Virtual Reality Training of Law Enforcement Officers in Predicting Terroristic Attacks Indicators

John Soldatos
Research and Development
INNOV-ACTS Limited
Nicosia, Cyprus
jsoldat@innov-acts.com

Anastasios Pantazidis
Research and Development
INNOV-ACTS Limited
Nicosia, Cyprus
tpantazidis@innov-acts.com

Aikaterini Margariti
CERIDES
European University of Cyprus
Nicosia, Cyprus
K.Margariti@research.euc.ac.cy

Pantelis Velanas
CERIDES
European University of Cyprus
Nicosia, Cyprus
P.Velanas@research.euc.ac.cy

Bogdan Gornea
Research and Development
SIMAVI Software Imagination & Vision
Bucharest, Romania
Bogdan.Gornea@siveco.ro

***Abstract*— Serious games have been recently proposed as an effective way for training security professionals in cyber and physical security processes. Nevertheless, state of the art games tend to focus on simple security process and pay limited emphasis on ergonomic and ease of use. This paper introduces a novel serious game for training security professionals in predicting potential suspicious activities. The game incorporates background knowledge about terroristic attacks and incorporates intelligence modules based on machine learning. Most importantly, it is aims at being pleasant, ergonomic, and interesting to use, leveraging Virtual Reality (VR) interfaces. (*Abstract*)**

Keywords— Virtual reality, serious game, law enforcement, machine learning, counter terrorism data modelling *(key words)*

I. Introduction

For over two decades Virtual Reality (VR) technology is considered an excellent choice for creating virtual training platforms for first responders, law enforcement personnel and security officers [1]. This is because it can enable the development of realistic training settings based on immersive scenes in a three-dimensional (3D) Information Technology (IT) environment. Such settings enable trainees to acquire practical knowledge in the scope of ergonomic, realistic, yet safe environments. For instance, the users of VR applications can experience the feeling of threat without a need to interact with an adversary in a hazardous setting [2]. Hence, they obviate the need for training policemen in harsh and potentially dangerous environments.

The training value of VR environments is usually amplified in the context of gaming environments. Serious games are among the most prominent and effective applications for training practitioners in realistic settings. Serious games provide a fun way to train and educate. They are used by many industries to help employees learn new skills, but they are especially useful in the security industry. Security officers need a wide range of knowledge, from how to handle volatile situations to how to use their equipment properly. Serious games can teach these skills in an easy and engaging way that is usually more effective than traditional methods. Overall, using serious games in security forces training provides distinct benefits including: (i) They make training fun; (ii) They provide lessons that are easier to learn; (iii) They enable trainees to cope with more information in less time; and (iv) Employees that are trained through serious are more likely to retain the information. The integration of VR modules within serious games yields training environments that are more ergonomic, pleasant and easy to use, which reinforces the engagement of the trainees and the overall effectiveness of the training processes.

In recent years, a considerable number of VR-based serious games for security professionals have been developed, including games for cybersecurity professionals, first responders and law enforcement officers. Most of these games are focused on operational processes rather than on how to improve tactical and strategic decision making. In this context, they tend to focus on navigation and activities within on-the-job settings rather than on the acquisition, generation and analysis of intelligence information. This is also the reason why the make quite limited use of Machine Learning (ML) and Artificial Intelligence (AI) to process historic data and drive the end users' decision making. Moreover, to the best of our knowledge, there is a lack of AI-based VR-enabled environments that support Law Enforcement Agencies (LEAs) in predicting potential terroristic actions, as part of strategic-level and tactical-level decision making. Motivated by the lack of such gaming environment, this paper introduces a novel VR game for LEAs that helps officers understand and anticipate actions that are likely to be part of terroristic activity. Furthermore, the paper illustrates the use of AI modules to enhance the intelligence of the game in the direction of assessing terroristic actions related risks. In this direction, the game serves as a data generator module, which provides the ever-important data that are needed to train machine learning modules. The game is positioned against related work in serious game development and terroristic data modelling and generation. Its implementation is work in progress, as only a subset of the modules of the gaming engine have been implemented. The remaining of the paper is structured as follows: Section 2 presents related work in terroristic data modelling and serious games development. Section 3 illustrates the architecture of the gaming engine, including information about the VR modules. Section 4 presents main data entities of the game and their use in driving data generation and training of ML modules. It also presents gaming scenarios. Section 5 concludes the paper and outlines future work.

II. Related Work

A. Serious Games

Serious games have been developed for training purposes in various sectors, including healthcare [3], human resources [4], emergency management [5], and vocational training [6]. In the security sector, many serious games for cybersecurity training have been developed, including for example tabletop games for cybersecurity awareness [7] and digital forensics [8]. Moreover, there are various games that integrate VR functionalities and interfaces. The most prominent examples are found in emergency management and critical infrastructure protection [9], [10], where VR-based serious games are used to train stakeholders in complex processes like evacuation.

There are also VR platforms for training policemen in different settings [2], [11]. Such games facilitate law enforcement officers in simulating operations in complex scenarios, including unexpected and untrain situations where they have to respond fast and adequately. VR-based games alleviate the high cost and safety risk of real-life on the field training. In this direction, most training exercises focus on operational processes, notably processes that are difficult, expensive or risk to replicate in practice. Nevertheless, state of the VR games do not focus on strategic and tactical level tasks where historical data must be collected and analyzed, in conjunction with operational-level information. Likewise, existing games make very limited use of AI and ML modules in their application logic. To alleviate this limitation, serious games can serve as a basis for generating data and using them to train ML/AI algorithms to identify abnormal adversarial behaviors. The latter algorithms can facilitate the analysis of historic information in order to identify potential terroristic activities. To this end, state of the art techniques for terroristic modelling should be developed.

B. *Terroristic Modelling*

Most security and defense applications, notably the ones that process large datasets, exploit data models towards representing and sharing information. The semantic web has been acknowledged as a crucial tool for counter-terrorism researchers [12], given that ontologies provide the means of describing sequences of events, along with the social networks of terrorists and their organization. Moreover, ontologies provide the means for representing relationships within networks of individuals and organizations, which is very handy in the scope of applications that detect and track the evolution of communities. A large number of security applications employ general purpose ontologies for situation awareness [13], which are very common in applications that employ data fusion from multiple sources [14]. Over the years ontologies that are devoted to counter-terrorism applications have been also developed. They reflect theoretical concepts of terrorism including the representation of events, assets, and terroristic activities [15], [16]. These ontologies can be extended/ enhanced on the basis of concepts peculiar to specific terroristic attacks.

Beyond ontologies, we have also witnessed the emergence of models that capture actions, events and relationships, which are commonly related to terroristic activities. Indeed, both RISS [16] and Bennett [15] provide taxonomies of common terroristic activities and events, which they characterize as terroristic indicators. These taxonomies take into account the semantic of recent terroristic attacks such as 911 in New York. They have a significant amount of overlapping constructs and commonalities, while they seem to capture the activities that occurred during the planning of several terroristic attacks in the period 2000-20120 (such as the bombings in the London and Madrid metros). In [17] a system able to collect information about these terroristic indicators (based on sensors) has been developed, including algorithms for reasoning over these indicators with a view to predicting terroristic threats and activities. Overall, the data entities to be designed, integrated, and managed in the scope of a counter terrorism game must consider actions, events and other pieces of information that are common in terroristic activities [17].

III. Serious Game Architecture and Main Components

A. *Gaming Platform Engine*

The terroristic attacks training serious game is empowered by a general-purpose gaming engine, which supports multiple data-driven games for training law-enforcement agencies. The latter games are developed in the scope of the EU funded LAW-GAME project [18]. Specifically, LAW-GAME designs, develops and validates serious games for training LEA (Law Enforcement Agencies) on how to best perform analytical activities such as forensic examination, effective questioning, threatening, cajoling, persuasion, negotiation, as well as identification and analysis of terroristic activities. Different gaming functionalities are developed to support the above-listed activities, which are supported by a common set of game-independent modules and a set of game-specific modules that different for each one of the games. The common components include: (i) Data sources management: They collect and analyze information from various information sources, including real-time data streams and data-at-rest (e.g., procedures, evidence, lists etc.). Raw data from the various sources are pipelined to appropriate analytics functions towards generating important events for the trainees that use the serious games; (ii) Platform Core: This is the heart of the system that where data/event monitoring, data/event synchronization, and data organization takes place; (iii) Platform Client Application: This is the serious game specific modules that leverage intelligent data processing to create game specific events and trigger game specific activities; and (iv) System output components: These components disseminate information to components and users of the serious games.

B. *Serious Game VR Client Application*

The VR client application of the serious game will enable the interaction with the end-users. The VR Client application of the game comprises the following components: (i) Library module: It hosts internal resources for specific game scenarios. These vary from 3D models (e.g., FBX (Filmbox)) to materials, shaders, textures and animations; (ii) AI tools: These enable various AI-based functionalities including narration, conversation and dialogues generators, interactive storytelling, and incident scene analysis component); (iii) Data transfer module: It is in charge of the two way data transfer between the gaming platform and the VR application; (iv) Physics engine module: This module provides integration with a bballistic engine in support of scenarios that need it; (v) UI/UX modules: Enable the implementation of workflows that provide a graphic representation of game scenarios and scenes; (vi) Gamification engine: Allow trainers to set goals, achievements, points and rewards for specific actions in order to implement scoring within serious games; (vii) Authoring tool: Supports manual and automatic scene generator, along with reconstruction of real scenarios; (viii) Multiplayer module: This module synchronizes actions and interactions between users, objects and environments, in cases of multi-player scenarios; and (ix) Communication module: This module supports live audio communications between trainers and trainees.

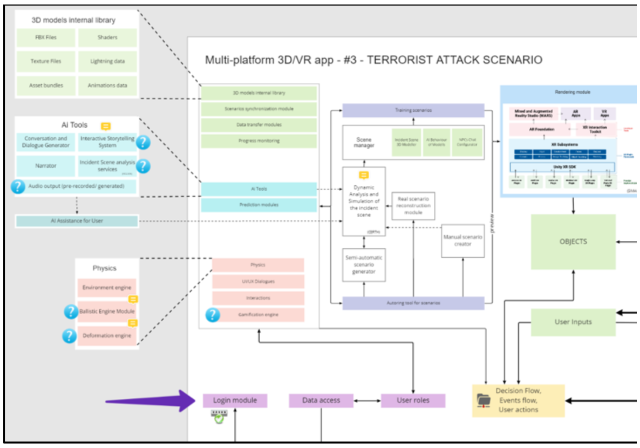

Fig. 1. Terroristic Attack Prediction Game Architecture

C. *Serious Game Architecture and Components*

The development of the terroristic prediction serious games leverages the gaming engine and VR client application presented in the previous version. Each user uses an instance of the VR client application to connect to the serious game and to perform actions in-line with the rules of the game. Fig. 1 depicts the architecture of the serious game, which comprises the following components: (i) Authentication: Supports registration, account management, user management and role management for the various trainees that use the game. Only properly authenticated users can gain access to the functionalities of the game based on their role; (ii) Data Lake: It provides the central data management point, where data from all VR Clients are synchronized; (iii) Analytics module: This module analyses information that is persisted in the data lake. It also connects to a conventional training platform (i.e., LMS (Learning Management System)) to access and process statistics in the form of learning analytics; (iv) Automatic Training Assessment: This tool collects information from the data lake towards performing functions like human emotion detection; (v) Operations Centre: This module provides support for social VR learning, while supporting chain of custody and crime records persistence using blockchain technology; (vi) Security module: This module performs data validation across all the different modules of the platform; (vii) Data repository: It is a repository where environmental information regarding objects, avatars, animations, scenarios and user logs is persisted. This information is important for configuring the operation of the game and is provided by the Authoring tool module; (viii) AI behaviour modelling and assessment: This module comprises AI and ML algorithms that learn the normal behavior of avatars leveraging data generated from the game. Moreover, it can identify and spot potentially abnormal and suspicious behaviors.

IV. TERRORIST ACTIVITIES PREDICTION DATA MODELLING AND GAME SCENARIOS

A. *Serious Game Context and Purpose*

Using the previous presented gaming platform, a multi-player game is designed and implemented. It involves users (i.e. avatars) belong to one of thefollowing two roles:

- Terrorist: Represents a member of a terrorist or activist group. It aims at successfully completing a series of actions towards launching a terroristic attack. The terrorist collects points based on successful actions and wins the game when it successfully completes the actions and launches the attack.
- LEA officer: This role represents an officer of the LEA. It aims at identifying terroristic actions towards preventing the attack. The LEA officer collects points based on the successful identification of actions and wins the game when it prevents the attack.

In practice LEA officers assume both two above roles when playing the serious game. The serious game is played towards the following ultimate objectives: (i) Training LEA officers in understanding the various indicators of terroristic actions and attacks, as well as in methods for correlating and analysing them. Based on this training LEAs will improve their ability to analyse counter terrorism information and will become more efficient in preventing terroristic actions; (ii) Generating data that can used to train develop AI modules for analysis and correlation of terroristic actions. These AI modules aim at assisting humans in the collection, analysis and correlation of information. Along with avatars, the game activities entail objects, messages, and actions, as illustrates in Table 1. Objects are non-human actors in the game scenes, while actions are terroristic-related activities. Finally, messages are used to convey important domain information (e.g., information about suspects) to the LEAs.

TABLE I. MAIN DATA ENTITIES OF THE SERIOUS GAME

Data Entity	***Description and Role in the Game***
Avatar	A human actor that participates in the game. The human actor can be either physical (i.e. a user playing the game) or virtual (i.e. participating in the game scenarios and scenes). Human actors / Avatars can represent terrorists, law enforcement officers, members of the public etc.
Object	A virtual object that is part of the game. Examples include buildings, buses, weapons, drones etc. Objects can be classified into stationary and mobile objects.
Action	An important action/event that links to an indicator of terroristic activity. Actions are typically linked to known indicators of terrorism in-line with the terrorist model of the game
Message	Denotes an important piece of information about terroristic activities (e.g., information about a stolen weapon or an arrested terrorist) that the LAW-GAME platform transmits/sends to one or more actors or objects.

B. *Terroristic Modelling*

According to the terroristic activities modelling literature (e.g., [14], [16], [17]) terrorists operate according to a well-defined plan, which includes a range of prerequisite actions that they should carry out prior to the launch of a terrorist attack. These actions fall typically in the following categories: (i) Actions towards pre-operational surveillance of the potential target, in order to gather information for purposes of planning their attack; (ii) Seeking and elicitation of information about the target, which complement the information gathered during the pre-operational surveillance; (iii) Probing and testing security measures of the target, in order to understand the security protocols in place; (iv) Acquisition of supplies, including collection of the materials that are necessary for their attack and (v) Engaging in practice sessions (in the form of a dry or rest run of their attack) in order to identify flaws and potential unanticipated situations that could happen during the course of their attack deployment and execution. The preparation of most terrorist attacks involves all of the above steps. Hence, the ability of the LEAs to identify, correlate and connect information associated with the above steps for a given target should raise the level of their alert about potential terrorist activity. A range of more specific actions are defined and associated with each one of the above types of activities. For example, persons or vehicles being seen in the same location on multiple occasions can be a sign of pre-operational surveillance in a location, while a series of false alarms requiring law enforcement or emergency services response can be an indication of probing security measures. Table 2 illustrates some sample actions and the users' gaming activities (i.e., sub-actions) that trigger them.

TABLE II. HOW GAMING ACTIVITIES TRIGGER ACTIONS

Action	Triggering Sub-Actions (Workflow)
FootSurveillance	Choose Target (Tx) → Inspect target from proximity → Look around → Check / test security measures → Intrusion to the building
VehicleSurveillance	Get into the car → inspect target → Take photos → Stay in illegal parking place
Information Seeking	Ask people around → Talk with security officer or people working in shops / neighborhood
TestAlarm	Trying to destroy a camera or leaving a bag near the target
PrepareBomb	Gathering ingredients to a flat → Visiting the flat multi times → Mixing the ingredients
PlaceBomb	Taking the bomb from a flat → Approach the target → Trigger the bomb → Place the bomb

The actions in Table 2 correspond to terroristic activities identified in the terroristic models of the literature, which are used in LAW-GAME as well. The implementation of the game is based on a user-friendly environment using Virtual Reality (VR). 3D representations of targets and resources are provided. A full unity 3D town is provided to represent the real world environment, where the game activities take place.

C. Artificial Intelligence

The LAW-GAME artificial intelligence module analyses the recorded sequence of played actions and provides indications and recommendations about the potential next move (i.e., sub-action) of the opponent. In this way, the player, benefits from AI-based analysis of large volumes of past events/moves across multiple games.

V. CONCLUSIONS AND FUTURE OUTLOOK

The paper has described the rationale behind the development of a serious game for training LEAs in terroristic activities prediction and analysis. It has also presented the architecture of the gaming platform that supports the implementation and execution of the game, along with the main technical modules of the platform. The modules enable the implementation of gaming scenarios comprising different sets of avatars, objects and actions. The latter are streamlined to the terroristic models of the game, which define the most common activities that are undertaken by terrorists prior to launching an attack. The presented design and implementation activities can be classified as work in progress, as the implementation of several modules (e.g., AI modules) in on-going. Our ambition is to finalize the implementation and deployment of the game, and to validate it based on the engagement of law enforcement officers as users of the gaming platform. The validation will focus on a variety of different aspects including training effectiveness and ease of use.

ACKNOWLEDGMENT

Part of this work has been carried out in the scope of the LAW-GAME Project, which has received funding from the European Commission under the H2020 programme (contract No. 101021714). The authors acknowledge support and contributions from all partners of the project.

REFERENCES

[1] J. S Hormann, "Virtual Reality: The Future of Law Enforcement Training," NCJ Number 156174, Journal FBI Law Enforcement Bulletin vol: 64 Issue: 7 pp: 7-12, July 1995.

[2] P. Caserman, P. Schmidt, T. Gobel, J. Zinnacker, A. Kecke and S. Gobel, "Impact of Full-Body Avatars in Immersive Multiplayer Virtual Reality Training for Police Forces," in IEEE Transactions on Games, doi: 10.1109/TG.2022.3148791.

[3] J. Guo, N. Singer and R. Bastide, "Design of a serious game in training non-clinical skills for professionals in health care area," 2014 IEEE 3nd International Conference on Serious Games and Applications for Health (SeGAH), 2014, pp. 1-6, doi: 10.1109/SeGAH.2014.7067096.

[4] P. Gebhard et al., "Serious Games for Training Social Skills in Job Interviews," in IEEE Transactions on Games, vol. 11, no. 4, pp. 340-351, Dec. 2019, doi: 10.1109/TG.2018.2808525.

[5] G. Jacob, R. Jayakrishnan, and K. Bijlani, "Smart fire safety: Serious game for fire safety awareness," in Information and Decision Sciences. Springer, 2018, pp. 39–47.

[6] A. Hamza, P. Pernelle, C. Ben Amar and T. Carron, "Serious games for vocational training: A compared approach," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, pp. 1-8, doi: 10.1109/AICCSA.2016.7945712.

[7] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education,". Computers and Security, 95, [101827].

[8] J. Yerby, S. Hollifield, M. Kwak, and K. Floyd, ''Development of serious games for teaching digital forensics,'' Issues Inf. Syst., vol. 15, no. 2, pp. 335–343, 2014

[9] J. Molka-Danielsen, E. Prasolova-Førland, M. Fominykh and K. Lamb, "Use of a Collaborative Virtual Reality Simulation for Multi-Professional Training in Emergency Management Communications," 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 2018, pp. 408-415, doi: 10.1109/TALE.2018.8615147.

[10] J. Haskins et al., "Exploring VR Training for First Responders," 2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), 2020, pp. 57-62, doi: 10.1109/VRW50115.2020.00018.

[11] J. Bertram, J. Moskaliuk and U. Cress, "Virtual police: Acquiring knowledge-in-use in virtual training environments," 2011 IEEE International Symposium on VR Innovation, 2011, pp. 341-342, doi: 10.1109/ISVRI.2011.5759669.

[12] A. Mannes and J. Golbeck, "Building a terrorism ontology", University of Maryland, College Park, 2005.

[13] M. Kokar, C. Matheus, and K. Baclawski. Ontology-based situation awareness. Information Fusion, 10(1):83–98, 2009.

[14] C. Matheus, M. Kokar, and K. Baclawski. A core ontology for situation awareness. In Proceedings of FUSION 03, pages 545–552, 2003.

[15] RISS/ROCIC Special Research Report, "Indicators of terrorist activity: Stopping the next attack in the planning stages", Dissemination restricted to Law Enforcement Agencies, 2004.

[16] B.T. Bennett, "Understanding, assessing and responding to terrorism: Protecting critical infrastructure and personnel," Hoboken, NJ: John Wiley & Sons, 2007.

[17] R. Sormani, J. Soldatos, S. Vassilaras, G. Kioumourtzis, G. Leventakis, I. Giordani and F. Tisato, "A serious game empowering the prediction of potential terrorist actions," Journal of Policing, Intelligence and Counter Terrorism, 11:1, 30-48, DOI: 10.1080/18335330.2016.1161222, 2016.

[18] H2020 LAW-GAME, "An Interactive, Collaborative Digital Gamification Approach to Effective Experiential Training and Prediction of Criminal Actions", https://cordis.europa.eu/project/id/1010217