IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 28 February 2024, accepted 29 May 2024, date of publication 3 June 2024, date of current version 10 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3408685

RESEARCH ARTICLE

tCOFELET: Conceptual Framework for Team-Centric e-Learning and Training

MENELAOS N. KATSANTONIS, ATHANASIOS MANIKAS, IOANNIS MAVRIDIS, AND PANAGIOTIS FOULIRAS

Department of Applied Informatics, University of Macedonia, 546 36 Thessaloniki, Greece

Corresponding author: Panagiotis Fouliras (pfoul@uom.edu.gr)

The publication of the article in OA mode was financially supported by HEAL-Link (Hellenic Academic Libraries Link).

ABSTRACT Despite the advancements in cyber security serious gaming, team-centric approaches have not been explored and the effectiveness of such approaches remains largely untapped. In this light, the main design trends and considerations of multiplayer and collaborative serious games are analyzed, along with weaknesses we identified in the field. Based on this analysis an extension of the Conceptual Framework for eLearning and Training is introduced, named Conceptual Framework for Team-Centric eLearning and Training (tCOFELET). The tCOFELET framework emphasizes the significance of team-centric learning and training and proposes a structured gameplay involving the distinct collaborative phases in planning, performing actions, and reflecting on achievements. tCOFELET integrates COFELET's main elements along with new concepts aiming to create immersive and engaging learning experiences that convey technical knowledge with practical application of skills and development of soft skills such as communication, teamwork, and strategic thinking. Based on the tCOFELET framework a blueprint of a prototype collaborative cybersecurity serious game was elaborated, named mHackLearn. A systematic presentation of mHackLearn's design, analyzed under the prism of the Activity Theory Model for Serious Games (ATMSG), is presented. Finally, a preliminary evaluation of the mHackLearn's game design is performed providing an initial estimation of its potential impact. The findings of the evaluation show that mHackLearn seamlessly integrates several key design considerations of collaborative games, providing promising insights into the tCOFELET's capability to facilitate effective team-centric cybersecurity serious game approaches.

INDEX TERMS Cybersecurity, serious games, design methodology, education, training threat modeling, e-learning, multiplayer, collaboration, COFELET.

I. INTRODUCTION

In the aftermath of the new digital age, the sector of cyber security needs to be strengthened to face the global concerns, resulting from cyber threats that have become progressively sophisticated and pervasive. Addressing these threats requires not just technical solutions, but an educated population, and the appropriate cyber security workforce equipped with the requisite knowledge and skills to face cyber adversities. The US National Institute of Standards and Technology [1] emphasizes the critical role of security training, noting that the security of resources is as much a human issue as it is a technological one.

Against this backdrop, serious games have emerged as valuable educational tools in cyber security education demonstrating their effectiveness in engaging learners in this complex domain. Frameworks like the Conceptual Framework for eLearning and Training (COFELET) [2] have guided the development of single-player cybersecurity serious games, assessing their impact and efficacy. However, despite these

The associate editor coordinating the review of this manuscript and approving it for publication was Jon Atli Benediktsson.

advancements, the exploration of multiplayer and collaborative gaming in cyber security education has been limited. The potential of multiplayer serious games in cyber security education remains largely untapped, particularly in fostering team-based learning, collaboration, and competition. These key aspects can significantly enhance the effectiveness of cyber security education, yet the complexity of developing enjoyable, immersive, and pedagogically sound multiplayer games poses many challenges.

Collaborative learning, grounded in Vygotsky's theory of the zone of proximal development, suggests that learners acquire knowledge and skills more effectively together than individually. This approach encourages the formation of small communities of practice, in which learners engage in mutual knowledge sharing, building a collective understanding of cyber security risks, threats, and responsibilities. Within these communities, learners are motivated through active participation and equal task distribution, integrating communication and collaboration into the game mechanics.

Based on these insights, we propose the tCOFELET framework, an extension of the existing COFELET framework, designed to advance the development and deployment of multiplayer serious cyber security games. The proposed framework aims to establish a comprehensive and multifaceted framework dedicated to the design and deployment of multiplayer serious cyber security games. Central to the tCOFELET framework is a set of key elements that must be considered for the creation of multiplayer cyber security serious games.

The methodology for developing the tCOFELET framework employed the Design-Based Research (DBR) [3] principles. Initially, a review of the literature on multiplayer and collaborative games was performed resulting in the identification of design considerations proposed for such games. Then, a thorough examination of the COFELET ontology and the COFELET-complaint games (i.e. HackLearn [4] and SCIPS [5]) was conducted, under the prisms of identifying key concepts that can be enhanced to advance the existing framework, and the formulation of new concepts that can innovatively foster the aspects of multiplayer and collaboration. This phase set the foundation for the design of prototype scenarios for three tCOFELET-compliant games with different game genres. Following the initial design phase, an iterative cycle of analysis, design, implementation, and evaluation was applied to the components of the prototype games and scenarios along with elements of the tCOFELET framework. Feedback from these cycles was utilized for the refinement and improvement of the tCOFELET framework, the prototype games, and scenarios, ensuring alignment with current needs.

II. BACKGROUND

A. THE COFELET FRAMEWORK

The Conceptual Framework for e-Learning and Training (COFELET) [2], is a design standard for the enhancement of cyber security education by guiding the development of effective game-based approaches, such as serious games. The framework proposes the employment of well-known cyber security standards, such as MITRE's CAPEC, MITRE's ATT&CK, and Lockheed Martin's Cyber Kill Chain model, to organize educational environments that model cyber-attacks, learners' actions, and attack strategies. Part of the framework is the COFELET ontology, which provides an analytical description of the key elements of COFELET-compliant serious games, along with the appropriate classes and their properties. These elements include elements of the cyber security domain that model the actions of attackers when they unleash cyber-attacks and employ strategies to achieve their malicious objectives; and educational elements that provide the means to infuse didactics into COFELET-compliant approaches [6], [7]. The COFELET framework involves the Gaming, Learning, and Instructional perspectives. The Gaming perspective focuses on the game mechanisms and the design elements that create an engaging and enjoyable experience for learners. Such elements are the roles, the characters, and the rewards. The Learning perspective emphasizes the delivery of effective learning and training, and it includes elements such as the educational content, the learning objectives (LOs), the underlying instructional strategy, and the assessment method. The Instructional perspective focuses on the principles that support the learning process incorporating elements such as feedback and scaffolding, which effectively support learners in developing their knowledge and skills and in achieving the learning objectives.

The primary element of the COFELET framework is the task representing user actions directed at the fulfillment of goals and the unleashing of cyber-attacks. Tasks are organized into Scenario Execution Flows (SEFs) elements, which determine the sequence of tasks users must perform to achieve their goals. Tasks are a subset of Actions that are all the actions that take place in COFELET-compliant approaches, and they are not prescribed in SEFs. The condition elements are the prerequisites that must occur to make the tasks performable, whereas the goal elements are the aims the task sequences achieve. Composite COFELET scenarios consist of stages named steps. Each step is associated with a sub-goal, a set of conditions, a set of learning objectives (LOs), and a sequence of hints [7].

B. PEDAGOGICAL FOUNDATIONS

Social constructivism theories emphasize learning within a socio-cultural context, in which individuals interact, communicate, and engage in activities cooperatively. In such socio-cultural settings, an individual can acquire and construct knowledge and skills with the assistance of the environment, which would be infeasible to achieve alone [8]. Social constructivism theories often focus on situated learning through the joint participation of individuals in communities of practice [9]. Such communities are significant, as they support learning through social interactions and the sharing of

practices in the process of acquiring knowledge and abilities [10]. A community of practice is a learning partnership related to a domain of practice, differing from a team, which is a task-oriented partnership defined by a joint task that members must accomplish together [11]. A community of practice is characterized by three dimensions: i) mutual engagement, referring to how members of the community build relationships, share knowledge, and perform joint activities; ii) joint enterprise, referring to the collective understanding of the community's goals, responsibilities, and mission; iii) shared repertoire, referring to a set of communal resources such as tools, artifacts, procedures, knowledge, skills, and terminology.

Multiplayer serious games can be viewed as constructivist activities, as they embody specific meanings, experiences, and relationships in particular contexts [12]. However, multiplayer serious games not only engage learners in collaborative but also in competitive and cooperative contexts. *Competitive serious games* involve direct or indirect conflicts (e.g., through the gain of points or resources) and are often enhanced by social features such as the dissemination of results and scores. *Cooperative serious games* employ the cooperative learning approach, in which tasks are divided into subtasks, assigned to learners, and each learner is responsible for playing a part in the solution. At the end of the process, the subtasks are combined into a joint output [13]. Thus, cooperative serious games employ an approach, in which learners have common goals, but their tasks and sometimes the rewards are not equally distributed. On the other hand, *collaborative serious games* are based on collaborative learning which focuses on the potential that shared group processes have for learning by merging individual and social processes [13]. Collaborative serious games involve common goals, rewards, and penalties, and they focus on providing interdependent experiences in which all learners contribute equally to the achievement of goals [14], [15]. The achievement of goals in such games is aligned with learners performing collaborative problem-solving activities to achieve the learning objectives and to face the game's challenges that cannot be successfully or efficiently completed by only one individual. However, collaborative learning is not homogenous or predictable, and it does not necessarily occur simply by putting learners together [16]. Continuous and conscious efforts have to be made towards the coordination of communications and activities concerning the common resources (e.g., shared knowledge) [16].

A subset of modern cooperative games are the *semi-cooperative games* in which learners share common goals, while also pursuing individual goals [17]. In such games, the team can fail to meet the common objectives, and individual team members can emerge as winners. In some cases, individuals can even try to provoke failure in the achievement of the team's goals, e.g., by tricking the rest of the team or misguiding them. Semi-cooperative approaches result in socially dynamic scenarios within the games' contexts, as they effectively simulate real-life situations, in which employees work secretly for third parties (e.g., competitors, corporate spies). Besides, such approaches combine aspects of cooperation and competition games, reflecting the multifaceted nature of real-world cases and scenarios.

III. LITERATURE REVIEW

A. MULTIPLAYER SERIOUS GAMES

The design and development of multiplayer serious games is a difficult process, as such games must be enjoyable, immersive, and, appealing; they must effectively govern the interactions of learners, their social roles, and the group dynamics ([18] as cited by [19]); and they must seamlessly merge learning and gaming aspects along with the pedagogy aspect [20]. In the remainder of this section, the design considerations of multiplayer and collaborative serious games are presented as a means of analysis and comprehension of the main trends of the field. The presented considerations include design guidelines, collaborative mechanics, tips for the creation of strong teams, and types of roles.

Researchers of Wendel et al. [20] combined in their study, the design concepts of collaborative learning and multiplayer game design and defined the following design guidelines for the development of collaborative multiplayer serious games. The guidelines are based on the mechanisms [21] and the components of collaborative learning [22]:

- *Common Goal/Success:*
  The achievement of the game's goals must mean success for all players.
- *Heterogeneous resources:*
  Players should not be able to succeed alone. Each player must have a unique resource (heterogeneous resource), such as a tool or an ability, that will allow them to perform game tasks that other players cannot perform.
- *Refillable personal resources:*
  The game should include refillable resources that decrease during gameplay.
- *Collectable and tradeable resources:*
  The game context ought to include the resources necessary for the players to achieve the game's goals. The resources need to be exchangeable through a trading system, fostering opportunities for negotiation and collaboration.
- *Collaborative tasks:*
  The game should involve collaborative tasks that are only doable if players perform them together. Collaborative tasks may involve the game's heterogeneous resources to create a need for certain players to participate in team tasks. This will trigger collaboration among players and communication.
- *Communication:*
  Communication is an essential mechanism of collaborative serious games. Communication is achieved through video, voice, or text-based chatting channels. Voice and video communication are more convenient than text-based chatting for players, whereas text-based

chatting is better for monitoring and evaluating players' communication. Communication can also include non-verbal contact through gestures and expressions, which promotes supportive interactions such as encouraging and appraising teammates [23].

- *Feedback facility:*
  A feedback system (e.g., scoreboard) should help evaluate the team's performance along with players' contributions. For example, players' scores aim to motivate player contributions to the team in an apparent manner.
- *In-game help system:*
  A help system is required to scaffold players' efforts. A sophisticated manner to provide help in a collaborative serious game is by including non-player characters (NPCs).

Oksanen and Hämäläinen [24] studied the conditions for the creation of collaborative learning and how players' actions can be structured to boost social interaction and collaborative activities. They propose the main game mechanics, which can foster collaboration among learners, presented below.

- *Complementary actions*:
  Complementary actions require learners to synchronize individual tasks for a joint outcome, creating interdependence and emphasizing each learner's critical role in problem-solving. This mechanism necessitates learners being aware of their own and others' situations and states of mind.
- *Indirect actions*:
  Indirect actions involve scenarios where one learner receives information or a task that requires another learner's action, requiring two or more players for successful completion. An example of this mechanic is a blind learner who moves an avatar based on other learners' instructions, fostering communication, information exchange, and joint understanding of the task for the achievement of the goal.
- *Encrypted information*:
  Encrypted information is the unique knowledge necessary for the achievement of the goal. This mechanic encourages players to share their knowledge to build a shared understanding. An example of this mechanic is involved in a game where learners collaboratively gather information to answer questions correctly. Apart from the collaboration, encrypted information also promotes individual accountability, keeping learners focused and not letting them be lazy (i.e., free-ride players). Besides, this mechanic ensures that players are aware of each other's knowledge and mental states, forming the foundation for new shared knowledge.

Regarding the roles of learners in collaborative approaches, generally, there are two perspectives: the scripted roles and the emergent roles [19]. The scripted roles involve the structuring of learners' activities in advance to prompt the collaborative learning process [25]. Such activities include elaborations (e.g., making analogies, predicting outcomes, visualizing), explanations, argumentations, and question-asking [25]. Usually, each learner is assigned a specific role that is associated with a single task or responsibility. The emergent roles involve the development of flexible roles that learners develop spontaneously. Emergent roles emerge during the interaction of the learners with their teammates, without any role assignment or instruction being provided in advance by an external agent such as an instructor or a teacher [26].

B. MULTIPLAYER HOBBY GAMES

In this subsection some design recommendations for multiplayer hobby games also considerable in multiplayer serious games are explored. Recommendations that were not presented in the previous section are presented in the remainder of this section along with the manner they can be realized in the collaborative multiplayer serious games.

Schell [27] explored the creation of strong communities and presented several tips, some of which are also applicable to the formation of strong teams of learners in multiplayer serious games:

- *Conflict:*
  Games must include a form of conflict, as it can play a central role in the creation of a strong team. A conflict in a collaborative serious game means the learners working against the game's mechanisms or a team of adversaries (e.g., real or NPCs).
- *Create shared property:*
  The creation of shared properties (e.g., objects, artifacts) that do not belong to an individual learner can create bands among learners.
- *Self-expression:*
  Self-expression is an important factor in multiplayer serious games. When learners are required to present knowledge, skills, and attitudes through conversations, strategies, styles of play, editing of avatars, etc., they learn more effectively.
- *Support at least three levels of experience:*
  Multiplayer serious games must be designed for at least three levels of experience i.e., the newcomers to the team, the learners who comprehend the game mechanisms and activities, and the learners who have already achieved the game's goals and have already gained the benefits the game has to offer.
- *Team management:*
  A game must include the appropriate system and tools to let learners communicate and organize their activities.
- *Events:*
  Events can foster shared experiences among learners encouraging their banding. Events usually indicate significant moments in the game's timeline in which distinct incidents happen. Events remain memorable to learners, and they foster a sense of expectation by providing something to look forward to.

Tekinbas and Zimmerman in the chapter 'Games as Social Play' [28] explore games as social phenomena along with associated concepts that can be considered for the design of multiplayer and collaborative serious games such as social dynamics, player roles, and player communities:

- *Flexibility in Roles*:
  Multiplayer games involving dynamic shifts in learners' roles can foster a higher degree of engagement and immersion as they reflect more realistically social interactions.
- *Interactions*:
  Games should consider both the interactions that emerge naturally from the game's rules (internal interactions) and those that learners bring with them into the game from outside the game (external interactions). For example, in a multiplayer serious cyber-war game internal interactions refer to learners that assume the role of the blue team members (defenders), while another group of learners assumes the role of the red team members (attackers). On the other side, external interactions can refer to external social contexts or pre-existing friendship or rivalry interactions.
- *Meaningful Social Play*:
  Games should consider mechanisms that encourage learners to manipulate and transform their relationships with their teammates. This involves designing tasks that require collaboration, cooperation, semi-cooperation, and competition, thereby fostering a good repertoire of social interactions.
- *Community Building*:
  Designers should recognize the importance of communities formed for and because of the game. Design features, such as shared goals and events, should be considered under the prism of encouraging community building within the game's context.

Zagal et al. [18] analyzed a popular collaborative board game and highlighted the importance of selfless actions (i.e., actions that promote the interest of the team), over selfish actions which promote the interest of individual players in the context of collaborative games. Players need to be free to perform actions without the consent of their teammates and to have the chance to reflect on how their decisions affect the team's performance. An individual player should not be able to make decisions for the team.

C. IDENTIFIED ISSUES

1) HIGH INTERDEPENDENCY IN ROLES

In multiplayer serious games learners are assigned different scripted roles, which help them take on identities in the context of the game. Examples of such roles are the penetration tester presented in [7], or the attackers and defenders of a cloud system [29]. These roles are interdependent [30] and asymmetric in terms of abilities (i.e., a learner can perform actions others cannot), challenges (i.e., faced challenges depend on the roles), information (i.e., learners know different information) and responsibilities (i.e., learners pursue different goals) [31]. During gameplay, learners will have to play their part according to their role. The skills and efforts of each learner must be combined for the achievement of the game goals [30]. The pitfall of adopting highly interdependent roles is that collaboration between learners is not fostered in the games' mechanisms and it is downgraded. When the team faces challenges in the game, only specific learners will have to act according to their roles. For example, in the 'CSRAG' card-based game presented in [32], the users perform attacks according to their attacker role (i.e., network, social engineer, or physical attacker), whereas in the Escape from Wilson Island game presented in [20], the learner with the axe will get wood to build a hut, raft or fire. Likewise, in a hands-on hacking simulator (e.g., the HackLearn [4]), the learner assuming the role of a penetration tester will utilize appropriate resources (e.g., the Nmap tool) to perform port scanning actions on a network's host. Thus, when a learner applies their expertise to face the challenges of the scenario, the rest of the team members usually do not play an active role. More importantly, learners do not have the chance to practice knowledge and skills by performing activities alongside more experienced learners [10], as learners do not need the contribution of other team members to achieve the scenario's challenges. Conclusively, discussion, communication, and collaboration are not infused in the game's mechanisms.

2) ROLE ALIGNMENT WITH REAL-WORLD CONTEXTS

Another pitfall of multiplayer cyber security games is the detachment of learners' game roles from the activities they perform in their real-world environment. For example, in several serious cyber security awareness games (e.g., [29], [32], [33]) learners adopt the roles of attackers or defenders, although in real life they are students or employees who do not perform cyber-attacks, or it is not their responsibility to respond to these attacks. However, multiplayer educational approaches are more effective when they adopt the contextual learning paradigm [34] and assume roles associated with the activities they perform in real life. Besides, training aims to focus on fostering skills directly related to the trainees' jobs and responsibilities in their professional environments [35].

3) LACK OF STUDIES FOR COMMERCIAL GAMES

There is a gap between multiplayer serious games developed in academia and commercial hobby multiplayer and collaborative games produced in the industry [36]. Although commercial games have evolved drastically in the past decades, very few studies on serious games have systematically incorporated non-academic approaches in their scope. We argue that studying the collaborative mechanisms of commercial games and assessing their impact is critical for the evolvement of the serious games field. This is particularly important in certain domains of serious games (e.g., cyber

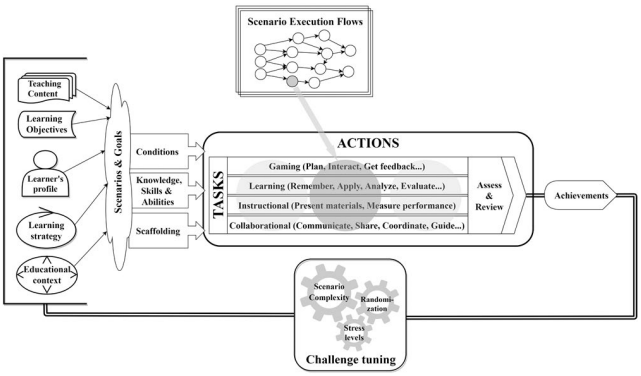


FIGURE 1. The tCOFELET framework.

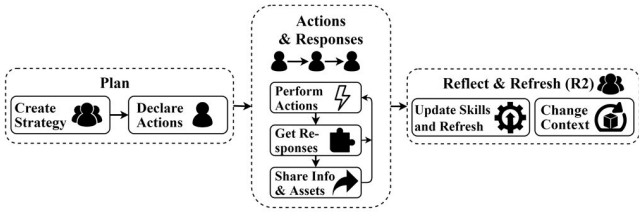


FIGURE 2. Phases of a tCOFELET round.

security awareness games), as the acceptance of design considerations of modern commercial games can result in wider reach and acceptance in civil society [36].

IV. THE PROPOSED FRAMEWORK

In this section, the tCOFELET framework is presented as a means to enhance the development of effective collaborative serious games, particularly proposed for cyber security learning and training. The elaboration of such a framework is necessary due to the lack of methodological frameworks on the concept and components of collaborative learning [37]. tCOFELET (Fig. 1) extends the COFELET framework by incorporating the appropriate elements that can foster collaboration and incorporate the design considerations presented in the previous section. Thus, includes the perspectives of the original COFELET framework, along with the additional Collaborational perspective.

In the Collaborational perspective, the emphasis is put on group dynamics, shared understanding, collaborative problem-solving, and the achievement of common goals. The guiding questions for the analysis and design of the game shift from "*Who is the player/learner?*" and "*What are the learning objectives of the game?*" [38] to "*Who are the members of the team?*" and "*Why do learners engage as a team in the game?*". The Collaborational perspective involves actions that foster communication, discussion, negotiation, debate, sharing, coordination, and guidance in such approaches. Learners are divided into small groups facilitating communication and sharing of knowledge. These groups are conceptualized as communities of practice [10], which, for simplicity, will be referred to as *teams*.

In tCOFELET approaches, learners adopt roles and execute actions similar to those of the original COFELET framework. However, tCOFELET further introduces new concepts and features, which it is recommended to consider when designing collaborative mechanisms in compliant approaches. The gameplay is structured in Rounds and Phases in which learners perform activities and they receive responses according to their collaborative roles and the policies they have. Actions are subject to action limits that represent real-world resource constraints, encouraging strategic planning and teamwork. Actions are also executed by NPCs regularly (e.g., in each round) or occasionally.

A. ROUNDS & PHASES

Learners perform their tasks in Rounds. A *Round* involves the execution of multiple tasks and the fulfillment of several steps. A Round consists of distinct phases of Plan, Action, Response, and Reflect & Refresh (R2) (as depicted in Fig 3). *T*he activities of the Collaborational perspective are actions, as they are not directly related to SEFs. For this reason, in the remainder of the paper, the term *actions* is used in a general way representing both the tasks (prescribed in the SEFs) and the actions not related to SEFs.

In the *Plan* phase, the objective is to elaborate the plan for the following round. To do so, learners must comprehend the scenario's goals and context, and perform the activities of communication, discussion, negotiation, debate, and strategy planning. To motivate all team members to actively participate in the planning phase, tCOFELET proposes to specifically declare the tasks or actions they will perform and limit their resources (e.g., preserve resources and tools).

The Action and Response phases occur sequentially for each learner. The *Action* phase includes the execution of tasks according to occurring conditions. The learner who takes the current turn is the active learner. Generally, actions are performed individually by active learners, though some actions (presented in subsection III-C) can be executed simultaneously by two or more learners.

The *Response* phase involves executing actions in response to the learners' actions. This phase may include counter-actions performed by adversary teams (non-playable characters or learners) or scenario entities (e.g., hosts). To enhance knowledge sharing and communication, tCOFELET proposes that full details of the scenario's context are disclosed exclusively to the active learner, while non-active learners perceive changes in the context in a more abstract manner. Such details include information about new entities (e.g., IPs of alive hosts on the target network), targets' vulnerabilities, assets (e.g., devices, files), and documents. For instance, in a host discovery attack performed in a hacking simulator, the active player identifies new hosts along with their IPs and hostnames, whereas non-active players are aware that new hosts have been discovered (e.g., shown in a graphic representation) but they do not receive further details (e.g., actual IPs, hostnames, etc.). Similarly, in a tabletop

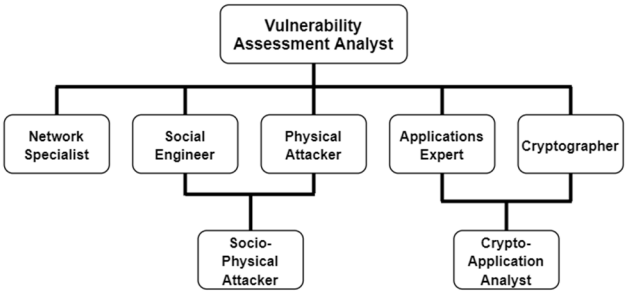


FIGURE 3. Roles hierarchy example.

exercise, the active learner receives cards and tokens that must be shared with the rest of the team.

The *R2* phase involves realizing the scenario's context because of tasks performed in the Action phase. The R2 phase also includes the change of context through the triggering of the round's post-conditions, the execution of events, and the disclosing of new entities and goals. In the R2 phase, learners refresh their resources (e.g., resources they can spend), upgrade, unlock, or lock their roles, and update their skills.

B. ROLES

tCOFELET utilizes the hierarchy of roles of the COFELET ontology [6], [7]. However, the proposed extension foresees the definition of multiple sibling roles that share tasks, knowledge, skills, and abilities (KSAs). For example, in a collaborative scenario, the role of the "Vulnerability Assessment Analyst (VAM)", according to the NCWF v.2 [1] "*performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy*", consists of the sibling sub-roles of Network Specialist, Social Engineer, Physical Attacker, Applications Expert and Cryptographer (Fig. 3). Although, these sub-roles include some distinct tasks and KSAs (e.g., the cryptographer has "*knowledge of cryptography and cryptographic key management concepts*"), the sub-roles of VAM share a common set of KSAs such as the "*knowledge of cyber-attack stages*" (K0177), "*skill in the use of penetration testing tools and techniques*" (S0051), and the "*ability to apply cybersecurity and privacy principles to organizational requirements*" (A0123).

Moreover, a key feature of tCOFELET is that in collaborative composite scenarios, learners can assume multiple roles. Current roles can be upgraded by inheriting tasks and KSAs from multiple roles (i.e., going down in the roles hierarchy), roles can be locked, and new roles can be unlocked. For example, during a scenario the learner assuming the "Applications Expert" sub-role can upgrade to the "Crypto-Application Analyst" by inheriting the KSAs of the "Cryptographer" sub-role (Fig. 3). In such a way, learners acquire progressively and more effectively the knowledge and skills of the VAM.

C. ACTIONS

In COFELET approaches, actions are performed by agents (e.g., learners, NPCs,) and non-agent subjects (e.g., tools) on scenarios' entities [6]. Entities are distinct entities that lie in the context of the scenario, such as the company's building networks, firewalls, hosts, and file systems. In the remainder of this section, tCOFELET introduces new key concepts and features associated with the actions presented.

- *Actions Limits:*
  Learners' actions are subject to action limits determined by the mechanisms and the scenario of an approach. These limits restrict the number or types of actions learners are allowed to perform in a single round. For example, game mechanisms may specify limits based on the number or types of actions learners are allowed to execute, or they may assign cost limits and specific costs to each action a learner undertakes. The types of actions can be categorized according to the kind of the action (e.g., attack, defend, or neutral actions), the tactic they employ according to the MITRE ATT&CK (e.g., reconnaissance, initial access, etc. [39]), or the mitigation strategy. Each scenario can specify different Action Limits, allowing to adjust the difficulty of scenarios. Action limits are an important concept that must be carefully considered by game designers, as they reflect the reality that individuals have limited resources [29]. In such a way, learners must make plans, prioritize, and coordinate their actions.
- *Sharing actions:*
  They are usually performed by active learners to pass around information and assets. Active players are expected to share information, credentials, and files they acquire during the Action phase.
- *Synchronous actions:*
  They are performed in parallel allowing learners to synchronize their actions during one or more rounds. For example, learners of a team can perform identical tasks by employing DOS attack patterns. Synchronous actions can also be *condition-triggering actions*, which temporarily activate or deactivate conditions. A condition-triggering action allows learners to temporarily prompt conditions (e.g., up to the end of the round) and provide teammates the opportunity to perform actions. For example, a learner can draw an employee's attention to allow a teammate to plug a USB device into the employee's computer.

D. POLICIES

It is a central concept of tCOFELET specifying the way learners and NPCs perform actions or the sequence of actions that must be performed to fulfill prescribed activities. For example, the "Strong Password" policy specifies that a strong password must include more than 12 letters and a unique combination of upper-case and lower-case letters, numbers, punctuation symbols, and special symbols. A learner

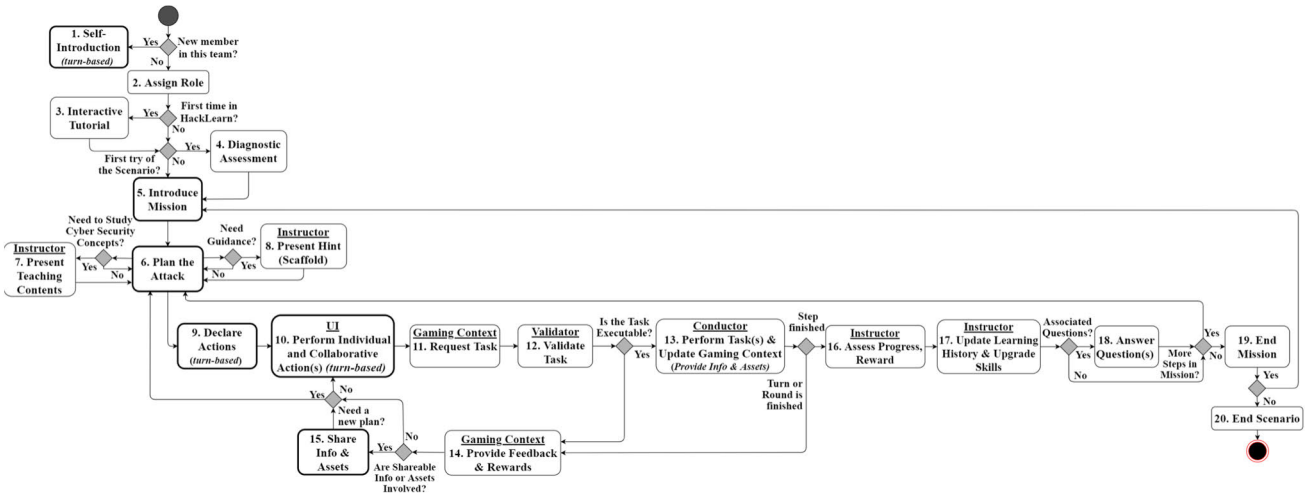


FIGURE 4. mHackLearn sequence diagram.

possessing the ''Strong Password'' policy represents the fact that they will create a strong password when asked to do so. Learners cannot create a strong password if they possess the ''Weak Password'' policy. Additionally, a policy can prescribe the sequence of actions a salesman of a company or an administrator performs to fulfill his/her duties.

E. NPC'S ACTIONS

NPCs perform actions in the phases of Actions & Responses and R2. NPCs can be associated with the following sets of actions.

- Base actions:
  They are performed regularly in the R2 phase or the Response phase as a response to players' actions. Base actions can be associated with triggering conditions, and only executed when these conditions occur. An example of a base action is an administrator taking a backup at the end of a round.
- Random actions:
  They are a set of actions from which an NPC randomly selects an action to execute. An example of a random action is when an administrator of a target system decides to thoroughly inspect the logs of the target.

F. GOALS

Generally, the tCOFELET goals and sub-goals apply to the whole team with achievements unlocking various forms of rewards such as scores and resources. These goals can be associated with specific preconditions, activated to guide learners to perform specific actions or apply policies, and postconditions which are triggered on the successful completion of these goals.

However, tCOFELET introduces the concept of individual goals assigned to each learner, diverging from the team-oriented goals. Individual goals can be utilized in approaches that designers need to introduce an additional layer of complexity and foster learners' strategies into the scenario. Individual goals can vary significantly from approach to approach, adding depth and unique learning experiences to the scenario. For example, a learner might be tasked to be the first one to execute a specific MITRE ATT&CK tactic, adding the aspect of selfishness to the team's collaborative efforts. Alternatively, a more complex individual goal might require a learner to play the 'traitor' role, making deliberate decisions that could compromise the team's goals, thereby simulating insider threat scenarios. This fosters critical thinking challenges and reflects the multifaceted nature of real-world cyber security threats. In a tCOFELET game session, learners can be provided with a set of individual goals from which they can choose which one to pursue, providing the opportunity to personalize their experiences. In such a way, learners are encouraged to reflect on the consequences of their actions, both as individuals and as part of a team, exercising deep analysis skills of cyber security principles and realizing the importance of trust and communication within a cybersecurity team.

V. APPLICATION EXAMPLE

In this section, a design excerpt of a tCOFELET game called multiplayer HackLearn (mHackLearn), is presented. mHackLearn is the multiplayer version of the HackLearn game, a hacking simulator COFELET-compliant game presented in [4] and [7].

A. COMPONENTS' ANALYSIS

For the analysis and design of mHackLearn, the ATMSG model [38] is employed to illustrate the game flow and the organization of its components. Initially, the mHackLearn's activities are identified, and depicted in a UML activity diagram, i.e., the mHackLearn's sequence diagram (Fig. 4). mHackLearn's sequence diagram depicts the game's

components and the manner they interconnect in the structure of the game. The rationale of the depicted components is provided below.

1) *Self-Introduction*: Newcomers notify their capabilities, experiences, and preferences to the team.
2) *Assign Role*: Roles are assigned to learners, randomly or based on their preferences and experiences.
3) *Interactive Tutorial*: Learners are presented with pop-up messages that outline the basic features of the user interface.
4) *Diagnostic Assessment*: Before the beginning of the game session, participants fill out a questionnaire to assess their initial level of knowledge.
5) *Introduce Mission*: It presents the mission to learners including the narrative and goals of the scenario.
6) *Plan the Attack*: Learners collaboratively decide on the strategies and the (SEFs) they will employ to reach the game's goal.
7) *Present Teaching Contents*: Contents explaining to learners the applicable attack patterns (i.e., SEFs), tactics, techniques, and procedures.
8) *Present Hint*: Presents suggestions for the completion of the next step(s).
9) *Declare Actions*: Each learner pledges commitment to the plan by detailing the actions they intend to perform, along with the tools and resources they will employ. The user interface then locks any tools and resources that are not scheduled for use.
10) *Perform Individual and Collaborative Action(s)*: Learners take turns becoming active and performing actions, with the UI enabling synchronous actions to be executed simultaneously.
11) *Request Task*: Actions that are parts of SEFs (i.e., the tasks) are assigned to the Task Engine.
12) *Validate Task*: The Validator component of the Task Engine verifies that a task is part of the sequence of a SEF and checks its validity by examining the occurring conditions.
13) *Perform Task(s) & Update Gaming Context*: Simulates the execution of a task, determines whether its completion triggers the achievement of a goal, and updates the game's context. The active learner receives exclusive information and assets. The execution is performed by the Conductor component of the Task Engine.
14) *Provide Feedback & Rewards*: It provides feedback primarily via the game's UI and rewards (e.g., score updates, animations).
15) *Share Info & Assets*: The active learner acknowledges acquired information to the team and hands over the acquired assets to the next active learner. These actions are not assigned to the Task Engine for validation.
16) *Assess, Progress, Reward*: The Instructor game component considers the learner's profile and learning history, and it assesses the learner's performance based on a grading scheme defined by the instructor.
17) *Update Learning History & Upgrade Skills*: The Instructor game component updates the learning history. When learners achieve specific goals, it manages the upgrade, locking, or unlocking of roles, tools, and capabilities.
18) *Answer Question(s)*: Learners are prompted to respond to reflective questions. Depending on the learning objectives of the step and mission, they may be directed to answer these questions individually or collaboratively.
19) *End Mission*: If there are no remaining steps it concludes the mission.
20) *End Scenario*: If replaying the mission is not required, then the scenario ends.

The phases of the tCOFELET framework are realized in the activities performed in the following components:

- Create Strategy of Plan phase: "6) Plan the Attack",
- Declare actions of Plan phase: "9) Declare Actions",
- Actions and Response phase: "13) Perform Task(s) & Update Gaming Context" and "15) Share Info & Assets",
- R2 phase: "14) Provide Feedback & Rewards", "16) Assess, Progress and Reward".

Table 1 presents a detailed analysis of the components in mHackLearn's game sequence diagram. Specifically, it identifies mHackLearn's components and categorizes them according to gaming, learning, instructional, and collaborative perspectives based on the activities they encompass. Particularly, Table 1 details the *actions* performed in the game for each component, the *tools* enabling these actions, and the *goals* representing the objectives that are achieved upon the completion of these actions. To design mHackLearn's components, elements from the ATMSG taxonomy for serious game components [38] were utilized. However, as the ATMSG model only encompasses gaming, learning, and instructional perspectives, Table 1 also incorporates additional elements for the analysis and design of components under the collaborational perspective mainly adopted from a systematic literature review on serious games for collaborative learning presented in [37]. To maintain brevity, Table 1 omits components that do not embrace collaborational actions, as their analysis is provided in [7].

Subsequently, descriptions of mHackLearn's components are presented. These include in-depth information on the activities occurring in the Collaborational perspective, the in-game tools used, and the goals driving these actions. Communication action happens in all collaboration components as it is a vital mechanism of such approaches. The communication tools include those facilitating face-to-face or digital interactions, including voice, chat functions, and gesture-based communication methods.

- *1. Self-Introduction:*
  New team members introduce themselves by sharing their skills, expertise, characteristics, and preferences. This process begins with learners completing structured

TABLE 1. mHackLearn's serious game components.

		Self-Introduction (turn-based)	Introduce Mission	Plan the Attack	Declare Actions (turn-based)	Perform Collaborative & Individualistic Action(s) (turn-based)	Share Info & Assets	Assess Progress, Reward & Upgrade
Gaming	Actions		Read Story	Plan/Strategy, Match		Create, Generate		See Performance Evaluation
	Tools		Story	Information		2D space, Time pressure		Progress bar, Points, Role/Virtual skills, Status level, Information
	Goals		Get acquainted with story (and mission)	Complete quest & side quests		Complete quest & side quests		Maximize Performance
Learning	Actions		Observe, Identify	Observe, Identify Hypothesize, Combine, Plan, Restate		Apply, Recall, Repeat		Verify, Review
	Tools		Problem, Challenge	Creations, Inventions		Simulator, Experiment		Information, Graphics
	Goals		Understand, Analyze	Active Experimentation, Abstract Conceptualization		Apply, Concrete Experience		Understand, Reflective Observation
Instructional	Actions		Tell Story, Present Problem	Repetition, Scaffold		Reward good performance, Repetition		Qualitatively assess performance
	Tools		Story	Information, Multiple choices, Limited set of choices		Performance measures, Multiple chances		Performance measures
	Goals		Inform Learner, Gain Attention	Provide learning guidance		Elicit performance		Assess performance, Provide feedback
Collaborational	Actions	Group briefing (characteristics, capabilities, preferences)	Common goals, Individual goals	Discussion, Acceptance, Rejection, Advisement, Indirect actions (in advising actions of the plan), Decision making	Task assignment	Distribution of contribution, Information division, Indirect actions (in performing the plan)	Coordinate, Share, and combine information	Joint rewards, Group briefing, Group reflection, Shared property
	Tools	Questionnaires, TKSAs Lists, Achievements, Alternating turns	Open/private information	Shared workspace (e.g., board)	Task lists, Tool lists, Alternating turns	Shared virtual space, Private (or encrypted) information, Alternating turns, Shared Objects	Exchange of Shared Objects (e.g., information and assets)	Common property, Open/private information
	Goals	Team awareness Pooling of capabilities, Self-expression	Shared understanding (for goals and context), Interaction, Communication	Interaction, Establish shared meaning (for the plan), Individual accountability, Self-expression	Establish rules of engagement, Commitment to common success, Self-expression	Individual accountability, Switching leadership	Interdependence, Contribution by all team members, Teamwork Motivation	Group engagement, Teamwork motivation, Repair problems in shared understanding

forms, such as questionnaires, tasks, and KSAs listing KSAs they are comfortable with. The Self-Introduction component aims to enhance team awareness, setting a basis for effective collaboration and strategic team formation.

- *5. Introduce Scenario:*
  A scenario is presented to the team to establish common goals and facilitate communication and interaction among learners. The scenario is analyzed collaboratively to identify the scenario's objectives and establish a shared meaning of its context. The scenario allocated the game's resources evenly to the team, ensures a shared meaning of the mission's goals and challenges, motivates teamwork, and improves team awareness [37].
- *6. Plan the Attack:*
  Learners engage in decision-making activities in which they discuss, accept, or reject various ideas regarding attack patterns and strategies of the upcoming action phase. Learners may assume leadership roles offering advice, encouragement, and information on the execution of actions. A shared workspace, such as a virtual board, can facilitate the activities of a collaborative plan facilitating brainstorming and visualization of attack steps. The team must establish a common understanding of the plan, mutual agreement, and commitment, as each team member is important for the achievement of goals.
- *9. Declare Actions:*
  Learners take turns expressing their role in executing the plan, demonstrating their commitment to the team's efforts, and establishing rules of engagement. This activity may involve the reservation of resources (e.g., energy points) and tools.
- *10. Perform Individual & Collaborative Actions:*
  Learners take turns using the reserved resources to perform actions within the game's virtual space, following the elaborated plan. Active learners receive specific responses from the game encompassed in component *14. Provide Feedback & Rewards*. Such responses include detailed information and assets (i.e., shared objects), and the rest of the team receives more abstract feedback acknowledging changes in the game's context. For example, in a hacking simulation game, the active learner discovering live hosts in the network receives precise information such as IPs and hostnames, while the others see only general representations of these hosts on the network map. Additionally, the active learner can initiate collaborative actions, which require the contribution of non-active learners.
  This component often presents challenging experiences, as active learners might need to adjust the elaborated plan in response to unexpected incidents triggered by their actions, such as an administrator detecting malicious traffic. In such a way, active learners assume a leadership role, enhancing their sense of individual responsibility.
- *15. Share Info & Assets:*
  Before the end of a turn, the active learner is required to disseminate information and assets to the rest of the

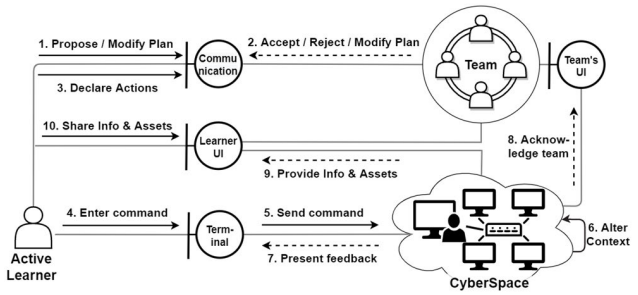


FIGURE 5. UML communication diagram.

team. This ensures that the subsequent active player has the necessary means to continue executing the plan. Games must contain the appropriate facilities for the exchange of shared objects and information and the coordination of their actions.

- *16. Assess Progress, Reward & Upgrade:* At the end of the rounds and the completion of the appropriate steps, various post-conditions are activated triggering events such as the evaluation of the team's progress, the allocation of collective rewards or penalties, the enhancement of the learners' repertoire and skills, the revealing of new entities and characters, and the establishment of new goals. Learners reflect on their efforts and discuss their successes or failures during a team briefing. In such a way, a sense of team victory or defeat is fostered among learners, misconceptions about the team's common understanding are repaired, and learners' engagement is boosted.

B. LEARNERS' INTERACTIONS

Fig. 5 presents interactions among learners, and the cyberspace of a typical mHackLearn scenario. Central to these interactions is the use of a terminal interface, in which learners enter commands that initiate actions (i.e., COFELET tasks) simulating real-world cyberspace operations. Additionally, the scenario's user interface is designed with the appropriate features that facilitate team communication and collaboration.

Specifically, the user interface includes components that enable learners to:

- Engage in live communication and collaboration with their teammates, featuring a workspace for planning and decision-making,
- Declare planned actions, self-express themselves, and commit themselves to the pursuit of goals,
- Allocate resources, ensuring that each team member can access necessary tools and assets to perform their actions,
- Exchange information and resources, enhancing collaboration.

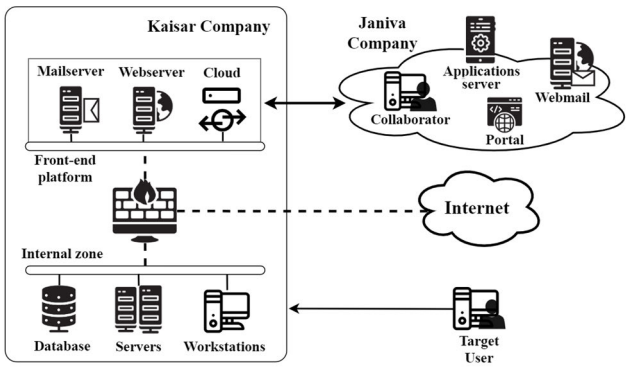


FIGURE 6. Scenario's cyberspace.

C. PROTOTYPE SCENARIO

The prototype scenario, presented in this section, shows how the theoretical knowledge of Mitre's ATT&CK framework is transformed into a real-life cyber-attack simulation based on tCOFLET. Learners assume the roles of a freelancing team of hackers recruited by the competitors of the Kaisar company to steal a document file containing specifications and designs of 3D models for a new product. Learners are expected to discover entities of Kaisar (illustrated in Fig. 6) along with the entities of the Janiva company which cooperates with Kaisar. Learners will try to exploit the vulnerabilities of the discovered entities that will bring them closer to the achievement of their goals.

The scenario consists of the following phases:

1) *Reconnaissance and Information gathering*: learners use search engines and social media to gather information about the target organization, and identify key employees, the organizational structure of the company, and potential vulnerabilities.
2) *Target Identification and Credential Harvesting*: learners set individual targets that may have access to the target file. The activities of this phase include searching social media and the dark web for credentials and other sensitive information.
3) *Exploitation of Vulnerabilities*: learners attempt to gain initial access to the target and the associative organization through the exploitation of vulnerabilities of the public-facing applications. It includes the usage of spear-phishing and other social engineering techniques.
4) *Data Access and Extraction*: Includes the acquisition of the target file and the cracking of any protective measures on the file.

1) ROLES

The scenario includes the appropriate roles to help the collaboration of learners discover and exploit vulnerabilities and perform cyber-attacks on the cyber and physical surface of the target entity. These roles include *Network Specialist*,

Applications Expert, *Cryptographer*, *Social Engineer,* and *Physical Attacker* (depicted in Fig 4). As the scenario evolves the *Social Engineer* and *Physical Attacker* roles are upgraded to the *Socio-physical Attacker* role, which inherits the knowledge and skills of *Social Engineer* and *Physical Attacker* parent roles. The expertise of these roles is provided below:

- Network Specialist: masters actions involving deep knowledge of network systems, protocols, vulnerabilities of public-facing services, applications, and the network infrastructure,
- Applications Expert: specializes in targeting software applications and services, including the development of weaponized files, custom coding, and the injection of malicious scripts in files and applications,
- Cryptographer: focuses on the aspects of encryption, decryption, coding, encoding, obfuscation, and steganography. Cryptographer specializes in password cracking, dictionary attacks, brute force attacks, and rainbow table attacks to decrypt passwords.
- Socio-physical Attacker: specializes in Social Engineering and Physical Security techniques including impersonation of characters and roles, physical attacks (e.g., dumpster diving, tailgating), and maintaining fake accounts and profiles.

2) ACTIONS

In each R2 phase, mHackLearn's mechanisms assign a limited amount of energy points to learners required for the execution of actions in the Action and Response phases. Actions belong to the physical or the virtual domain. Physical actions represent direct and tangible interactions of learners with the targets such as the inspection of a character, place, or asset (e.g., website, dumpster), and the oral communication with a person. These actions also include verbal communication with individuals, simulating real-world reconnaissance, and social engineering techniques. Virtual actions are performed in the cyberspace domain through computing devices. Each device is equipped with an in-game operating system and a suite of tools that simulate the functionality of real-world systems. In-game tools include web browsers for internet navigation, email clients, chat programs for instant messaging, a terminal for execution of Unix-like commands, and a set of specialized tools for the performance of cyber-attacks (detailed in Table 2).

3) POLICIES

Learners hold specific policies that prescribe conditions, and how actions are executed. These policies are role-specific, enhancing the realism of the game. For instance, a policy of a learner assuming the role of a Network Specialist reduces the energy cost of cyber-attacks based on the MITRE ATT&CK's 'Exploit Public-Facing Application' technique. Similarly, the Cryptographer character is more efficient at decrypting password-protected files, requiring fewer rounds to achieve the decryption; the Socio-physical attacker can choose an NPC and convince it to perform a base, or a random action which the learner devises; and the Applications Expert can create custom pieces of code that can be utilized in the creation of weapon files. The use of policies ensures that learners collaborate effectively, to try to leverage each character's strengths and effectively navigate the scenario's challenges.

TABLE 2. The tools of the prototype scenario.

Description	Tool
Network analyzer to determine the status of ports running on a target.	Nmap
Browsers to perform reconnaissance actions in the world wide web and dark web.	browser, tor browser,
	Email client
URI brute-force tool to enumerate directories and websites.	gobuster, dirb
Web shell to brute force authentication mechanisms of services.	PAS webshell
Search tool of the exploit-db service for finding code exploits for specific vulnerabilities.	searchsploit
Remote access tool for remote target connection.	ssh
A file transfer tool for retrieving files from the target.	ftp
HTTP(S) file transfer tool that clones websites.	wget
Password cracking tools for hash extraction from an office file and brute forcing of the extracted hash.	john, office2john
Tool for the creation of weapon files.	msfvenom, metasploit

4) GOALS

The scenario's goal requires learners to steal a confidential file from a company. Learners are also assigned individual goals that require them to be the first ones to apply specific Mitre ATT&CK techniques corresponding to their role as follows:

- Network specialist must be the first learner to perform port scanning,
- At least once in the scenario, an applications expert must create a weaponized file,
- Socio-physical Attacker must perform a dumpster diving attack during the scenario by performing an inspection action on the dumpster of the Kaisar or Janiva,
- Once in the scenario cryptographer must instruct another learner to create a wordlist.

5) POLICIES

Learners hold specific policies that prescribe conditions, and how actions are executed. These policies are role-specific, enhancing the realism of the game. For instance, a policy of a learner assuming the role of a Network Specialist reduces the energy cost of cyber-attacks based on the MITRE ATT&CK's 'Exploit Public-Facing Application' technique. Similarly, the Cryptographer character is more efficient at decrypting password-protected files, requiring fewer rounds to achieve the decryption; the Socio-physical attacker can choose an NPC and convince it to perform a base, or a random

TABLE 3. The LOs of the prototype scenario.

Code	Bloom Level	LO Statement
L1	Application (affective)	Learners articulate their knowledge, skills, and strategies to the team, enhancing collective understanding and collaborative efforts.
L2	Application (affective)	Learners demonstrate openness to accept suggestions, advisements, and feedback, from any team member, fostering a culture of continuous improvement and mutual respect.
L3	Analysis, Evaluation (affective)	Learners critically assess the validity and the applicability of arguments presented by teammates, deciding to adopt, reject, or propose modifications.
L4	Analysis (cognitive)	Learners analyze scenario's cyberspace to identify key clues, assets, and information, that can inform the team's strategy.
L5	Evaluation (cognitive)	Learners recognize assets (e.g., tools) and pieces of information that can be strategically deployed in orchestrating cyber-attacks.
L6	Evaluation (cognitive)	Learners exercise critical thinking and risk assessment capabilities to identify potential points of vulnerability.
L7	Synthesis (cognitive)	Learners demonstrate deep knowledge of the TTPs of MITRE's ATT&CK framework, and strategic application of this knowledge through the design of cyber-attacks based on the ATT&CK's techniques.
L8	Application (cognitive)	Learners apply practical skills by utilizing the appropriate tools for the execution of simulated cyber-attacks.
L9	Application (cognitive)	Learners execute techniques of the MITRE's ATT&CK in a controlled and simulated environment, transforming knowledge into practical cyber security skills.
L10	Application (cognitive)	Learners create a phishing campaign, by combining, a persuasive phishing text, a credible sender's email, and a phishing link to a fake website mimicking a legitimate one.

TABLE 4. The steps of the prototype scenario.

Code	DESCRIPTION	MITRE ATT&CK TTPS
S1	Learners browse the target company's website and social media and acquire information regarding the company's organizational structure, employee names, and emails.	Search Open Websites / Domains, Search Victim-Owned Websites
S2	Learners acquire additional information about the company and its employees on the dark web.	Gather Victim Identity Information
S3	Learners investigate the associate company's website, social media, and the dark web for further details regarding the company and employees.	Network Trust Dependencies
S4	Learners use the sqlmap tool to exploit the associate company's public-facing portal and obtain passwords.	Exploit Public-Facing Application
S5	Learners use the collected credentials to compromise the associate company's webmail service.	Compromise Accounts: Email Accounts
S6	Learners create a fake cloud service website and a spear-phishing email to target the primary company's employees.	Phishing for Information
S7	Learners use the stolen credentials to access the target company's platform and locate the desired target file.	Spearphishing Link, Data from Information Repositories
S8	Learners decrypt the locked target file using password-cracking tools and contextual information. Finally, they open the target file, and they achieve the scenario's goal.	Brute Force: Password Cracking

action which the learner devises; and the Applications Expert can create custom pieces of code that can be utilized in the creation of weapon files. The use of policies ensures that learners collaborate effectively, to try to leverage each character's strengths and effectively navigate the scenario's challenges.

6) NPC'S ACTIONS

The prototype scenario involves employees of the Kaisar and the Janiva target companies including the secretary and the administrator of the Kaisar company. Learners can interact with the secretary NPC, but they will not be able to discover any clues that will help them with their mission. Learners are not able to interact with the rest of the scenario's employees, but they will be affected by administrator actions who apply more strict cyber security policies during the scenario's course such as whitelisting email addresses and alarming the employees and asking them to change passwords.

7) STEPS AND LEARNING OBJECTIVES

The LOs presented in Table 3 are designed to enhance learners' capabilities across both cognitive and affective domains, highlighting the multifaceted nature of cyber security expertise. Cognitive domain LOs include the comprehension of cyber security concepts and methodologies as well as the application of practical skills. Cognitive domain LOs are supported by analysis and synthesis skills, and critical thinking, to navigate the scenario's threat landscape effectively.

The affective domain LOs are designed to foster attitudes and principles essential to cyber security. These include the willingness to share KSAs (L1), the receptiveness to accept and critically assess other people's views and suggestions (L2, L3), and to development of a sense of responsibility towards achieving the team's goals [39].

Table 4 presents the list of steps for the achievement of the scenario's goals, correlating each step with its respective MITRE ATT&CK TTPs and reference codes.

Affective domain objectives, such as L1, L2, and L3, are integral throughout the scenario, facilitating knowledge exchange, evaluation of suggestions, and refinement of strategies within the team's collaborative planning process. This is essential in all the instances of the tCOFELET plan phase.

Cognitive domain objectives are categorized across various Bloom taxonomy levels [40], encompassing application, analysis, synthesis, and evaluation. Participants engage with a quiver of tools (as listed in Table 2) to apply their acquired skills across all steps of the scenario (L8), based on the elaborated plan and attack strategy. Initial reconnaissance activities detailed in steps S1, S2, and S3 (aligned with L4 and L5) are critical for acquiring information, for contextual

TABLE 5. mHackLearn's evaluation.

Design Considerations	Support	Rational
Common Goal/Success	✔	The mHackLearn goals apply to all learners of a team.
Refillable personal resources	✔	Actions are associated with resources (i.e., energy points) required to perform actions during a learner's turn. Action limits are a central element setting a boundary to the energy points learners hold and the number of actions that can be performed. Energy points are not transferred or exchanged, but they can be affected by the team's overall performance. For example, actions that reveal assets or achieve goals award learners with resources representing that learners feel confident and have good performance.
Heterogeneous resources	✘	Includes a limited set of heterogeneous resources as learners execute the team's plan sequentially and collaboratively. Learners perform their actions as soon as they have resources and subsequently, their teammates continue with the plan's execution.
Collectible and tradeable resources	?	Active learners acquire assets and information as they interact with the scenario's entities and characters. Active learners must share or pass these assets and information to non-active learners before the end of the turn (depicted in Fig. 6). Then, the next active learner will carry on the team's mission according to the specified scenario and plan.
Collaborative tasks	✔	The prototype scenario involves two types of collaborative actions (presented in section V): the transfer of information and assets, and the condition-triggering actions.
Communication	✔	It is supported intrinsically. In the planning phase, learners propose, accept, or reject propositions to decide their strategies on the manner they will spend their resources in the subsequent round.
Feedback facility	✔	Through the mHackLearn interface feedback, rewards, and penalties are provided to learners (depicted in Fig. 6).
In-game help system	✔	mHackLearn includes a help facility providing hints and teaching materials to learners (illustrated in the sequence diagram of Fig. 4).
Complementary actions	✔	Are supported intrinsically. Due to the employment of action limits, and the distribution of information and assets to all team members, learners can only achieve the scenario's goals if they collaborate, coordinate, and synchronize their actions.
Indirect actions	✔	As detailed in the presentation of the tCOFELET phases, in the plan phase learners disseminate their strategies and plans, which involves providing instructions on how their teammates should act. Moreover, the policy of the socio-physical attacker specifies that the attacker can act indirectly by persuading NPCs to perform actions (presented in Section B of VI).
Encrypted information	✔	During the Response phase assets and information are only disclosed to the active learner. Active learners are required to share these assets and information. Additionally, individual goals can foster individual accountability, as they can assess learners' performance.
Scripted and emergent roles	?	mHackLearn only includes the perspective of the scripted role.
Conflict	✔	mHackLearn includes a form of conflict, as learners will have to unleash cyber-attacks.
Create shared property	✔	The prototype scenario involves several entities that belong to the team (e.g., USB flash drives acquired during the Response phase).
Self-expression	✔	Learners have many opportunities to express themselves. In the Plan phase, they can discuss potential strategies with their teammates and subsequently declare their actions. During the Action and the R2 phases, they can reveal aspects of their personalities through the employment of different styles of play or strategies.
Support at least three levels of experience	✘	mHackLearn does not adapt to three different levels of experience of the learners.
Team management	✔	mHackLearn complies with tCOFELET which intrinsically supports the organization of learners' activities and the fostering of collaboration. Learners communicate in the Plan phase, share resources in the Action phase, and reflect on their activities and achievements during the R2 phase.
Events	✔	Learners have several things to expect during a mHackLearn session. Learners' and NPCs' actions are performed during the pre-defined phases and several events can occur, which refer to cyber-attacks and unexpected incidents. Learners also expect the upgrade of roles, tasks, and policies, and the rounds' post-conditions.
Flexibility in Roles	✔	Central to tCOFELET and the proposed scenario is the dynamic shift of roles through the upgrade, the locking, and the unlocking of roles' capabilities. Learners can develop their own social identity, through the adoption of different roles and the acquisition of policies that prescribe the manner that learners perform actions.
Interactions	?	mHackLearn caters only to the internal interactions of learners, as it does not keep information about the social context of the learners outside of the game.
Meaningful Social Play	✔	mHackLearn foresees the interactions of learners and fosters collaboration and teamwork.
Community Building	✔	The team of learners formed in mHackLearn is realized like a community of practice, where learners engage in mutual knowledge and sharing, and building of collective understanding of risks, threats, and responsibilities.
Selfless .vs Selfish actions	✔	Learners perform selfless actions in mHackLearn. However, selfishness can be expressed when learners deliberately diverge from the elaborated plan trying to fulfill their individual goals at the expense of the team.
Highly Interdependent Roles	✔	Although mHackLearn contains interdependent roles, the collaborative aspect of the game is not downgraded as learners share a large set of capabilities

TABLE 5. *(Continued.)* **mHackLearn's evaluation.**

		allowing them to collaboratively share their challenges.
Role alignment with real-world contexts	✔	Learners assume roles associated with knowledge and skills they need to perform their duties as penetration testers, thus mHackLearn is closely related to real-world context.
Lack of study of commercial games	✘	Although the presented analysis has included in its scope some studies performed on commercial games, it has not systematically analyzed this domain.

analysis, and for the strategic envisioning of an attack plan optimized by the information gathered.

Subsequently, learners validate high-level capabilities (as prescribed in L6, L7, L8, and L9) by leveraging the MITRE ATT&CK framework. They envisage a comprehensive cyber-attack strategy incorporating techniques for exploiting vulnerabilities (step S4), compromising email accounts (step S5), and orchestrating a spear-phishing campaign (steps S6 and S7). This approach demonstrates the practical application of theoretical knowledge, and it also highlights the critical role of collaborative planning and critical thinking in developing effective cyber security strategies.

VI. EVALUATION

The tCOFELET framework envisions the creation of effective collaborative cybersecurity serious games, by addressing the design considerations outlined in Section III and tackling the challenges identified therein. This section shows how mHackLearn, along with the prototype scenario, embodies these design considerations, offering an initial appreciation of its potential impact.

VII. DISCUSSION

The results of the evaluation presented in section VII allow a good appreciation of mHackLearn's potential, as most of the recommendations presented in section III are embraced. Specifically, mHackLearn employs 19 out of the 26 design considerations and it seems eligible to confront 2 out of 3 identified pitfalls (presented in Section III). mHackLearn effectively implements the design considerations of '*Common goals*', '*Refillable personal resources*', '*Collaborative tasks*', '*Encrypted information*', '*Shared property*', '*Complementary actions*', and '*Communication*' that they uniquely support the collaboration aspect of the game involving the creation of a community of learning (as presented in section II). In this community learners share the understanding while they discuss the scenario details and build their strategy, they jointly perform the appropriate actions to confront the scenario challenges, and they share information, assets, and a large repertoire of capabilities. Shared responsibility and interdependence are fostered among learners and in the plan, Action, and R2 phases there are many opportunities for pedagogically productive interactions. mHackLearn presents an innovative approach in the manner it employs '*Team-management*', '*Self-expression*', and '*Indirect Actions*' design considerations, allowing the organization of learners' activities while providing opportunities for all learners to participate in the team's efforts and express themselves through verbal communication and gameplay. Although mHackLearn does not support emergent roles, it implements the '*Flexibility in roles*' design consideration presenting significance in helping learners to assimilate KSAs associated with new roles, as they are combined with capabilities of known roles. Additionally, '*Flexibility in roles*' provides learners something to expect increasing their engagement with the game.

On the other hand, although mHackLearn implements the '*heterogeneous resources*' and '*collectible and tradeable resources*' design considerations, these considerations are not adopted to a satisfactory degree that they will foster the negotiation aspect in the game. Additionally, mHackLearn does not adapt its scenario according to the learners' level of experience, and it does not consider external interactions of learners, which can facilitate the effective assignment of roles and individual goals.

VIII. CONCLUSION

Given the critical importance of cybersecurity, the presented study focuses on the domain of multiplayer and collaborative cybersecurity serious games. The key design considerations of multiplayer collaborative games, both in serious and fun settings, are explored. Leveraging the insights from this exploration and building upon the COFELET framework, elaborated for the design and implementation of single-player cyber security serious games, the tCOFELET framework is proposed as a strategic extension. It describes the main elements that capitalize on team-centric learning inside game-based settings. Utilizing the tCOFELET framework, a prototype scenario was developed for the multiplayer version of the HackLearn COFELET-compliant serious game, known as mHackLearn. An initial appreciation of the tCOFELET approach's impact was derived through the comparison of the prototype scenario's features with the explored design considerations. The results indicated that approaches like the mHackLearn prototype can boost the effectiveness of cybersecurity serious games by fostering the sharing of knowledge and skills among learners and unique learning experiences. The work presented in this study sets the ground for the implementation of impactful and highly organized multiplayer serious cybersecurity games, particularly focused on the collaboration of learners.

Future work on tCOFELET focuses on the implementation of mHackLearn, and the utilization of the presented scenario in the real educational setting of a university. An extensive testing of mHackLearn's effectiveness will help comprehend how tCOFELET approaches can impact their learning outcomes, and it will provide valuable insights into the tCOFELET's impact. Nevertheless, this study aims to expand the utilization and application of tCOFELET beyond digital

games to include tabletop games for raising cybersecurity awareness among university students and teaching staff. This continuing expansion of tCOFELET implementations and applications in real settings is expected to enhance the understanding of the practical implications and effectiveness of the framework, as well as team-centric learning in cybersecurity.

REFERENCES

[1] B. Newhouse, S. Keith, B. Scribner, and G. Witte, "Nice cybersecurity workforce framework (NCWF)," *Draft NIST Special Publication*, vol. 181, pp. 181–800, Nov. 2016.

[2] N. M. Katsantonis, I. Kotini, P. Fouliras, and I. Mavridis, "Conceptual framework for developing cyber security serious games," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Apr. 2019, pp. 872–881.

[3] P. Reimann, "Design-based research," in *Methodological Choice and Design: Scholarship, Policy and Practice in Social and Educational Research*. Dordrecht, The Netherlands: Springer Netherlands, 2010, pp. 37–50.

[4] M. Katsantonis and I. Mavridis, "Evaluation of HackLearn COFELET game user experience for cybersecurity education," *Int. J. Serious Games*, vol. 8, no. 3, pp. 3–24, Sep. 2021.

[5] S. O'Connor, S. Hasshu, J. Bielby, S. Colreavy-Donnelly, S. Kuhn, F. Caraffini, and R. Smith, "SCIPS: A serious game using a guidance mechanic to scaffold effective training for cyber security," *Inf. Sci.*, vol. 580, pp. 524–540, Nov. 2021.

[6] M. N. Katsantonis and I. Mavridis, "Ontology-based modelling for cyber security e-learning and training," in *Advances in Web-Based Learning—ICWL*, vol. 18, Magdeburg, Germany. Springer, 2019, pp. 15–27.

[7] M. N. Katsantonis, I. Mavridis, and D. Gritzalis, "Design and evaluation of COFELET-based approaches for cyber security learning and training," *Comput. Secur.*, vol. 105, Jun. 2021, Art. no. 102263.

[8] L. S. Vygotsky, *Mind in Society: The Development of Higher Psychological Processes*. Cambridge, U.K.: Harvard Univ. Press, 1978.

[9] J. Lave and E. Wenger, *Situated Learning: Legitimate Peripheral Participation*. New York, NY, USA: Cambridge Univ. Press 1991.

[10] E. Wenger, *Communities of Practice: Learning, Meaning, and Identity*. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[11] V. Farnsworth, I. Kleanthous, and E. Wenger-Trayner, "Communities of practice as a social theory of learning: A conversation with etienne wenger," *Brit. J. Educ. Stud.*, vol. 64, no. 2, pp. 139–160, Apr. 2016.

[12] I. Bogost, *Persuasive Games: The Expressive Power of Videogames*. Cambridge, MA, USA: MIT Press, 2010.

[13] B. A. Schwendimann, B. De Wever, R. Hämäläinen, and A. A. P. Cattaneo, "The state-of-the-art of collaborative technologies for initial vocational education: A systematic literature review," *Int. J. Res. Vocational Educ. Training*, vol. 5, no. 1, pp. 19–41, Apr. 2018.

[14] D. Daylamani-Zad, H. Agius, and M. C. Angelides, "Reflective agents for personalisation in collaborative games," *Artif. Intell. Rev.*, vol. 53, no. 1, pp. 429–474, Jan. 2020.

[15] V. Wendel and J. Konert, "Multiplayer serious games," in *Serious Games*. New York, NY, USA: Springer, 2016, pp. 211–241.
Serious Games, Springer International Publishing, New York City,

[16] S. D. Teasley and J. Roschelle, "Constructing a joint problem space: The computer as a tool for sharing knowledge," in *Computers as Cognitive Tools*. Evanston, IL, USA: Routledge, 2013, pp. 229–258.

[17] G. Engelstein and I. Shalev, *Building Blocks of Tabletop Game Design: An Encyclopedia of Mechanisms*. Boca Raton, FL, USA: CRC Press, 2022.

[18] J. P. Zagal, J. Rick, and I. Hsi, "Collaborative games: Lessons learned from board games," *Simul. Gaming*, vol. 37, no. 1, pp. 24–40, Mar. 2006.

[19] R. H. Hämäläinen, M. Niilo-Rämä, T. Lainema, and K. Oksanen, "How to raise different game collaboration activities: The association between game mechanics, players' roles and collaboration processes," *Simul. Gaming*, vol. 49, no. 1, pp. 50–71, Feb. 2018.

[20] V. Wendel, M. Gutjahr, S. Göbel, and R. Steinmetz, "Designing collaborative multiplayer serious games," *Educ. Inf. Technol.*, vol. 18, no. 2, pp. 287–308, 2013.

[21] P. Dillenbourg, "What do you mean by collaborative learning?" in *Collaborative-Learning: Cognitive and Computational Approaches*. Oxford, U.K.: Elsevier, 1999, pp. 1–19.

[22] D. W. Johnson and R. T. Johnson, *Learning Together and Alone: Cooperative, Competitive, and Individualistic Learning*. Upper Saddle River, NJ, USA: Prentice-Hall, 1987.

[23] R. Hämäläinen, T. Manninen, S. Järvelä, and P. Häkkinen, "Learning to collaborate: Designing collaboration in a 3-D game environment," *Internet Higher Educ.*, vol. 9, no. 1, pp. 47–61, 2006.

[24] K. Oksanen and R. Hämäläinen, "Game mechanics in the design of a collaborative 3D serious game," *Simul. Gaming*, vol. 45, no. 2, pp. 255–278, Apr. 2014.

[25] L. Kobbe, A. Weinberger, P. Dillenbourg, A. Harrer, and R. Hämäläinen, "Specifying computer-supported collaboration scripts," *Int. J. Comput.-Supported Collaborative Learn.*, vol. 2, nos. 2–3, pp. 211–224, 2007.

[26] J.-W. Strijbos and M. F. De Laat, "Developing the role concept for computer-supported collaborative learning: An explorative synthesis," *Comput. Hum. Behav.*, vol. 26, no. 4, pp. 495–505, Jul. 2010.

[27] J. Schell, *The Art of Game Design: A book of Lenses*. Boca Raton, FL, USA: CRC Press, 2014.

[28] K. S. Tekinbas and E. Zimmerman, *Rules of Play: Game Design Fundamentals*. Cambridge, MA, USA: MIT Press, 2003.

[29] T. Zhao, T. Gasiba, U. Lechner, and M. Pinto-Albuquerque, "Raising awareness about cloud security in industry through a board game," *Information*, vol. 12, no. 11, p. 482, 2021.

[30] M. Riar, B. Morschheuser, R. Zarnekow, and J. Hamari, "Gamification of cooperation: A framework, literature review and future research agenda," *Int. J. Inf. Manag.*, vol. 67, Dec. 2022, Art. no. 102549.

[31] J. Harris, M. Hancock, and S. D. Scott, "Leveraging asymmetries in multiplayer games: Investigating design elements of interdependent play," in *Proc. Annu. Symp. Comput.-Human Interact. Play*, Oct. 2016, pp. 350–361.

[32] A. Yasin, L. Liu, T. Li, R. Fatima, and W. Jianmin, "Improving software security awareness using a serious game," *IET Softw.*, vol. 13, no. 2, pp. 159–169, Apr. 2019.

[33] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Comput. Secur.*, vol. 95, Aug. 2020, Art. no. 101827.

[34] E. B. Johnson, *Contextual Teaching and Learning: What it is and Why it's Here to Stay*. Thousand Oaks, CA, USA: Corwin Press, 2002.

[35] R. Buckley and J. Caple, *The Theory and Practice of Training*. London, U.K.: Kogan Page, 2009.

[36] C. Sousa, S. Rye, M. Sousa, P. J. Torres, C. Perim, S. A. Mansuklal, and F. Ennami, "Playing at the school table: Systematic literature review of board, tabletop, and other analog game-based learning approaches," *Frontiers Psychol.*, vol. 14, Jun. 2023, Art. no. 1160591.

[37] C. Wang and L. Huang, "A systematic review of serious games for collaborative learning: Theoretical framework, game mechanic and efficiency assessment," *Int. J. Emerg. Technol. Learn. (iJET)*, vol. 16, no. 6, p. 88, Mar. 2021.

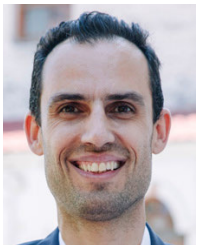
[38] M. B. Carvalho, F. Bellotti, R. Berta, A. De Gloria, C. I. Sedano, J. B. Hauge, J. Hu, and M. Rauterberg, "An activity theory-based model for serious games analysis and conceptual design," *Comput. Educ.*, vol. 87, pp. 166–181, Sep. 2015.

[39] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre att&ck: Design and philosophy," MITRE Corp., McLean, VA, USA, Tech. Rep. MP180360R1, 2018.

[40] B. L. Martin and L. J. Briggs, "The affective and cognitive domains: Integration for instruction and research," *Educ. Technol. Publications*, vol. 35, pp. 123–130, 1986.

[41] L. W. Anderson, D. R. Krathwohl, P. Airasian, K. Cruikshank, R. Mayer, P. Pintrich, and M. Wittrock, *A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy*. New York, NY, USA: Longman, 2001.

MENELAOS N. KATSANTONIS received the B.Sc. degree in computer science from the University of Reading, U.K., the M.Sc. degree in distributed systems and networks from the University of Kent, Canterbury, U.K., and the Ph.D. degree in cybersecurity game-based learning from the University of Macedonia, Greece. Since 2004, he has been serving, in an experienced informatics instructor's capacity, various institutes, and schools. He is currently a Postdoctoral Researcher with the Department of Applied Informatics, University of Macedonia. His current research interests include cybersecurity education, serious games, game-based training, and cyber ranges.



ATHANASIOS MANIKAS received the B.Sc. degree in computer science from Alexander TEI, Thessaloniki, Greece, and the M.A. degree in educational sciences from the Open University, Cyprus. He is currently pursuing the Ph.D. degree in cybersecurity education with the Department of Applied Informatics, University of Macedonia, Greece. Since 2006, he has been a Computer Science Teacher in public secondary education. His research interests include cyber security education and training, collaborative learning, serious games, and cyber ranges.

IOANNIS MAVRIDIS received the Diploma degree in computer engineering and the M.A. degree from the University of Patras, Greece, and the Ph.D. degree in information systems security from the Aristotle University of Thessaloniki, Greece. He is currently a Professor of information security with the Department of Applied Informatics, University of Macedonia, Greece. He is the Director of the Multimedia, Security and Networking (MSN) Laboratory. He has published more than 100 papers in journals and conferences. He is the author or coauthor of three books on information security. He has participated as a Principal Investigator and a Researcher of several international and nationally-funded research and development projects. His current research interests include cybersecurity education on risk management, access control, cyber threat intelligence, digital forensics, and security economics. He serves as an Area Editor for *Journal of Cyber Security* (Elsevier) and *Array* (Elsevier).

PANAGIOTIS FOULIRAS received the B.Sc. degree in physics from the Aristotle University of Thessaloniki, Greece, and the M.Sc. and Ph.D. degrees in computer science from the University of London, U.K. (QMW). He is currently a permanent Assistant Professor with the Department of Applied Informatics, University of Macedonia, Thessaloniki. He has participated in several national and European-funded (H2020) research projects and published articles in many international journals. His research interests include computer networks and network security, blockchain, and system evaluation methods.