]. The standard practice in online and face-to-face classes is to use a software system to detect similarity such as TurnItIn or MOSS [54]. Our observation is that TurnItIn is, however, helpless when screenshots are embedded in the answer, and this view is shared by [55]. For example, answers of a digital investigation case study could include quite a few screenshots (i.e. evidence pieces and the used tools).

The teaching staff for Cyber-security related modules have come up with an idea that combines case study-based teaching (i.e. or capstone projects) with the peer assessment methodology to serve the following objectives:

1) Meeting the feedback deadline for all end of the module projects which is three days after the submission of the work.
2) Minimising the possibility of Googling the answers online.
3) Benefiting from the diverse expertise and background of our students to create a rich pool of case studies that are different for each run of the module.
4) Enabling teaching staff with little experience in teaching cyber-security to cover/teach such courses when needed.

The teaching team attempted a new strategy for the end of the module project where the students are placed into arbitrary groups. Each group is required to design a case study along with its solution sheet. The former is shared with the class while the solution sheet is shared with the teaching staff for verification. Then, each group is required to work on another group's case study. For example, the students in CKIT-519 are asked to create a bit-by-bit disk image of a scenario of their choice and to share the disk image with other groups to investigate. In this way, we combine the benefits of case study-based projects and peer-assessment while avoiding the problems of the latter since the teaching staff does the actual assessment with the help of the solution sheets provided by groups.

Our experience with this technique is positive as supported by the Module Report that includes auditing data, faculty feedback, and student satisfaction. About 50% of CKIT-530 module runs shows fewer occurrences of academic integrity incidents compared to previously taught classes. The same percentage was reported for CKIT-519. It is worth noting that, theoretically, the implementation of the new case study technique is not collusion-free. Two student groups could collude and share the answers for the two case studies they are working on. For example, $Group_A$ designed a case study for $Group_B$ to investigate while investigating (i.e. $Group_A$) $Group_B$'s case study. Both groups could collude and exchange answers to the case studies or solution pointers as, for example, where to find the hidden information in a disk image as part of a digital forensics investigation process. In such a situation, group discussion history can be used to establish whether the answer was incremental or done all at once (i.e. plagiarised).

An interesting observation is that the student's retention and completion rates as seen in Figure 2 are outperforming (i.e. Good/Excellent in terms of our UoL/LOE KPIs) those modules that did not implement the new case study projects. It is worth noting that 'completion' status of a student in a course is when the student did not drop out before the end of Week two of the module. After implementing the innovative method of designing case studies, the overall student's grades saw an increase and the number of failed and marginally failed students decreased (i.e. as seen in Figure 3).

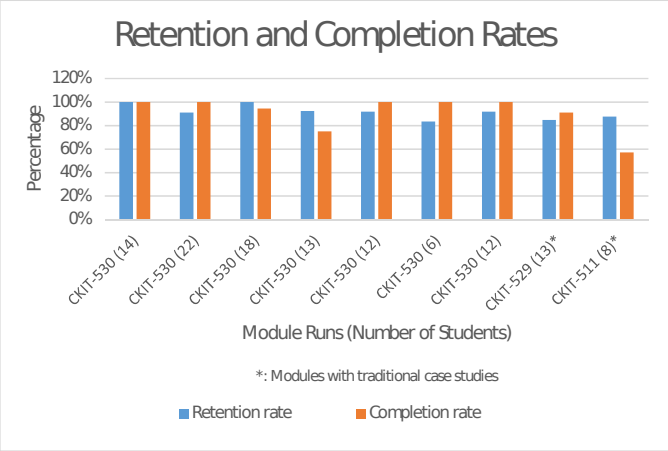


Fig. 2. Student's Retention and Completion: Traditional vs Innovative Method

The teaching staff observed a challenge in this way of implementing the new case study projects. In some case studies where the students are to build a deliberately vulnerable system for other groups to ethically hack, the vulnerable system needs to be up and running 24/7 during the project time for others to probe. Without utilising services such as Amazon AWS and alike services that are pre-loaded with the required tools (i.e. web-server), it is a stretching task for the students to implement/deploy the vulnerable systems and keep it running on their local machines all time. This observation is supported by the responses of the students at the end of the module

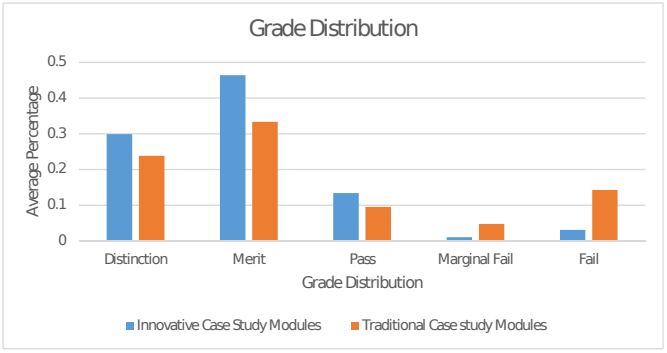


Fig. 3. Student's Grade Distribution: Traditional vs Innovative Method

satisfaction survey where quite often than not, they require to be given access to university created AWS instances. One of the teaching staff acknowledged the problem and recorded in the Faculty Feedback form that "We may go for AWS for this project but as I discussed with [..] and [..], we need to consider the legal obligations of running pen tests on AWS". It is worth noting that AWS requires approval before network stress testing and denial of service simulation [3]. The same issue has been observed by a senior academic staff member during the moderation process.

## V. Conclusion

Designing a case study project that serves as a small capstone project for online courses is challenging due to many reasons. Using the students to design the case studies could potentially decrease plagiarised answers, enrich the project selection pool, enable teaching staff with little experience in cyber-security to cover or teach modules when needed, and support meeting the feedback deadlines. Our experience with this innovative way of implementing case study projects is positive since it decreased the number of academic integrity breaches, increased the retention and completion rates, increased the success rate and hence decreased the fail one. It is worth noting that, the new method does not eliminate the possibility of collusion amongst groups from the same cohort, which could be solved by verifying the group's chat history is sound, which the teaching team has employed. At the moment, this way of designing module projects puts the students at the centre of the education process allowing more collaboration across different groups. Our observation is that the instructions for such group work need to be clear as some issues regarding the clarity of the instructions have been raised in the student satisfaction surveys. It is worth noting that, this innovative way of designing case-study-based projects for online courses could be generalised to any computing courses (i.e. further research is needed to investigate how would such practices be reused in other STEM subjects). It would be interesting to investigate how well students perform in a standard face-to-face class though, which requires further research.

[3]https://aws.amazon.com/security/penetration-testing/ accessed 07.04.2020

An observation is there is no significant difference when forming the groups randomly or based on time zones. The issue has been acknowledged in one of the modules' moderation process where the senior faculty running the moderation process said, "One interesting comment on time zones: Eastern Standard Time has no daylight saving, hence submission timestamp is one-hour off. [The] Student needed to indicate to tutor". The teaching team have had no major issues in the last ten years for group members who are geographically dispersed. We are seeing potential gain within groups with various time zones and/or backgrounds/skills [31]. Different time zones provide continuity of work in a way that a group member could post his/her contribution overnight to another group member who will be working on it on the evening of the same day due to time difference. In this way, there is always someone who is working on the project. We acknowledge, however, the challenge this may impose to synchronous communication (i.e. online meetings).

## REFERENCES


[1] S. Furnell, P. Fischer, and A. Finch, "Can't get the staff? the growing need for cyber-security skills," *Computer Fraud Security*, vol. 2017, no. 2, pp. 5 – 10, 2017.

[2] L. Topham, K. Kifayat, Y. A Younis, Q. Shi, and B. Askwith, "Cyber security teaching and learning laboratories: A survey," *Information Security: An International Journal*, vol. 35, 12 2016.

[3] Frost and Sullivan, "2017 global information security workforce study benchmarking workforce capacity and response to cyber risk," Center for Cyber Safety and Education (ISC), resreport, May 2017.

[4] M. Hentea, H. S. Dhillon, and M. Dhillon, "Towards changes in information security education," *Journal of Information Technology Education: Research*, vol. 5, no. 1, pp. 221–233, January 2006.

[5] P. Darbyshire, "On-line learning, quality and student satisfaction: A case study," School of Information Systems, Victoria University, P.O. Box 14428, Melbourne City MC, VICTORIA 8001, AUSTRALIA, techreport IT4806, 2003.

[6] K. D. Rajab, "The effectiveness and potential of e-learning in war zones: An empirical comparison of face-to-face and online education in saudi arabia," *IEEE Access*, vol. 6, pp. 6783–6794, 2018.

[7] M. Coleman and Z. L. Berge, "A review of accessibility in online higher education," *Online Journal of Distance Learning Administration*, vol. 21, no. 1, 2018.

[8] K. Kelm and G. Miles, "Group projects in in-ground undergraduate and on-line graduatedegree programs: Guidelines for success," *Information System Education Journal*, vol. 4, no. 80, pp. 1–9, Sep. 2006.

[9] D. Grant, A. Malloy, M. Murphy, J. Foreman, R. Robinson, and E. Summary, "Real world project: Integrating the classroom, external business partnerships and professional organizations," *Journal of Information Technology Education: Innovations in Practice*, vol. 9, 01 2010.

[10] F. Suleman, "The employability skills of higher education graduates: insights into conceptual frameworks and methodological options," *Higher Education*, vol. 76, 08 2018.

[11] J. Blanford, P. Kennelly, B. King, D. Miller, and T. Bracken, "Merits of capstone projects in an online graduate program for working professionals," *Journal of Geography in Higher Education*, vol. 44, pp. 1–25, 11 2019.

[12] W. Rowe, B. Harris, M. Graf, and S. Rogers, *Enhancing Student Learning Experience through Group Supervision Using a Digital Learning Platform*. Royal Roads University, 2016, ch. 5, pp. 113–138.

[13] A. Davis, "Project-based learning in distance learning highschool courses," mathesis, SIT Graduate Institute, May 2017.

[14] A. Sherman, M. Dark, A. Chan, R. Chong, T. Morris, L. Oliva, J. Springer, B. Thuraisingham, C. Vatcher, R. Verma, and S. Wetzel, "Insure: Collaborating centers of academic excellence engage students in cybersecurity research," *IEEE Security Privacy*, vol. 15, no. 4, pp. 72–78, 2017.

[15] M. Rahouti. and K. Xiong., "A customized educational booster for online students in cybersecurity education," in *Proceedings of the 11th International Conference on Computer Supported Education - Volume 2: CSEDU,*, INSTICC. SciTePress, 2019, pp. 535–541.

[16] A. Konak and M. R. Bartolacci, "Using a virtual computing laboratory to fostercollaborative learning for information securityand information technology education," *Cybersecurity Education, Research and Practice*, vol. 2016, no. 1, 2016.

[17] K. Salah, "Harnessing the cloud for teaching cybersecurity," in *Proceedings of the 45th ACM Technical Symposium on Computer Science Education*, ser. SIGCSE '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 529–534.

[18] K. Salah, M. Hammoud, and S. Zeadally, "Teaching cybersecurity using the cloud," *IEEE Transactions on Learning Technologies*, vol. 8, no. 4, pp. 383–392, 2015.

[19] V. Padman and N. Memon, "Design of a virtual laboratory for information assurance education and research," pp. 17–19, 07 2002.

[20] J. Hu, C. Meinel, and M. Schmitt, "Tele-lab it security: An architecture for interactive lessons for security education," in *Proceedings of the 35th SIGCSE Technical Symposium on Computer Science Education*, ser. SIGCSE '04. New York, NY, USA: Association for Computing Machinery, 2004, p. 412–416.

[21] Z. Yang and Q. Liu, "Research and development of web-based virtual online classroom," *Computers Education*, vol. 48, pp. 171–184, 02 2007.

[22] J. Haag, T. Horsmann, S. Karsch, and H. Vranken, "A distributed virtual computer security lab with central authority," in *Computer Science Education Research Conference*, ser. CSERC '11. Heerlen, NLD: Open Universiteit, Heerlen, 2011, p. 89–95.

[23] L. Xu, D. Huang, and W. Tsai, "Cloud-based virtual laboratory for network security education," *IEEE Transactions on Education*, vol. 57, no. 3, pp. 145–150, 2014.

[24] A. K. Amorin, B. N. Shekar, and C. L. AlAuf, "Cloudwhip: A tool for provisioning cyber security labs in theamazon cloud," in *International Conference on Security and Management (SAM)*, 2014, pp. 1–7.

[25] J. Sianipar, C. Willems, and C. Meinel, "A container-based virtual laboratory for internet security e-learning," *International Journal of Learning and Teaching*, 01 2016.

[26] J. Wroclawski, T. Benzel, J. Blythe, T. Faber, A. Hussain, J. Mirkovic, and S. Schwab, *DETERLab and the DETER Project*. Cham: Springer International Publishing, 2016, pp. 35–62.

[27] J. Sianipar, C. Willems, and C. Meinel, "Team placement in crowd-resourcing virtual laboratory for it security e-learning," in *Proceedings of the 2017 International Conference on Cloud and Big Data Computing*, ser. ICCBDC 2017. New York, NY, USA: Association for Computing Machinery, 2017, p. 60–66.

[28] R. S. Weiss, S. Boesen, J. F. Sullivan, M. E. Locasto, J. Mache, and E. Nilsen, "Teaching cybersecurity analysis skills in the cloud," in *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, ser. SIGCSE '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 332–337.

[29] T. Estes, J. Finocchiaro, J. Blair, J. Robison, J. Dalme, M. Emana, L. Jenkins, and E. Sobiesk, "A capstone design project for teaching cybersecurity to non-technical users," in *Proceedings of the 17th Annual Conference on Information Technology Education*, ser. SIGITE '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 142–147.

[30] W. He, X. Yuan, and L. Yang, "Supporting case-based learning in information security with web-based technology," *Journal of Information Systems Education*, vol. 24, pp. 31–40, 01 2013.

[31] D. F. J.-G. B. Karsten Lundqvist, Ali Ahmed, "Interdisciplinary agile teaching," in *Proceedings of IEEE Frontiers in Education Conference (FIE)*, Cincinnati, Oct. 2019.

[32] Z. Masood, R. Hoda, and K. Blincoe, "Adapting agile practices in university contexts," *Journal of Systems and Software*, vol. 144, pp. 501 – 510, 2018.

[33] K. Topping, *Peers as a source of formative and summative assessment*. United Kingdom: SAGE Publications, 2013, pp. 395–412.

[34] M. Usher and M. Barak, "Peer assessment in a project-based engineering course: comparing between on-campus and online learning environments," *Assessment Evaluation in Higher Education*, vol. 43, pp. 745–759, 01 2018.

[35] L. R. Kearns, "Student assessment in online learning:challenges and effective practices," *MERLOT Journal of Online Learning and Teaching*, vol. 3, no. 8, pp. 198–208, 2012.

[36] S. Ashton and R. S. Davies, "Using scaffolded rubrics to improve peer assessment in a mooc writing course," *Distance Education*, vol. 36, no. 3, pp. 312–334, 2015.

[37] S. J. Deeley and C. Bovill, "Staff student partnership in assessment: enhancing assessment literacy through democratic practices," *Assessment Evaluation in Higher Education*, vol. 42, pp. 463 – 477, 2017.

[38] A. Jaime, J. Blanco, C. Domínguez, A. Sánchez, J. Heras, and I. Usandizaga, "Spiral and project-based learning with peer assessment in a computer science project management course," *Journal of Science Education and Technology*, vol. 25, 02 2016.

[39] T. Harland, N. Wald, and H. Randhawa, "Student peer review: enhancing formative feedback with a rebuttal," *Assessment Evaluation in Higher Education*, vol. Accepted, 05 2016.

[40] M. Usher and M. Barak, "Peer assessment in a project-based engineering course: comparing between on-campus and online learning environments," *Assessment & Evaluation in Higher Education*, vol. 43, no. 5, pp. 745–759, 2018.

[41] M. Formanek, M. C. Wenger, S. R. Buxner, C. D. Impey, and T. Sonam, "Insights about large-scale online peer assessment from an analysis of an astronomy mooc," *Computers Education*, vol. 113, pp. 243 – 262, 2017.

[42] J. Sunol, G. Arbat, J. Pujol, L. Feliu, R. M. Fraguell Sansbelló, and A. Planas, "Peer and self-assessment applied to oral presentations from a multidisciplinary perspective," *Assessment Evaluation in Higher Education*, vol. 41, pp. 1–16, 05 2015.

[43] A. Fathelrahman, "Using reflection to improve distance learning course delivery: a case study of teaching a management information systems course," *Open Learning: The Journal of Open, Distance and e-Learning*, vol. 34, no. 2, pp. 176–186, 2019.

[44] Y. Liu, "Using reflections and questioning to engage and challenge online graduate learners in education," *Research and Practice in Technology Enhanced Learning*, vol. 14, pp. 1–10, 2019.

[45] M. Pecar and R. P. Gasparic, "Analysis of an asynchronous online discussion as a supportive model for peer collaboration and reflection in teacher education," *Journal of Information Technology Education: Research*, vol. 15, no. 1, pp. 369–393, December 2015.

[46] J. Smith and H. Greene, "Pre-service teachers use e-learning technologies to enhance their learning," *Journal of Information Technology Education:Research*, vol. 12, pp. 121–140, 01 2013.

[47] N.-S. Chen, C.-W. Wei, K.-T. Wu, and L. Uden, "Effects of high level prompts and peer assessment on online learners' reflection levels," *Computers Education*, vol. 52, no. 2, pp. 283 – 291, 2009.

[48] G. Salmon, "Mirror, mirror, on my screen exploring online reflections," *British Journal of Educational Technology*, vol. 33, no. 4, pp. 379–391, 2002.

[49] L. Mortari, "Reflectivity in research practice: An overview of different perspectives," *International Journal of Qualitative Methods*, vol. 14, no. 5, p. 1609406915618045, 2015.

[50] M. van Manen, "Linking ways of knowing with ways of being practical," *Curriculum Inquiry*, vol. 6, no. 3, pp. 205–228, 1977.

[51] Q. Liu, J. Ji, J. Chen, W. Zhao, and J. Yin, "Evaluating the effectiveness of situational case-based teaching: A view of concept mapping," in *Proceedings of ACM Turing Celebration Conference - China*, ser. TURC '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 60–66.

[52] J. Haag, H. Vranken, and M. van Eekelen, *A Virtual Classroom for Cybersecurity Education*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 173–208.

[53] V. Brown, "Evaluating technology to prevent academic integrity violations in online environments," *Online Journal of Distance Learning Administration*, vol. 21, no. 1, 2018.

[54] S. Schleimer, D. Wilkerson, and A. Aiken, "Winnowing: Local algorithms for document fingerprinting," *Proceedings of the ACM SIGMOD International Conference on Management of Data*, vol. 10, 04 2003.

[55] D. Rohwedder and B. R. Snider, "Plagiarism detection avoidance methods and countermeasures," *J. Comput. Sci. Coll.*, vol. 34, no. 1, p. 255–261, Oct. 2018.