Conceptual Analysis of Cyber Security Education based on Live Competitions

Katsantonis, Menelaos; Fouliras, Panayotis; Mavridis, Ioannis
Department of Applied Informatics
University of Macedonia
Thessaloniki, Greece
{mkatsantonis,pfoul,mavridis}@uom.gr

Abstract— **Live competitions, i.e. Capture the Flag, provide noteworthy experiences for the participants while offering both hands-on practice and entertainment. Aiming at performing a conceptual analysis as a basis for improving their pedagogical utilization, we investigate a number of live competition paradigms and analyse their structure by decomposing them into their respective elements and defining their relations. Moreover, we record the possible obstacles related to the pedagogical utilization of live competitions and group them into distinct categories. As a result, we construct a concept map of the technological and pedagogical characteristics of live competitions. Based on the proposed concept map and the recorded obstacles, we present a comparative evaluation scheme that we employ on three live competition approaches from the literature in order to reveal their value with respect to the educational impact. Finally, we discuss the results of our study and suggest directions for its utilization in the phases of analysis, feasibility and assessment towards developing of new live competition approaches for educational purposes. The adopted assumptions can bind the design of new efforts in cyber security education domain such as gamification and game based learning approaches that need to rely on sound learning theories, e.g. cognitive and experiential learning.**

Keywords*— cyber security; conceptual analysis; educational approaches; live competitions; ctf*

I. Introduction

While cyber security has increased as a critical issue over the last decade, governments and organizations have invested more and more in education and training of cyber security professionals. Moreover, the increase of cyber crime incidents, as well as their impact have provoked corresponding reflections on developing cyber security learning and training models, as well as searching for proper learning methods to produce more effective cyber security professionals.

Live competitions, such as Capture the Flag (CtF), provide noteworthy experiences for the participants while offering both hands-on practice and entertainment. Incorporating live competitions in the learning procedure, adds real-time value that facilitates motivation and deep involvement. Moreover, it introduces the crisis factor associated with many security situations. Consequently, pedagogues try to encompass live competitions to their educational contexts. However, various issues have been identified that limit the pedagogical values of live competitions. Under this perspective, a thorough reading of the literature reveals the lack of a conceptual framework to help in studying effectively the characteristics of live competitions and provides a basis for improving their pedagogical utilization.

II. Background

A. Live competitions

Live competitions are contests in which participants compete on their technical skills and knowledge in real time. Such contests have been organized for many years since the DefCon CtF, which was the first one employed in the nineties. The community appreciated the impact of such events and various competitions have been designed and developed, ever since. Nowadays, there are more than seventy CtF competitions organized in an annual basis [1], whereas there are numerous small-scale exercises organized in colleges and organizations that are not listed in a CtF ranking site.

According to the format and scale of the event, live competitions can be addressed as competitions, exercises or games. In addition, they have several directions that require participants to attack other teams, defend team's settings, or independently solve challenges in a so-called jeopardy style event [2]. Consequently, in attack and defend modes participants are required to interact directly with adversaries whereas in jeopardy mode events they act independently [3]. Many competitions use a combination of the aforementioned modes by setting the jeopardy style events as the playoffs of the competitions, and the attack/defense format in the finals.

Contestants take part in such events either as individuals or as team members. The knowledge barrier of the events may require participants to have a good background and experience in scripting languages, (e.g. Perl or Python), reverse engineering, operating systems, networking, system administration and application services [4] [5] in order to be competitive. Events occur on either physical or virtual machines and their development may require participants' physical co-location or allow remote connections by contestants from around the world. According to the motive of the competition, participants may be provided with numerous settings. Such settings may include network topologies, configured or deliberately misconfigured machines, operating systems and application software known or unknown prior to an event. Participants may also be provided with certain privileges and rules that permit or prohibit the use of certain

978-1-5090-5467-1/17/$31.00 ©2017 IEEE

tools and techniques (e.g. denial of service attacks and flooding). These settings vary according to each event's specified scenario. Scenarios typically demand to "capture" a specific file, called "flag", which is used as a proof that contestants have compromised a service or solved a challenge. Flags usually are long, random strings that are hard to guess [6]. They contain information and timestamps regarding the team, the host and the service they belong, their creation time and validity periods [7]. Some scenarios, in particular, may require compromising the settings of an adversary team, defending a system's services and files, attacking web sites, carrying out forensics investigations, reverse-engineering programs, attacking encrypted tokens, etc.

Participant assessment is usually based on a scoring scheme. According to the competition form and scenario, a participant's score increases when, for example, she manages to acquire a flag from another team or when she responds to a challenge correctly. On the contrary, the score of a team decreases when, for example, an adversary captures and submits one or more team's flags or its system's services become unavailable. Usually, the scoring scheme includes the employment of automated score-bots, whereas sometimes participants are required to write up their actions or evaluators supervise individuals' progress. Some scoring schemes are not typical; e.g., the iCtF scheme [8], which introduced the concept of money that allows teams to use the event's infrastructure to earn points and the notion of toxicity that constitutes a measure of damage effectiveness caused in a specific service [7].

The scoring system usually employs a setting, e.g. a web server, that includes a repository of flags or a service for automated submission testing and a displaying score device that provides feedback to all the concerned parties. The feedback is a critical aspect in the operation of live competitions [9]. Contestants that compete in the attack or jeopardy mode of a competition, receive feedback directly at the time that they submit a flag or other token, e.g. source code, to the scoring system [10]. When competing in the defend mode, they get feedback indirectly through the updates of scores that are based on the information provided by score-bots and on the submissions of the adversary participants [11].

Moreover, competition organizers always cater for the reliability and security of the contests so that participants will not be able to cheat the scoring schemes. Nevertheless, participants may be able to cheat by using prohibited tools and techniques or by successfully attacking the score services or by applying tricks. Specifically, contestants may try to:

- brute force flags,
- attack the scoring system to modify participants' records [10],
- tamper their own flags to make sure that no adversary team will submit them to the scoring system [3],
- make their services available only to the bots and deny access to everyone else [3].

Live competitions represent a useful pedagogical utility, particularly valuable in the multidisciplinary and complex domain of cyber security education. Their pedagogical significance has been widely stated in many studies [12]. In particular, it has been stated that live competitions provide the means to motivate participants to focus on the cyber security field by engaging participants in hands-on practices. They also include an entertainment factor as they constitute a gamified environment, in which contestants can compete, cooperate and express their feelings. Furthermore, live competitions can harvest to competitors the willingness to engage in continuous self-directed learning, experimentation and development in order to cope with the increasing demands of harder challenges and events [13]. Competitions that include the attack factor tend to be more enjoyable [6] and motivating for the participants.

B. Learning Theories

Live competitions promote experiential learning as the participants are engaged to hands-on activities, e.g. when they make efforts to reach competitions' goals [14]. Learners observe the results of their actions while getting feedback during the course of an event. For example, an effectively applied defensive policy can protect the participant's system from attacks, whereas an unsuccessful policy can lead to loss of points. In both cases, participants will reflect on their ideas and actions. According to the event's settings and rules, participants might share and discuss their ideas and feelings with their teammates or peers and instructors. Sometimes they are required to report their ideas or discuss them after the end of the process. In this a way, learners create mental models and generalization concepts on what part of the event they accomplished. Acquired concepts could then be applied in different experiences and settings in subsequent competition challenges or in real world situations [15].

Live competitions are consistent with problem-based learning as they require participants to apply their knowledge and skills to solve authentic problems. They also support situational learning by transferring capabilities and experiences in realistic situations [16]. Besides, team competitions can embrace socio-cultural learning approaches that can maximize their educational impact through collaboration, communication and teamwork [14]. Such approaches can train the participants to act effectively in team settings and subsequently prepare them to work and cooperate in similar settings of organizations and departments [17].

III. Methodology

For the purpose of this study, a literature search was undertaken during the spring of 2016 in the academic database Google scholar. The search strings used included keywords like "cyber", "security", "information", "systems", "defense", "hacking", "competition", "exercise", "game", "challenge", "education", "educational", "ctf", "capture the flag" and various combinations of them. Searches were limited to articles published in English from 2008 onwards. Each search yielded numerous hits to be examined and, therefore, we specified a number of selection criteria to aid in specifying the appropriate articles for inclusion in our study. Specifically, an article could be included in our study if it:

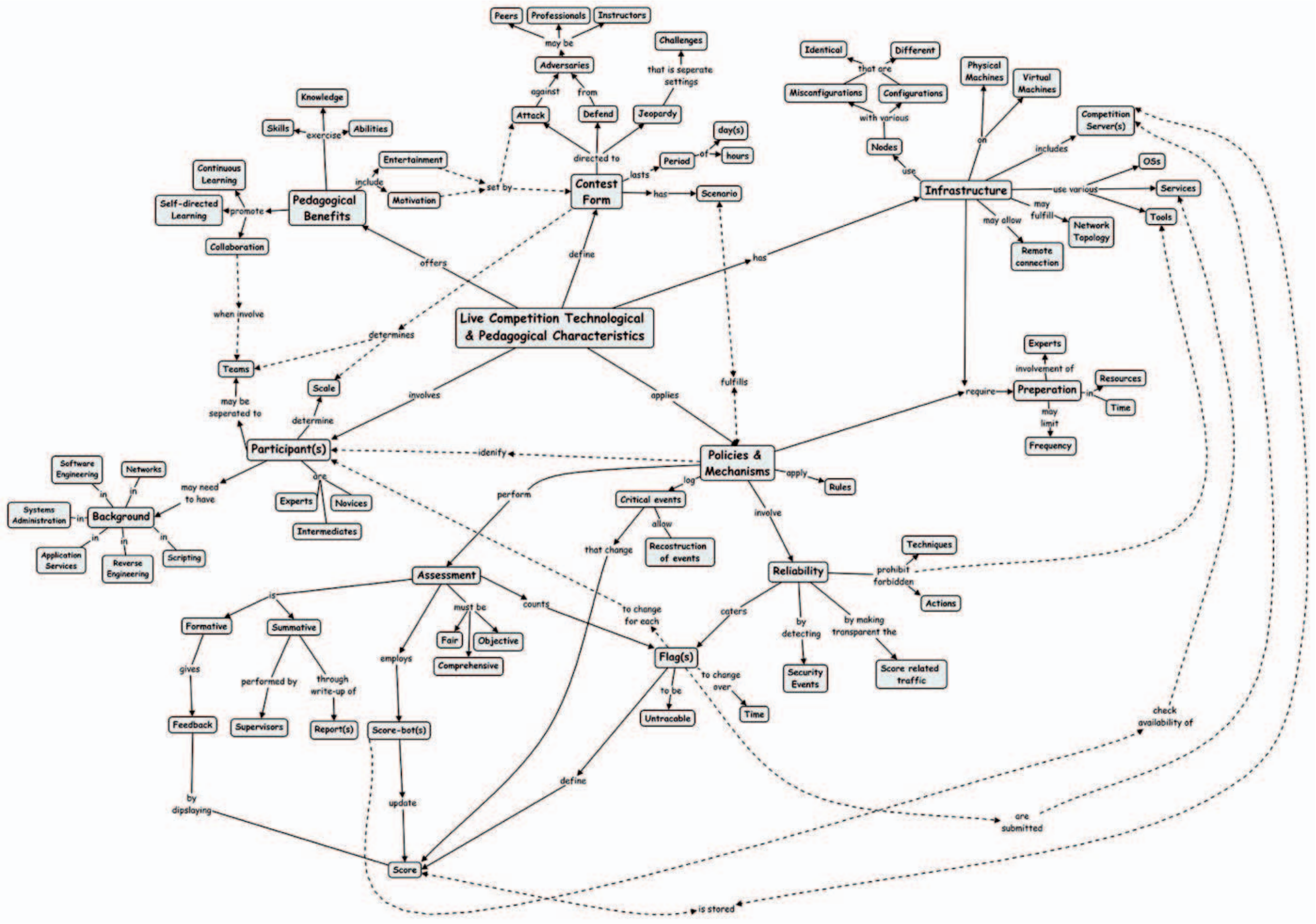

Fig. 1. Concept Map of Live Competitions Technological and Pedagogical Characteristics.

- proposed new approaches and provided directives for the exploitation of live competitions' in educational contexts, or
- presented the benefits, problems and issues related to live competitions, or
- documented experiences of organizing live competitions events, or
- described various modes (types) of live competitions.

The final selection consisted of 34 papers ([2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36]) that fulfilled the above described selection criteria to be considered relevant to the scope of this study.

Each of the selected papers was examined to derive multiple aspects of live competitions with the forms of concepts, characteristics, problems and challenges. The identified characteristics were recorded as nodes in a concept map with the help of the CMapTools program [37]. The focus question defined for the construction of the concept map was: "What are the key technological and pedagogical characteristics of live competitions?". The recorded nodes were correlated and merged gradually. Subsequently, they were analyzed in terms of their subjects (e.g. pedagogical side, rules of the contest, participants' profile, etc.) and their relations with the associated nodes, and they were grouped into categories. Both, the categories and the included concepts were then interconnected with labeled links to form a concept map (Fig. 1). Finally, the related concepts that were placed into separate groups (e.g. the notions of "motivation" and "attack"), were connected with crosslinks in order to specify the interrelationships between concepts of different categories.

Likewise, the identified problems and issues were compared, associated and grouped in distinct categories to form an index of challenges that live competition approaches can encounter. Based on the proposed concept map and the index of challenges, a comparative analysis scheme was elaborated. Subsequently, the analysis scheme was utilized on three notable approaches from the literature ([12], [18], [19]), in order to reveal their value with respect to the educational impact. The specific approaches were selected, as they are recent studies published in well-structured, justified and documented articles.

IV. Conceptual Analysis

A. Concept Map

Concept maps are graphical tools comprised of nodes that represent concepts and labeled links that symbolize the relations between concepts. They were invented by Joseph Novak in 1970s, based on the theories of Ausubel [38]. Novak defines the concept "as a perceived regularity in events or objects, or records of events or objects, designated by a label". In a concept map, concepts and relations are read as propositions that form meaningful statements. Concepts are organized in segments (domains) that are groups of nodes related to a specific sub-discipline of the map. In this a way, segments form hierarchical structures of concepts and segments. Relations that connect concepts of different segments are named cross-links. Concept mapping is a popular pedagogical tool used in multiple phases of a learning process, e.g. generation of ideas, diagnostic assessment, etc. Furthermore, they constitute a powerful research instrument that aids in analyzing and organizing ideas, creating new knowledge and communicating complex notions [39].

Fig. 1 depicts the proposed concept map of live competitions' key characteristics located in the selected papers of the literature. Although the proposed concept map includes only the typical key characteristics of live competitions, it contains numerous elements that reflect the diversity of the topic. In particular, the concept map consists of 77 concepts organized in 6 segments that share 14 cross-links represented in Fig. 1 with dashed lines for readability reasons. More detailed information is presented in Table I.

The concepts in the proposed concept map were organized in a nonhierarchical network structure, as live competition is a complex topic containing several concepts with multiple connections among them. Consequently, the concept map is logically organized in two clusters. The inner cluster contains the central node of live competitions characteristics and the general concepts. The latter are depicted as labels of the concept map's segments listed in Table I. On the contrary, the outer cluster includes more specific notions belonging to the domain of each general concept.

The rational of the proposed concept map segments is described below:

- "Contest Form": includes concepts related to the mode (format) of the event.
- "Pedagogical Benefits": contains the notions associated with the educational impact of the competition.
- "Participant(s)": includes characteristics associated to the contestants, i.e. profile in terms of background and experience in cyber security, and the manner they affect the live competitions' format.

TABLE I. Number of Nodes and Cross-Links per Segment

Segments	***# of nodes***	***# of cross-links***
Contest Form	13	7
Pedagogical Benefits	9	5
Participant(s)	13	5
Infrastrucutre	14	4
Preparation	5	0
Policies & Mechanisms	23	7
Sum	**77**	**28**

- "Infrastructure": depicts concepts related to the framework of the competition in terms of devices and software.
- "Preparation": involves notions related to the demands for the set-up of the competitions.
- "Policies & Mechanisms": depicts the concepts related to the rules and the processes applied to ensure the reliability and the fairness of the competitions and to perform the evaluation of the participants.

Observing Fig. 1, it can be noticed that "Policies & Mechanisms" is the most substantial and complex segment, as it involves the "Assessment" and "Reliability" sub-segments and numerous concepts, including the "Flag(s)" and "Score" concepts that have a large number of relationships. Besides, the "Policies & Mechanisms" segment has a considerable number of cross-links comprised of four relations to the "Infrastructure" segment, two to the "Participant(s)" segment, and one to the "Contest Form" segment. The segments "Policies & Mechanisms" and "Infrastructure" also share the "require" relation to the "Preparation" segment. The fact that "Policies & Mechanisms" and "Infrastructure" segments have multiple cross-links and they are both related to the "Preparation" segment is considered ordinal as the former is instantiated and applied on the devices of the latter.

Likewise, the "Contest Form" segment is a crucial factor in the implementation of live competitions as it encompasses numerous cross-links and critical elements. These elements need to be defined early in the design phase of an event, as they can affect the entire development process. More specifically, the "Contest Form" segment includes the "Scenario" concept that has an influence on the policies and mechanisms necessary to implement. It embraces two cross-links to the "Scales" and "Teams" concepts of "Participant(s)" segment that symbolize the number of contestants contributing to the event and whether they are separated in teams. Additionally, it includes the contest and attack notions that affect the pedagogical impact of live competitions ("Pedagogical benefits" node), through the formed cross-links to the "Motivation" and "Enjoyment" concepts. Finally, pedagogical benefits are also designated by the "Participant(s)" segment that includes the notion of "Teams".

B. *Identified Problems and Issues*

During the past years, various problems and issues of live competitions have been identified in the literature. We reviewed and grouped them into three categories: drawbacks in the competitions' aims, learning obstacles affecting their value, and concerns on competitions' organizational and functional issues.

1) Drawbacks in competitions' aims

a) Contests aim is to measure skills: A competition, in general, is concerned with the measurement of skills while participants acquire knowledge and skills (KSAs) in a self-directed and unstructured manner. Conversely, an educational approach in cyber security aims at a different purpose. More specifically, it aims in setting the environment and defining the processes that will guide learners to adapt by acquiring new knowledge, skills and abilities [22].

b) Fail to address the management of settings realistically: The aims of the contests are unlinked to the day-to-day management of network settings and services. Participants use ad-hoc methods and strategies and they often adopt unsuitable behaviors because they deploy extreme defense approaches. These approaches do not take into account the operational costs of the systems, i.e. amount of memory, CPU time and size of log files, and thus - in real settings - they are inapplicable. In addition, contestants often take into consideration only the initial setup of their system but they do not pay attention in keeping their system up-to-date, implementing disaster-recovery policies, and employing effective backup schemes [23].

c) Diversity of topics is not supported: Live competitions usually focus on a restricted set of topics, e.g. performing exploits or protecting vulnerable code [18], while they do not address particular subjects in their aims, e.g. threats related to the availability of resources and brute-force attacks. This happens because live competitions are limited by certain characteristics such as the duration of events or because the contest organizers are biased towards certain types of problems [10]. As a result, organizers suppress certain aspects by rule sets, e.g. intentional loss of availability, and participants do not practice in handling them [24].

2) Learning Obstacles

a) Not calibrated to participants' needs: Nowadays, there are many competition events available, some of which are oriented towards specific profiles for their participants. For example, DefCon is organized for cyber security experts that are experienced in offensive tactics, whereas CSAW (Cyber Security Awareness Week) aims at novice students new to cyber security concepts. Nevertheless, designers of competitions' challenges still face issues in deciding and adjusting the right level of difficulty. For instance, sometimes they try to create difficult challenges by making the solutions convoluted. Consequently, participants often are overwhelmed and discouraged, whereas in other cases they are not sufficiently challenged [10] [22].

b) Not an experiment environment: In competitions where participants compete against each other, there are no comparable and repeatable results related to the contestants, either as individuals or as a team. Participants do not have the opportunity to refine failed policies instantly and try different approaches to receive new feedback [24].

c) Partial credit is not supported: Scoring schemes usually assign points to the competitors, when they accomplish tasks or they do not assign points at all. By applying such policies, participants are forced to modify their approaches until they succeed [10]. However, they do not get the appropriate feedback and rewards while making progress towards their target. Moreover, they do not reinforce their positive feelings [9]. As a result, they can be discouraged and disengaged from the learning process. Furthermore, competitors tend to assess the difficulty of a challenge by the appointed score value. Since there is no partial credit, when they believe that it is difficult for their level of expertise, competitors avoid trying to solve it.

3) Competitions' organizational and functional issues

a) High demands in resources and preparation time: Competition organization demands a high number of hardware and software resources for the infrastructure. According to the scale of a particular event, a proper place is needed to host the event and weeks of preparations [18].

b) Needs for expert support personnel: Arranging a proper environment requires personnel of expertise dedicated to the event's preparation for a long period prior to the competition. Personnel, e.g. administrations and technicians [25], may also be required to support the event during its operation.

c) High quality assurance standard: Designers of live competitions need to follow strict quality assurance processes to ensure that there are no errors in the contest. Faults in the organizational structure or ambiguities in contest's challenges might interrupt event operation [10] and discourage future participation.

d) Events do not take place frequently: To mitigate the costs, organizations tend to set fewer, larger and multi-participant events rather than smaller but more frequent ones [26].

C. *Analysis scheme*

Issues of live competitions triggered the academic community to propose several approaches that attempted to utilize the merits of live competitions, mitigate the aforementioned problems and fit such events in particular educational contexts. Our study can be used to analyze new approaches and make some assumptions on their feasibility and educational impact. In the remainder of this section we refer to some recent and notable efforts from the literature, mainly aiming at decreasing demands in cost and resources required for organizing live competitions.

1) Class Capture-the-Flag exercises: Mirkovic and Peterson in [18] describe the Class Capture-the-Flag exercises (CCtFs) approach. CCtFs are small scale-attack and defense style competitions, in which students alternate between offensive and defensive roles. The exercises are conducted on

DeterLab (cyber DEfense Technology Experimental Research Laboratory) platform [40], a virtual facility which allows allocation of resources among users for the implementation of cyber security experiments. CCtFs can be repeated frequently throughout a semester and can decrease the organizational demands typically required in the preparation and operation of such events. They require a few weeks of preparation with the involvement of students instead of experts. Usually, CCtFs have a few hours duration, so that they can be arranged during classes and labs. Moreover, they provide the instructors with the option to use a wide range of scenarios that focus on versatile security topics such as cryptography, exploits, denial of service, etc. CCtFs are also facilitated with automated setup and assessment features that tolerate the least involvement of instructors during the events. Each CCtF is followed by a post-mortem analysis that helps students to better assimilate the cyber security concepts they have been taught, as well as to reflect on the strategies employed during the exercises [5].

2) Offline Capture the Flag Virtual Machine: Chothia and Novakovic [12] presented the Offline Capture-the-Flag Virtual Machine (OCtF VM) framework as part of the formative assessment of a cyber security course. According to their approach, a virtual machine is created and distributed through the web. The virtual machine hosts jeopardy style CtF challenges that students have to solve individually. Students download the virtual machine in the beginning of the semester and they employ it in their own hardware. The virtual machine has certain services pre-installed and configured, whereas specific settings are configured on its first boot, e.g. unique flags are generated for each student. As students are progressively introduced to miscellaneous cyber security topics of the university's course, they are required to solve challenges in the virtual machine. The challenges include implementing methods for decrypting files, auditing access control mechanisms, analyzing and attacking key exchange protocols, attacking web sites and reverse-engineering programs. They are usually straightforward so that cheating would be more time consuming than solving the exercises. When a student solves a challenge, she acquires a flag that she has to submit on a flag submission server. The submission server verifies the token and provides feedback instantly to the student. The results are only acknowledged to the student that made the submission, whereas some specific details, e.g. students and virtual machine identification, are recorded on the server. Students are also required to hand in reports explaining their activities for the solution of the challenges. Reports aid in reflecting on what they have accomplished and providing information to instructors in order to assess their work. At the end of the sessions, instructors mark the written reports and provide feedback to the students.

3) Tracer Fire Exercise: Researchers of Sandia National Laboratories [19] [22] describe the Tracer Fire (Forensic and Incident Response Exercise) training program. Tracer Fire is a classroom based multiday jeopardy style competition that focuses on forensics. Participants are individuals from U.S. government agencies, law enforcement, industry and universities, which work in teams of four to six, as they are required to solve realistic challenges to gain points. Challenges require contestants to use cyber security software tools, to utilize forensic analysis techniques (e.g. review server logs to identify suspicious entries) and to analyze adversary tactics. At the beginning of the event, participants are provided with laptops that have installed basic utility tools and the essential forensics software. Furthermore, participants are allowed to download additional tools and applications and install them on their laptops. The event's infrastructure is based on a specific software architecture that includes a web-based game server and a news server. The game server provides challenges to the participants, receives their answers and delivers feedback, whereas the news server makes announcements providing information relevant to the scenario of the event.

V. Results

In this section, we put the live competition approaches presented above on the test of the proposed analysis scheme. More specifically, we resolve them into their elements, identify the problems they tried to solve and appreciate their pedagogical effectiveness.

The results of our test scheme are summarized in the Table II that consists of two parts. The first part analyzes the elements of the investigated approaches with respect to the proposed concept map characteristics, depicted in Fig 1. The column "Characteristics" of the Table II contains the concept map's segments (described in the "A. Concept Map" subsection of section "IV. Conceptual Analysis") and the "Assessment" and "Reliability" sub-segments. The second part examines the effectiveness of the inspected approaches in confronting with the identified problems of live competitions presented in the "B. Identified Problems and Issues" section. In the remainder of this section, the results of our test scheme are discussed.

Live competitions are characterized by certain limitations that hold back their efficiency when they are integrated into particular educational contexts. The approaches we analyzed aim at decreasing the demands in cost and resources required for the organization of regular and durable security competitions [12]. However, our analysis proves that the problems stated earlier were mitigated by trading other attributes of live competitions. Attribute trading is notable to the OCtF VM approach. In this approach the preparation issues are solved quite effectively by minimizing the demands of preparation, as the contest's infrastructure is encompassed in a virtual machine. The "duration" and the "limitation of repetition" issues are tackled, as the exercise can last the whole semester and the presence of an instructor is not required. However, the exercise lacks the "attack" aspect, whereas the "contest" factor is downgraded because students do not interact with each other and they do not get feedback on the progress of their classmates. Subsequently, the pedagogical benefits of "enjoyment" and "motivation" are downgraded [10]. The authors in [12] rightly claim that the lack of the competition factor is useful for weaker students. Nevertheless, an optimal

TABLE II. Analysis Scheme for Live Competition Approaches

Characteristics	*CCtF*	*OCtF VM*	*Tracer Fire Exercise*
Contest Form	-Attack mode -Defense mode	Jeopardy mode	Jeopardy mode
Pedagogical benefits	-Exercise KSAs -Enjoyment and motivation -Collaboration	-Exercise KSAs -Enjoyment and motivation are downgraded due to the lack of contest and attack factors	- Exercise KSAs - Enjoyment and motivation are downgraded due to the lack of attack factor
Participants	-Students, novices to intermediates -Organized in teams -Small scale -Low to medium background prerequisite	-Students, mainly novices -Participate as individuals -Unlimited scale -Low background prerequisite	-Intermediates from U.S. government agencies, law enforcement, industry, universities -Organized in teams -Small scale -Low to medium background prerequisite
Infrastructure	-Depends on exercise's scenario -Employed on virtual settings -Requires physical co-location	-Challenges hosted in virtual machines -Virtual machines can be distributed remotely	-Fulfills a distinctive topology -Employed on physical devices -Requires physical co-location
Preparation	-Arrangements require a few weeks -Requires expert support personnel -Demands pre-installed resources -Allows frequent repetitions -The event lasts a couple of hours	-Arrangements require a little time -Some expertise is needed to prepare the challenges in the virtual machine -No resources are required as students bring their own hardware -Possibilities for unlimited duration and repetition	-Demands high preparation in all terms that limits the potential in frequency of repetitions
"Policies & mechanisms" and "Reliability"	-Depend on each exercise's scenario	-Identify participants -Different flags per challenge -Operate safely outside universities' network	-Depend on exercises' scenarios -Advanced logging capabilities
Assessment	-Custom scoring mechanisms that depend on each exercise's scenario	-Based on flag submissions and students' write-ups -Do not require instructors	-Provided by efficient scoring mechanisms
Issues	***CCtF***	***OCtF VM***	***Tracer Fire Exercise***
Contests aim to measure skills	Solved extrinsically: exercises supported by feedback and classes	Solved extrinsically: exercises supported by feedback and classes	Not solved
Fail to address the management of settings realistically	Not solved	Not solved	Not solved
Diversity of topics is not supported	Solved	Not solved	Not applicable as the exercises focus on forensics
Not calibrated to participants' needs	Solved	Solved	Solved
Not an experiment environment	Mitigated indirectly due to the fact that events can be repeated frequently	Solved	Not solved
Partial credit is not supported	Depends on exercises' scenarios and custom assessment mechanism	Mitigated extrinsically through students' reports	Supported intrinsically due to efficient assessment mechanisms
High demands in resources and preparation time	Solved	Solved	Not solved
Needs for expert support personnel	Not solved	Mitigated	Not solved
High quality assurance standard	Mitigated	Mitigated	Not solved
Events do not happen frequently	Solved	Solved	Not solved

solution would be to have a setting that contains the "attack" and "contest" ingredients with additional features that group or pair the participants according to their background and capabilities. In this a way, everyone has an opportunity to win with the appropriate scaffolding.

On the contrary, our analysis scheme clarifies that the CCtF approach preserves the qualities of live competitions that were downgraded in the OCtF VM approach. However, by contrasting the CCtF and OCtF VM approaches, we can observe that the preparation considerations have only been mitigated in the first case, the scale is set to the size of a class, the instructors' presence is required during the exercises, and ad hoc assessment methods may be used. Therefore, CCtF seems a more balanced approach but in the cost of not addressing drastically the organizational issues.

On the other side, the Tracer Fire exercise differs significantly from the OCtF VM and CCtF approaches. Tracer Fire exercises are organized for intermediate level participants that have background knowledge and experience in cyber security. They focus on the domain of forensics and they incorporate some noteworthy logging and assessment capabilities that constitute them valuable research tools. Tracer Fire relies on an elaborated software framework that facilitates its preparation arrangements by explicitly defining some elements of the infrastructure, like "topology", "competition server" and "nodes" (fig. 1). However, the issues related to the organization of the event remain unsolved, as the event arrangement demands significant resources in terms of time, physical devices and personnel of expertise. Consequently, the frequency of events is limited to once per year.

The notion of attribute trading that is derived from our scheme is identified not only in the approaches we included in the presented analysis scheme, but also in other approaches from the literature. Another fact we observed during our study is that very few works explicitly studied sound learning theories in live competitions [29], as for example experiential learning in [14]. Moreover, the lack of empirical data in the majority of the studies does not provide the ability to explicitly connect live competition characteristics with particular educational impacts.

VI. Discussion

The availability of proper means to mitigate the problems associated with live competitions could lead to essential improvement of particular educational impacts. Organizers need to reduce the demands and the logical complexity of live competitions. They also need to consider the proper learning theory their approach will embrace and utilize it to guide the entire competition design process. More specifically, they need to provide the means to create and parameterize the educational environment in order to set the conditions for an effective learning process. In this way, the assessment and feedback factors will be better facilitated. Moreover, live competitions need to adapt to the learners' knowledge, capabilities and expectations and to provide scaffolding facilities to contestants. Hence, we argue that the unstructured nature of current approaches does not help to better facilitate these features and effectively deal with their challenges without trading other significant attributes. The comparative analysis elaborated in this work provides a proof of this concept, as well as indicative directions for its utilization in the phases of analysis, feasibility study and assessment for the development of successful live competition approaches.

VII. Conclusion

While cyber security education attracts more attention, new teaching and training approaches are developed and tested. Live competitions domain is an essential part of cyber security education that has been employed in relevant contexts in the last decade. In this work, we identified the lack of conceptual models that facilitate the comprehension and analysis of such approaches and their pedagogical effectiveness. We also stressed the lack of using pedagogical theories in the foundations of the majority of live competition approaches. After a thorough review of the literature in the live competitions field, we recorded a number of related problems, we created a concept map of live competition technological and pedagogical characteristics and we derived an analysis scheme by resolving and comparing three notable approaches of live competitions. Finally, we reflected on our observations and results and made assumptions that offer an appreciation of the field's potentials and limitations. The presented analysis scheme can be put into effect in the development of new live competition approaches and the produced deductions can be used in the development of new pedagogical methodologies relative to the concept of live competitions, e.g. gamification and game based learning [41].

References

[1] C.team, "Ctftime.org / all about ctf (capture the flag)," 2016. [Online]. Available: https://ctftime.org/ctf-wtf/

[2] B.A. Bratosin, "Cyber Defense Exercises and their Role in Cyber Warfare," Journal of Mobile, Embedded and Distributed Systems 6, no. 2, 2014, 70-76.

[3] G. Vigna, K. Borgolte, J. Corbetta, A. Doupe, Y. Fratantonio, L. Invernizzi, D. Kirat and Y. Shoshitaishvili, "Ten years of ictf: The good, the bad, and the ugly," in 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.

[4] R.S. Cheung, J.P Cohen, H.Z. Lo, F. Elia, and V. Carrillo-Marquez, "Effectiveness of cybersecurity competitions," in Proceedings of the International Conference on Security and Management (SAM), p. 1, The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012.

[5] J. Mirkovic, A. Tabor, S. Woo, and P. Pusey, "Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015," in 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15), 2015.

[6] A. Davis, T. Leek, M. Zhivich, K. Gwinnup, and William Leonard, "The Fun and future of CTF," in 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.

[7] A. Doupé, M. Egele, B. Callait, G. Stringhini, G. Yakin, A. Zand, L. Cavedon, G. Vigna, "Hit'em where it hurts: a live security exercise on cyber situational awareness," Proceedings of the 27th Annual Computer Security Applications Conference, ACM, 2011.

[8] Childers, N., Boe, B., Cavallaro, L., Cavedon, L., Cova, M., Egele, M., and Vigna, G., "Organizing large scale hacking competitions," in International Conf. on Detection of Intrusions and Malware, and Vulnerability Assessment, pp.132-152, Springer Heidelberg, 2010.

[9] A. Dabrowski, M. Kammerstetter, E. Thamm, E. Weippl, and W. Kastner, "Leveraging Competitive Gamification for Sustainable Fun and

Profit in Security Education," in 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15), 2015.

[10] K. Chung, and J. Cohen, "Learning Obstacles in the Capture The Flag Model," in 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.

[11] J. Werther, M. Zhivich, T. Leek, and N. Zeldovich. "Experiences in cyber security education, The mit lincoln laboratory capture-the-flag exercise," in The 4th Workshop on Cyber Secuirty Experimentation and Test, San Francisco, CA, United states, 2011.

[12] T. Chothia and C. Novakovic, "An Offline Capture The Flag-Style Virtual Machine and an Assessment of its Value for Cybersecurity Education," in 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15), 2015.

[13] M. Carlisle, M. Chiaramonte and D. Caswell, "Using CTFs for an Undergraduate Cyber Education," in 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15). 2015.

[14] A. Rege, "Multidisciplinary Experiential Learning for Holistic Cybersecurity Education, Research and Evaluation," in USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15), 2015.

[15] A. Konak, T.K. Clark and M. Nasereddin, "Using Kolb's Experiential Learning Cycle to improve student learning in virtual computer laboratories," Computers & Education 72 (2014): 11-22.

[16] P. Pusey, D. Tobey Sr and R. Soule, "An Argument for Game Balance: Improving Student Engagement by Matching Difficulty Level with Learner Readiness," in 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.

[17] B. Mauer, W. Stackpole and D. Johnson, "Developing Small Team-based Cyber Security Exercises," in Proceedings of the International Conference on Security and Management (SAM), p. 1, The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012.

[18] J. Mirkovic, & P.A. Peterson, "Class capture-the-flag exercises," in 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.

[19] J. McClain, A. Silva, G. Emmanuel, B. Anderson, K. Nauer, R. Abbott, and C. Forsythe, "Human performance factors in cyber security forensic analysis," Procedia Manufacturing 3, 2015, pp.5301-5307.

[20] V.V. Patriciu and A.C. Furtuna, "Guide for designing cyber security exercises," in Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy, pp. 172-177. World Scientific and Engineering Academy and Society (WSEAS), 2009.

[21] T. Sommestad and J. Hallberg, "Cyber security exercises and competitions as a platform for cyber security experiments," in Nordic Conference on Secure IT Systems, pp. 47-60. Springer Berlin Heidelberg, 2012.

[22] A. Silva, J. McClain, T. Reed, B. Anderson, K. Nauer, R. Abbott and C. Forsythe, "Factors impacting performance in competitive cyber exercises," Proceedings of the Interservice/Interagency Training, Simulation and Education Conference, Orlando FL, 2014.

[23] L. Catuogno and A. De Santis, "An internet role-game for the laboratory of network security course," in ACM SIGCSE Bulletin, vol. 40, no. 3, pp. 240-244, ACM, 2008.

[24] S. Koch, J. Schneider and J. Nordholz, "Disturbed Playing: Another Kind of Educational Security Games," in Proceedings of the 5th USENIX conference on Cyber Security Experimentation and Test, USENIX Association, Berkeley, CA, USA, 2012.

[25] L.J. Hoffman, T. Rosenberg, R. Dodge and D. Ragsdale, "Exploring a national cybersecurity exercise for universities," IEEE Security & Privacy 3, no. 5 (2005): 27-33.

[26] P.D. Allen and K.A. Straub, "Using Games to Enrich Continuous Cyber Training," Johns Hopkins APL Technical Digest, vol. 33, no 2, 2015.

[27] P. Sroufe, S. Tate, R. Dantu and E.C. Cankaya, "Experiences During a Collegiate Cyber Defense Competition," Journal of Applied Security Research 5, no. 3 (2010): 382-396.

[28] M. Mink and R. Greifeneder, "Evaluation of the offensive approach in information security education," in International Information Security Conference (IFIP), pp. 203-214. Springer Berlin Heidelberg, 2010.

[29] B. Martini and K.K.R. Choo, "Building the Next Generation of Cyber Security Professionals," Proceedings of Twenty Second European Conference on Information Systems, Tel Aviv, 2014.

[30] W.C. Feng, "A Scaffolded, Metamorphic CTF for Reverse Engineering," in 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15), 2015.

[31] W.J. Adams, E. Gavas, T.H. Lacey and S.P. Leblanc, "Collective Views of the NSA/CSS Cyber Defense Exercise on Curricula and Learning Objectives," in Proceedings of the USENIX Workshop on Cyber Security Experimentation and Test (CSET 2009), August 2009.

[32] Y. Bei, R. Kesterson, K. Gwinnup and C. Taylor, "Cyber defense competition: a tale of two teams," Journal of Computing Sciences in Colleges 27, no. 1 (2011): 171-177.

[33] R.L. Fanelli and T. O'Connor, "Experiences with practice-focused undergraduate security education," in Proceedings of the 3rd Workshop on Cyber Security, Washington, DC, United states, 2010.

[34] T. Flushman, M. Gondree and Z.NJ. Peterson, "This is not a game: early observations on using alternate reality games for teaching security concepts to first-year undergraduates," in 8th Workshop on Cyber Security Experimentation and Test (CSET 15), 2015.

[35] E. Gavas, N. Memon and D. Britton, "Winning cybersecurity one challenge at a time," IEEE Security and Privacy 10, no. 4 (2012): 75-79.

[36] S.M. Glumich and A.B. Kropa, "DefEX: Hands-On Cyber Defense Exercise for Undergraduate Students," in Proceedings of the 2011 International Conference on Security and Management (SAM'11), July 2011, USA.

[37] A.J. Cañas, G. Hill, R. Carff, N. Suri, J. Lott, T. Eskridge, G. Gómez, M. Arroyo and R. Carvajal, "CmapTools: A knowledge modeling and sharing environment," in Concept maps: Theory, methodology, technology, Proceedings of the first international conference on concept mapping, vol. 1, pp. 125-133. 2004.

[38] J.D. Novak and A.J. Cañas, "The theory underlying concept maps and how to construct and use them," IHCM Technical Report Cmap Tools 2006-01 Rev 01-2008 Florida Institute for Human and Machine Cognition, 2008.

[39] K.M. Markham, J.J. Mintzes and M.G. Jones, "The concept map as a research and evaluation tool: Further evidence of validity," Journal of research in science teaching 31, no. 1 (1994): 91-101.

[40] J. Mirkovic and T. Benzel, "Teaching cybersecurity with DeterLab," IEEE Security & Privacy 10, no. 1, pp. 73-76, 2012.

[41] P. Chapman, J. Burket and D. Brumley, "PicoCTF: A game-based computer security competition for high school students," in USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.