Open Access License Notice

Are Cybersecurity Laboratory Exercises Constructivist in Use?

Abstract

Private industry and U.S. government entities alike have expressed urgent demand for employable students with practical experience in cybersecurity. In response, education increasingly utilizes laboratory exercises as part of an overarching pedagogy. To date, the design and implementation of such exercises has purportedly been of a constructivist nature. As such, prominent learning theory maintains that students are at the center of knowledge acquisition. A body of research supports this notion. However, a gap exists in the literature insofar as there has been no examination of how these exercises manifest learning theory when in use. Therefore, the purpose of this study was to measure how users of cybersecurity laboratory exercises describe those exercises, in use, in the context of learning theory. Through a mixed method approach, data revealed that users describe the exercises as objectivist in nature. Such a result is significant for educators and researchers. Further, based on the results, this study includes several recommendations for future work.

Keywords: Cybersecurity, laboratory exercises, pedagogy, constructivism, objectivism

I. Introduction

Demand for skilled cyber security professionals in private industry and the U.S. federal government has resulted in increased attention on the education of tomorrow's cybersecurity professionals [1]. A great deal of this attention focuses on the use of laboratory exercises in cybersecurity education. In fact, laboratory exercises have become the primary means of providing students with hands on learning [2][3][4]. Furthermore, researchers such as Irvine [5], Yurcik and Doss [6] Kaucher and Saunders [7], and Goel et al. [8] noted educators have adopted the constructivist-learning model as the predominant theory in the education of learners in this field of study. Such research identified laboratory exercises as primarily constructivist within cybersecurity education at the collegiate level.

There exists research focused on learning theory related to the design of cybersecurity laboratory exercises. Moreover, literature found in different knowledge domains considered potential differences in learning theory expression between design and use [9][10]. Yet, in the context of cybersecurity education, there is a general failure to address the role of laboratory exercises as pedagogical tools *in use*. In response to this shortfall, the purpose of this study was to measure how the users of cybersecurity laboratory exercises describe those exercises, in use, in the context of learning theory. A single research question guided this study- *do the users of cybersecurity laboratory exercises describe those exercises in a manner that is consistent with constructivist learning principles*?

A. Learning Theory

Learning theories provide a framework for describing different methods of instruction [11]. Regardless of the categorization of these theories, a common relationship exists insofar as each theory provides guidance for the creation of pedagogical techniques [12]. Learning theory sets the stage for how the educator and the learner will engage in knowledge construction. While multiple learning theories exist this research is concerned with two pedagogical approaches, which have dominated cybersecurity education: objectivist and constructivist.

Earlier paradigms of teaching stemmed from concepts of objectivist learning theory [13]. The

objectivist model promotes passive teacher-centered learning methods that accentuate the separation between learner and educator. The educator is the primary provider of information through one-way communication. Characteristic of objectivist learning theory is instructional material presented logically and sequentially through lecture and demonstration [14].This method facilitates memorization of information with the expectation that the educator provides prompts and feedback throughout the learning process. Objective truths exist independent of learner understanding [15]. Arbaugh and Benbunan-Fich [16] argued, "Learning is impoverished when students are passive recipients of content that is delivered to them" (p. 436). As a result, learners are inadequately educated. A more active approach is necessary for cybersecurity learners to acquire knowledge [7].

In contrast to objectivist learning, constructivist learning provides an environment where knowledge acquisition is an active learner-centered process built on problem solving [17]. The assumption is that student learning is greater when they are empowered to discover knowledge rather than instructed. In objectivism the instructor role centers on providing direction and guidance and is but one of many sources of information. Constructivism allows knowledge to be constructed in the mind of the learner because of learner experiences and investigation built on prior knowledge and experience [18]. The constructivist model accommodates an open and dynamic learning experience better suited to cyber education [19].

II. Method

A. Participants

The population for the quantitative portion of this mixed method study included four types of students from cybersecurity or related fields: students pursuing a four year undergraduate degree, students holding four year undergraduate degrees, students in graduate school, and students with a graduate degree. Participants consisted of 120 web-based survey respondents. Class level of respondents varied between undergraduate freshmen (15%), sophomores (16%), juniors (27%), and seniors (19%). Three percent identified as former students holding a four-year degree but no longer enrolled. The balance of respondents, 20%, identified as graduate school students.

This study used purposive sampling to garner participants for the quantitative questionnaire.
In total, 200 participants started the study. The final sample size was 120. Of the 80 participants opting out, 30 failed to start the questionnaire, 10 started the questionnaire but did not respond to any questions and the remaining 40 did not complete enough of the questionnaire to supply meaningful data. Calculation of confidence interval and margin of error used a total population size of 20,000, as the actual size was unknown. Given the final sample size of 120, the confidence interval computed as approximately 96% while the margin of error computed to approximately seven and a half percent.

B. Research Method and Design

The purpose of this study was to measure how the users of cybersecurity laboratory exercises describe those exercises, in use, in the context of learning theory. Actualization of this purpose required two data sets: a set of objectivist and constructivist learning theory characteristics and descriptive data from users of cybersecurity laboratory exercises. The former fit qualitative models of inquiry while the latter fit quantitative models. Thus, a mixed research methodology qualified as the most appropriate technique for this study [20][21].

The mixed method approach included a qualitative exploratory design and a quantitative survey research design. According to Jupp [22], an exploratory research design is appropriate when analyzing

existing primary data with the goal of further defining a problem or concept. In the scope of this study the exploratory design aided in the analysis of existing learning theory literature with the goal of generating keywords for development of the survey questionnaire. Therefore, the exploratory design was appropriate.

In conjunction with the qualitative exploratory design, a quantitative descriptive research design was appropriate for studying the attitudes or beliefs concerning a central event [21]. Furthermore, according to Leedy and Ormrod [23], a survey research design is appropriate when descriptive data is collected through a questionnaire. This study employed a web-based questionnaire instrument to collect the attitudes of participants, thus a survey research design fit. Other descriptive research designs were not appropriate because this study did not involve direct observation of the participants or involve a limited case in time and place.

C. Data Collection and Analysis

Data collection occurred first through conventional content analysis [24] of learning theory literature and second through voluntary participation in a web-based survey. As part of the exploratory research, this study collected and analyzed data from published literature related to learning theory. Identification of seminal research occurred through exhaustive cross-referencing of literature in academic databases such as ProQuest, Google Scholar and Academic Search Premier (EBSCOHost). Next, the exploratory design allowed keywords (e.g. passive versus active, dependent versus independent) to emerge from the literature through content analysis techniques, which in turn became the coded themes used for development of the quantitative questionnaire. Coded themes represented unique knowledge categories as well as definitive characteristics of objectivist and constructivist learning theory.

The survey instrument consisted of a Likert scale with six items and five multiple-choice questions (Table 1). The Likert scale included five possible responses: *strongly agree, agree, neutral, disagree,* and *strongly disagree*. The five nominal categorical values correspond to nominal discrete data values of one (1), two (2), three (3), four (4) and five (5) respectively. Multiple choice questions varied in response arrays from simple *true* or *false* to several topical choices. In all cases, the nominal categorical data correspond to nominal discrete values of one (1) and two (2). The questionnaire employed bounded questions throughout. Data analysis was limited to frequency, statistical measure of center (median), and statistical measure of spread (inter-quartile range [IQR]).Statistical analysis consisted of loading the questionnaire results into an R statistical computing environment and outputting frequency graphs and statistical measures.

D. Pilot

This study piloted the survey instrument with ten volunteers with the goal of establishing reliability and validity of the questionnaire. Data associated with the pilot were not included in the findings. Rather, data from the pilot in conjunction with feedback from participants guided revisions to the questionnaire. The pilot test captured participant feedback through four additional open-ended questions. The additional questions were as follows.

1. Were the questions clearly worded? If no, which questions were not clearly worded and how would you advise changing those questions?
2. Was the meaning of the questions easily understood? If no, which questions were not clear and how would you suggest revising such?
3. Do you feel that the questionnaire was too lengthy or took too long to complete?

4. What suggestions, if any, do you have to improve the questionnaire?

Table 1
The eleven questions contained in the survey instrument and the associated question type

Three questions within the survey instrument received updates based on feedback from pilot participants. Such updates consisted of word order shifting and synonym exchange to make the meaning of the three questions more clear. With reliability and validity established, the survey instrument was then frozen from changes and made available for the direct study population sample.

III. Results

The purpose of this study was to measure how the users of cybersecurity laboratory exercises describe those exercises in the context of learning theory. Furthermore, a single research question guided this study- *do the users of cybersecurity laboratory exercises describe those exercises in a manner that is consistent with constructivist learning principles*? In order to answer the research question, this study employed a mixed research methodology- utilizing an exploratory qualitative design and a quantitative survey design.

Qualitative data analysis occurred in conjunction with the exploratory phase of this study. In this, the first phase of the original research, content analysis of existing learning theory literature produced six overarching categories of knowledge behavior with 12 corresponding characteristics (six for objectivist learning theory and six for constructivist learning theory). Subsequently, analysis of primary data collected through a web-based questionnaire in the second phase of this research yielded results demonstrating clear trending and attitudes.

A. Characteristics of Learning Theory

Table 2 summarizes the qualitative findings from the content analysis of objectivist and constructivist learning theories [15][14][25]. Knowledge categories emerged from the content analysis as attributes of the knowledge acquired during objectivist and constructivist learning activities. The knowledge categories, in turn, directed grouping of questions for the quantitative questionnaire. In contrast, characteristics of objectivist and constructivist learning theories emerged during content analysis as attributes of the actors (e.g. professor, student, or laboratory exercise). The specific characteristic associated with each category became the basis for individual questions on the survey instrument.

Table 2
The Categories of Knowledge with Characteristics of Objectivist and Constructivist Learning Theory

B. Descriptions of Cybersecurity Laboratory Exercises In Use

Participants in this study answered 11 questions, six Likert items and five multiple choice questions, concerning cybersecurity laboratory exercises as the participants experienced using such exercises (Table 2). The questions generated nominal discrete data. Data underwent statistical analysis in order to produce frequency, statistical measure of center (median), and statistical measure of spread (IQR). Because the survey questions stemmed from the qualitative portion of this study, this study grouped data according to the same six categories. Questions appear in multiple categories because the underlying meaning applied across knowledge categories.

Analysis of the questionnaire data occurred in two stages. In the first stage, calculation of the statistical median and inter-quartile range for the individual questions within the overall questionnaire array occurred. The second stage included frequency of response calculation within each discrete knowledge category. Presentation of the results follows this approach for readability purposes.

I. Overall question array results

Results for all questions contained the full range of responses. At least one participant provided a response in each of the Likert items. Therefore, the minimum (*Min*) for each question appeared as one and the maximum (*Max*) appeared five. The number (*N*) of responses totaled 120 for each question after pruning partial responses and eliminating no responses from the count. Questions one through six were Likert items. Data associated with Q1 through Q6 revealed that participants view cybersecurity laboratory exercises as objectivist in use (Table 3). Further, the data showed most participants disagreeing (questions 1, 2, 3, 4, and 6, *Median*=4) or agreeing (question 5, *Median*=2). In all questions, low IQR values supported uniformity in responses.

Questions seven through 11 were multiple-choice questions. Three of these questions required participants to judge the question (statement) as true or false. The remaining two questions asked participants to select one of two bounded responses that best described the individual participant's attitude in the context of the question. All participants responded (*N*=120) and with all possible values (*Min*=1, *Max*=2). As with the Likert items responses indicated an overtly objectivist description of cybersecurity laboratories in use. Data associated with these questions were coalesced and uniform.

II. Knowledge action results

Participants responded to one Likert item and one multiple-choice question in the knowledge action category. The Likert item asked participants to grade the level of agreement with the notion that *successfully completing laboratory exercises requires replicating the steps shown in the lab manual*

Table 3
Measures of center and measures of spread belonging to the 11 survey questions

(Q5). Affirmation the notion indicated an underlying objectivist mechanism whilst disagreement equated to the constructivist idea of active learning. Results, displayed in Figure 1, showed that 68% (*N*=82) of participants agreed that replicating steps from the manual resulted in success while 15% (N=18) strongly agreed. On the other hand, ten percent disagreed (*N*=12) and three percent strongly disagreed *N=4*). Additionally, three percent remained neutral to the assertion.

Figure 1. Response frequency distribution of disagreement and agreement with the notion that successful completion of laboratory exercises requires replicating steps from the lab manual.

Similarly, the multiple-choice question (Q8) inquired if *completing laboratory exercises requires* (a) following the exact steps in the laboratory manual or (b) synthesizing knowledge from prior and new experiences. The first option stemmed from the concept of knowledge acquisition being passive in objectivist learning theory. On the contrary, the second option described an active or constructivist idiom. The results of the multiple-choice question, shown in Figure 2, indicated that 68% (*N*=81) of participants passively follow the laboratory manual as opposed to 33% (*N*=39) that synthesize

knowledge. These results comported with the same-group Likert data and further indicated an objectivist nature.

Figure 2. Response frequency distribution associated with the action of knowledge acquired through laboratory exercises according to study participants.

III. Knowledge direction results

With the knowledge direction category, participants answered two multiple-choice questions. The first question (Q9) inquired if participants would describe laboratory exercises as reinforcing *memorization of new information or active synthesis of new information through action.* Seventy-four percent of participants (*N*=89) described cybersecurity laboratory exercises as reinforcing memorization. Meanwhile, 24% (*N*=29) selected the synthesis of information option. Overall, as shown in Figure 3, these results demonstrated an objectivist characteristic as the direction of the knowledge appeared to be from an authority to the student.

Figure 3. Response frequency distribution of the knowledge direction pertaining to whether laboratory exercises reinforce memorization or synthesis of information.

In the second question of this grouping (Q11), participants described the assertion that *laboratory exercises act as lectures in showing me new commands and tools* as true or false. As summarized in Figure 4, the majority of participants viewed the assertion as true (69%, *N*=83) while a small number (29%, *N*=35) felt that the assertion was false. The data described an objectivist characteristic here as well since the direction of knowledge stemmed from a central authoritative source. Such consensus regarding laboratory exercises taking a lecture-based role reaffirmed the earlier data in this category (Figure 3).

Figure 4. Response frequency distribution associated with the notion that laboratory exercises perform the same role as lecture.

IV. Knowledge state results

The knowledge state category included three questions: two Likert items and one multiple-choice question. These questions probed for responses that might indicate whether knowledge acquisition occurred independent of existing experiences or dependent upon prior experiences. The first Likert item (Q2) asked participants to select a level of agreement with the statement that *laboratory exercises portray meaningful cybersecurity activities*. Most participants expressed disagreement (54%, *N*=65) while a smaller contingency expressed agreement (25%, *N*=30). At opposite ends, 8% (*N*=9) strongly disagreed and 3% (*N*=3) strongly agreed. One percent remained neutral (Figure 5).

Figure 5. Response frequency distribution of agreement and disagreement with the assertion that cybersecurity laboratory exercises portray meaningful activities.

Question four, also a Likert item, inquired about the degree of agreement participants had with the assertion that *laboratory exercises rely on existing knowledge to build new skills*. A position of agreement with this statement would indicate constructivist pedagogy whereas disagreement would indicate an objectivist nature. Similar to results from question two, most participants disagreed with the statement (68%, *N=81*). Another 6% (*N*=6) strongly disagreed. On the other hand, as seen in Figure 6, 18% (*N*=22) agreed that laboratory exercises rely on existing knowledge and three participants (3%)

strongly agreed. Six percent selected the neutral position (*N=7*).

Figure 6. Response frequency distribution of agreement and disagreement with the statement that laboratory exercises rely on existing knowledge to build new skills.

The final question in the knowledge state category (Q8) asked participants if *completing laboratory exercises requires* (a) following the exact steps in the laboratory manual or (b) synthesizing knowledge from prior and new experiences. Although this question appeared in the knowledge action category, the meaning applied to the knowledge state category as well. Knowledge exists independent of understanding when adhering to the lab manual while synthesizing knowledge draws upon prior experience. Continuing from Figure 2, 81 participants (68%) responded that following the exact steps in the laboratory manual precipitated success as opposed to 39 (33%) that synthesize based on prior experiences.

V. Knowledge motivation results

Both questions in the knowledge motivation category asked participants to evaluate a given statement as true or false based on the individual participant's experience with using cybersecurity laboratory exercises. Overall, motivation in acquiring knowledge can serve as a strong indicator of what learning theory empowers the pedagogy. The first question claimed that, *I am motivated by my own passion to complete laboratory exercises* (Q7). As shown in Figure 7, Seventy percent of participants described the claim as false (*N*=84) which indicated an underlying objectivist pedagogy because the motivation for knowledge acquisition would be extrinsic. Conversely, 36 participants viewed the claim as true (30%). Such indicated an intrinsic motivation, which equated to constructivist theory.

Figure 7. Response frequency distribution associated with the potential intrinsic motivation of knowledge acquisition when using laboratory exercises.

The results from question 10 were corroborative with question nine. Here, in the second question of the knowledge motivation category (Figure 8), many participants (*N*=83) viewed the notion that *the final grade of a laboratory exercises is less important than the information gained from the exercise* as false. In contrast, a 29% minority (*N*=35) considered the notion to be true.

Figure 8. Response frequency distribution associated with the potential extrinsic motivation of knowledge acquisition with using laboratory exercises.

VI. Knowledge outcomes results

Two Likert items elicited feedback on the knowledge outcome associated with cybersecurity laboratories in use. The first Likert item asserted that *laboratory exercises reinforce multiple ways of accomplishing a goal* (Q3). Participants selected from amongst five Likert scalar responses. Disagreement with this assertion indicated an objectivist learning mechanism due to the pre-established nature of the knowledge outcome. Alternatively, agreement indicated constructivist principles based upon the open-ended concept of promoting multiple paths to knowledge acquisition. The results indicated that the majority of participants disagreed with the assertion (Figure 9). More specifically, 64% disagreed, 17% strongly disagreed, 12% agreed, and three percent strongly agreed. Four percent selected the neutral response (Figure 9).

*Figure 9***.** Response frequencies describing disagreement and agreement with the assertion that labs reinforce multiple ways of accomplishing a goal.

The second question (Q6) queried participants as to whether *mistakes in laboratory exercises served as valuable feedback*. Incorporation of mistakes, in constructivist theory, can be important sources of knowledge acquisition as such provide alternate paths of learning. Contrarily, objectivist theory maintains that knowledge outcomes are pre-determined which precludes incorporation of mistakes as a form of feedback acquisition. To that end, 60% of participants disagreed (N=72), thus describing an objectivist expression of knowledge acquisition (Figure 10). An additional three percent strongly disagreed. In support of objectivist characteristics, twenty-six participants agreed that mistakes serve as valuable feedback. A further 10% percent strongly agreed. Five percent remained neutral.

Figure 10. Response frequency distribution associated with agreement levels of whether mistakes in laboratory exercises served as valuable feedback.

VII. Knowledge environment results

One final question, a Likert item, fell under the knowledge environment category. The environment in which knowledge acquisition occurs stems either from abstract concepts that represent experiences (objectivist) or from real experiences directly (constructivist). Therefore, the question (Q1) inquired if *laboratory exercises mimic real-world activities in a realistic manner*. As summarized in Figure 11, most participants disagreed with this notion (62%, N=74) or strongly disagreed (12%,N=14) although some (20%, N=24) agreed and strongly agreed (5%, N=6). Just two participants selected the neutral response. Overall, the results pointed towards a basal objectivist description of knowledge.

Figure 11. Response frequency distribution describing the level of agreement with the notion that laboratory exercises mimic real-world activities in a realistic manner.

IV. Conclusion

Industry has placed a high demand on acquiring a skilled cybersecurity workforce [1]. A timely and topical pedagogy employed to meet such demand is the laboratory exercise [2][3][4]. Existing research [5][6][7][8] categorized laboratory exercises as constructivist- that is; learning originates with the student as opposed to an external, centralized source of knowledge authority. However, such literature has not considered how learning manifests when a laboratory exercise is in use.

Thus, the purpose of the study was to measure how the users of cybersecurity laboratory exercises describe those exercises in the context of learning theory. Furthermore, a single research question guided this study- *do the users of cybersecurity laboratory exercises describe those exercises in a manner that is consistent with constructivist learning principles*? In order to answer the research question, this study employed a mixed research methodology- utilizing an exploratory qualitative design and a quantitative survey design. The exploratory design used content analysis to produce knowledge categories and knowledge characteristics. In turn, the content analysis output seeded the creation of the quantitative survey instrument. Resultant data underwent statistical analysis using mean, IQR and frequency distribution modeling.

The results of the quantitative data analysis revealed a gap between the design of cybersecurity laboratory exercises and the manifestation of learning when students engage these exercises. The majority of participants described objectivist characteristics associated with exercises in use across the

11 questions. In fact, in no questions did the majority of participants describe knowledge acquisition, in use of laboratory exercises, as constructivist. Further, all data were uniform and demonstrated a strong central tendency.

The best analogy to explain the results might be the creation of a specific color and shade through the mixture of two complimentary colors. Consider the color green as an output of yellow and blue. Conceptually, the production of green is a straightforward process. However, the practical implementation of the process can produce a large array of green colors depending upon the precise mixture of yellow and blue. Here, learning theory is similar to the conceptual process of mixing yellow and blue. The laboratory exercises, as an expression of learning theory, are like the color green. The practical process of using the laboratory exercises then is akin to real-world paint mixing. Accordingly, the recommendations in this study seek to refine the mixing process, as it were, rather than abandoning the entire endeavor.

V. Recommendations

One recommendation would be to incorporate a type of unit testing into the laboratory exercise development cycle whereby pilot users can report on learning characteristics. Of course, this recommendation applies to exercises newly created. Existing cybersecurity laboratory exercises may still be deficient. Therefore, another recommendation stemming from the results of this study would be to identify the specific objectivist constructs within existing laboratory exercises and exchange those for constructivist concepts.

Admittedly, the above recommendations operate from the assumption that educators and researchers desire constructivist laboratory exercises. In reality, such may not be true. When considering modern pedagogy (e.g., flipping the classroom), objectivist laboratory exercises may indeed be a desirable tool. In this case, future work may be desirable along the lines of investigating how to leverage the objectivist nature of laboratory exercises in use to supplement or eliminate traditional lecture.

Alternatively, as a final recommendation, future studies may want to consider updating the learning theory construct associated with development of cybersecurity laboratory scenarios. Changing the underlying concept would mitigate the need to modifying the laboratory exercises directly. One such example is peer learning, a constructivist pedagogy that could rapidly absorb existing laboratories into a student centered knowledge acquisition environment.

References

[1] Yang, T.A., Yue, K., Liaw, M., Collins, G., Venkatraman, J. T., Achar, S., ... Chen, P. (2004). Design of a distributed computer security lab. *Journal of Computing Sciences in Colleges, 20*(1), 332 346. Retrieved from http://dl.acm.org/citation.cfm?id=1040274

[2] Ananthapadmanabhan, V., Frankl, P., Memon, N., &Naumovich, G. (2003, July).Design of a Laboratory for Information Security Education.In C. Irvine, & H. Armstrong (Eds.), *Security education and critical infrastructures* (61-73). Norwell, MA: Kluwer Academic Publishers.

[3] Duffany, J. L., & Cruz, A. (2012). Design of a computer security teaching and research laboratory. In *Proceedings of the 43rd ACM technical symposium on Computer Science Education* (p. 678). New York: ACM New York. doi:10.1145/2157136.2157421

[4] Mattord, H. J., & Whitman, M. E. (2004). Planning, building and operating the information security and assurance laboratory. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 8-14). New York: ACM New York. doi:10.1145/1059524.1059527

[5] Irvine, C. E. (1999). Amplifying Security Education in the Laboratory. In *Proceedings IFIP TC11 WC 11.8 First World Conference on Information Security Education* (pp 139–146). New York: Springer Publishing Company. Retrieved from cisr.nps.edu/downloads/papers/99paper_ampseced.pdf

[6] Yurcik, W. & Doss, D. (2001). Different approaches in the teaching of information systems security. *Proceedings of the Information Systems Education Conference 2001,* 32-22. Retrieved from http://proc.isecon.org/2001/04a/index.html

[7] Kaucher, C. E., & Saunders, J.H., (2002, June). *Building an information assurance laboratory for graduate-level education*, Paper presented at 6th National Colloquium for Information System Security Education, Redmond, WA.

[8] Goel, S., Pon, D., Bloniarz, P., Bangert-Drowns, R., Berg, G., Delio, V., ... Hobbs, J. (2006). Innovative model for information assurance curriculum: A teaching hospital. *Journal of Educational Resource, 6*(3), 2-15.doi:10.1145/1243481.1243483

[9] Kanuka, H. (2006). Instructional design and eLearning: A discussion of pedagogical content knowledge as a missing construct. *e-Journal of Instructional Science and Technology, 9*(2), 1-17. Retrieved from http://www.ascilite.org.au/ajet/e-jist/docs/vol9_no2/papers/full_papers/kanuka.pdf

[10] Wilson, B. G. (1995). Maintaining the ties between learning theory and instructional design. Presented at the meeting of the American Education Research Association, San Francisco, March 1995. Retrieved from http://carbon.ucdenver.edu/~bwilson/mainties.html

[11] Ormrod, J. E. (2012). *Human learning*(6th ed.). Boston: Pearson.

[12] Hill, W.F. (2002) *Learning:A survey of psychological interpretation* (7th ed).Boston, MA: Allyn and Bacon.

[13] Vrasidas, C. (2000). Constructivism versus objectivism: Implications for interaction, course design, and evaluation in distance education. *International Journal of Educational Telecommunications, 6*(4), 339-362. Retrieved from http://www.cardet.org/vrasidas/pubs/continuum.pdf

[14] Kundi, G. M., & Nawaz, A. (2010) From objectivism to social constructivism: The impacts of information and communication technologies (ICTs) on higher education. *International Journal of Science and Technology Education Research, 1*(2), 30-38. Retrieved from https://www.researchgate.net/publication/228888921

[15] Anson, C. S., & Miller-Cochran, S. K. (2009). Contrails of learning: Using new technologies for vertical knowledge-building. *Computers and Composition, 26*(1), 38-48.doi: 10.1016/j.compcom.2008.11.002

[16] Arbaugh, J. B. &Benbunan-Fich, R. (2006). An investigation of epistemological and social dimensions of teaching in online learning environments. *Academy of Management Learning and Education, 5*(4), 435-447. doi:10.5465/AMLE.2006.23473204

[17] Duffy, T. M., &Jonassen, D. H. (1992). *Constructivist and the technology of instruction: A conversation.* Hillsdale, NJ: Lawrence Erlbaum Associates.

[18] Anderson, T. &Dron, J. (2011). Three generation of distance learning pedagogy. *The Internation Review of Research in Open and Distance Education, 12*(3), 80-97. Retrieved from http://www.irrodl.org/index.php/irrodl/article/view/890

[19] Bednar, A.K., Cunningham, D., Duffy, T.M., and Perry, J.D. (1991). Theory into practice: How do we link?. In G. Anglin (Ed.), *Instructional Technology: Past, Present and Future* (100-112). Englewood, CO: Libraries Unlimited, Inc.

[20] Creswell, J. (2008). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. New Jersey: Pearson: Merrill Prentice Hall.

[21] Salkind, N. (2011).*Exploring research.* Boston: Pearson.

[22] Jupp, V. (2006). *The Sage dictionary of social research methods*. Thousand Oaks, CA: Sage Publications.

[23] Leedy, P. &Ormrod, J. (2010). *Practical Research*. Upper Saddle River: Merrill.

[24] Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9). 1277-1288.doi:10.1177/1049732305276687

[25] Phillips, P., Well, J., Curtis, R., & Kennedy, R. (2007).A case study of the relationship between socio-epistemological teaching orientations and instructor perceptions of pedagogy in online environment.*Electronic Journal for the Integration of Technology in Teacher Education, 6*, 3-27. doi:10.1.1.125.7383