INTELLIGENCE ANALYSTS' TRAINING THROUGH SERIOUS GAMES: THE LEILA PROJECT

A. ZANASI, F. RUINI & A. BONZIO
Zanasi & Partners, Italy.

ABSTRACT
Among the various initiatives directed at helping the intelligence community tackling today's security challenges, the EU FP7 research project LEILA (Law Enforcement and Intelligence Learning Applications) focuses on 'serious games' for improving the quality of intelligence analysts' training. LEILA investigates innovative methodologies for the development of core competencies required for performing intelligence analysis. Building upon an in-depth study of intelligence analysts' learning needs and inspired by a multitude of disciplines, LEILA developed a set of serious games, embedded into four comprehensive 'learning experiences' dedicated to intelligence analysis trainees. While the main target of LEILA is law-enforcement intelligence analysts, the competencies addressed by its learning experiences are potentially relevant to analysts operating across various sectors.
Keywords: cognitive biases; inference schemes; intelligence analysis, law enforcement; learning; LEILA; security; serious games; training.

1 INTRODUCTION

Over the last few years, security has become a top priority on the European political agenda. The rise of new threats, together with radical changes in the way people live, work and communicate, have increased the demand for sound intelligence analysis, while creating a set of complex challenges for security services. Improving the quality of intelligence analysis by means of more effective forms of training has been recognised as a key priority for coping with the challenges posed by today's scenarios. Following the multiple initiatives from the US for testing new ways to enhance the quality of training in intelligence analysis, the European Commission (EC) has also started taking steps in this direction. In 2014, the LEILA (Law Enforcement Intelligence Learning Application) project was launched under the EC's Seventh Framework Programme for Research and Technological Development (FP7) with the aim to provide law enforcement agencies with innovative training methodologies for their intelligence analysts, based on serious games.

The aim of this paper is to provide an overview of the work carried out during the LEILA project and to highlight the novelty of its findings. The paper begins by defining some of the key concepts underpinning the LEILA project, from 'law enforcement intelligence' to 'intelligence cycle'. This is followed by a review of some current trends and challenges in intelligence analysis training, with a particular focus on the growing popularity of serious game technology as a learning tool. The paper continues with a description of the main findings of LEILA as well as with an overview of the organisations involved in the project. The final section of the paper sheds some light on the most significant elements of innovation introduced by the LEILA project.

2 LAW ENFORCEMENT INTELLIGENCE AND THE INTELLIGENCE CYCLE

Within the realm of intelligence analysis (IA), the boundaries between governmental and corporate intelligence are progressively blurring. Both disciplines focus on technology, rely on sources such as social media, use text and data mining technologies. Often, the private

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://www.witpress.com/journals
DOI: 10.2495/SAFE-V7-N3-380-389

sector takes advantage of governmental intelligence to make business (e.g. McDonnell Douglas vs. Airbus or Raytheon vs. Thomson-Alcatel thanks to ECHELON). At the same time, government authorities often ask the private sector to participate in the development of intelligence (e.g. FBI-Apple encryption dispute, Yahoo! email scandal).

Despite some major overlaps, differences between law enforcement intelligence and other kinds of intelligence activities still exist. According to Carter & Schafer [1], national security intelligence deals with '*social, political, economic, and military issues relating with a nation's stability and safety*'. As the decisions it supports are often political in nature, national security intelligence does not always respond to strict legal requirements. On the contrary, law enforcement intelligence, being ultimately aimed at shaping the decisions and operations of police bodies, is subject to strict legal constraints.

The primary focus of LEILA is on intelligence activities conducted by law-enforcement agencies. Therefore, we borrow from Carter [2] a more comprehensive definition of the concept of law enforcement intelligence as: '*the end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgments and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution or project crime trends to support informed decision making by [law enforcement] management.*'

The concept permeating all intelligence activities is the 'intelligence cycle'. Underlying this concept is the notion that the production and use of intelligence follows a cyclical process consisting of multiple and interdependent steps. Every step of the cycle adds value to the initial input and contributes to its transformation into a completely different product [3]. According to its traditional interpretation, the intelligence cycle comprises five phases [4]: planning and direction, collection, processing, analysis and production, dissemination.

2.1 Planning and direction

This stage refers to the management of the intelligence cycle and the attribution of the single intelligence tasks. During this phase, the intelligence consumer sets out the requirements for the final intelligence product and plans the various intelligence activities needed for its achievement [5]. These activities include establishing the information needs, deciding how information is to be collected as well as defining a timetable for its collection. Requirements may also concern the particular form in which the final intelligence product must be delivered (e.g. a full report, a graph, a single piece of raw information, etc.).

2.2 Collection

A wide range of tools and techniques are employed by intelligence and law enforcement agencies for gathering raw data from all available sources. Collection methods depend on the nature of the information to be collected and the characteristics of the media it is transmitted through. There are five main categories of intelligence sources: Geospatial Intelligence (GEOINT), Human Intelligence (HUMINT), Measurement and Signature Intelligence (MASINT), Open-Source Intelligence (OSINT) and Signals Intelligence (SIGINT) [5]. To these, one may add a set of sub-disciplines, such as Imagery Intelligence (IMINT) and social media intelligence (SOCMINT), which have emerged in parallel to the spread of new technologies.

2.3 Processing

Once collected, the information needs to be converted into a format suitable for analysis. To transform raw and unstructured data into structured and unambiguous information, highly trained personnel and advanced technologies are required [5]. While making unprecedented amounts of data available to intelligence analysts, the rapid growth of IT technologies has created tools allowing to effectively process such data without incurring in the problem of information overload. Processing methods range from decryption, language translations and data reduction [6] to techniques such as data and text mining [7].

2.4 Analysis and production

The main purpose of this phase is to extract meaning from available data, converting raw inputs into a usable intelligence product [8, 9]. Such process requires '*the integration, evaluation, and analysis of all available data and the preparation of various intelligence products*' [9]. An intelligence product may consist either of single pieces of information being disseminated individually (sometimes referred to as 'the dots') – or of finished intelligence reports in which such dots are connected and conclusions about their meaning presented [6].

2.5 Dissemination

During the dissemination phase, the final intelligence product is delivered to the customers, who will then use it to support their decision-making. Dissemination may also induce the intelligence consumers to provide feedback on the received product, thus resulting in a new spin of the intelligence cycle.

3 CHALLENGES AND TRENDS IN INTELLIGENCE ANALYSIS TRAINING

Following the attacks on September 11th 2001 and the military invasion of Iraq in 2003, the US and their allies have devoted a great deal of resources to prevent future intelligence failures by improving the quality of intelligence analysts' training [10]. In the US, new training centres, either independent or belonging to larger organisations, have been set up for this specific purpose. In addition, training courses and curricula with a marked practical component have been introduced by both governmental agencies (e.g. the CIA, with its Career Analyst Programme) and academic institutions (e.g. the Intelligence Studies Department at Mercyhurst College, PA). Similar efforts, though of a lesser scope, have been undertaken by European countries like the UK, as witnessed by the recent flourishing of academic courses in intelligence (e.g. the Intelligence programme offered by the War Studies Department at King's College London [11]). Teaching methods have also undergone important changes over the past few decades. According to Marrin [10], the key to good intelligence analysis is no longer represented by the analyst's expertise on a specific issue but, rather, by the analyst's own reasoning skills. That is why training programmes in intelligence analysis are increasingly focused on structured analytical techniques, such as brainstorming, devil's advocacy, red team analysis, Team A-Team B, Analysis of Competing Hypotheses (ACH), key assumptions check and alternative futures.

Despite such transformations, many problems still undermine the effectiveness of analytic training in the intelligence sector. One of the weaknesses stems from the absence of a common training programme for intelligence analysts at entry-level, with single agencies

still maintaining the prerogative to instruct their trainees according to their specific mission and needs [12]. Another challenge has to do with the specific skills being taught during the training. A 2011 study of five different training providers in the UK, including private companies, law enforcement agencies and other public bodies, concluded that none of these institutions offered appropriate training for intelligence analysis [13]. Some of the programmes overestimated the statistical dimension of intelligence analysis at the expense of the investigative one, while others placed undue constraints upon the work of intelligence analysts by granting managers a control function over the analytical process. On a similar note, it has been observed that most currently available training programmes fail to adequately teach critical thinking skills: while training material on critical thinking is often included within courses, the reasoning process behind critical thinking tends to be addressed only minimally [14].

Another skill only marginally dealt with by current training programmes in intelligence analysis is *cognitive biases mitigation*. Richard J. Heuer, author of the first systematic study of cognitive biases applied to the intelligence domain [15], defined cognitive biases (CBs) as '*mental errors caused by our simplified information processing strategies'*. According to Heuer, CBs induce cognitive shortcuts and deviations in judgment based on factors such as '*memory, experience, education, cultural background, political or ideological bias, heuristics or simple rules of thumb*'. As an unconscious phenomenon, cognitive biases cannot be prevented just by being aware of their existence. Their mitigation requires deeper forms of intervention, targeting the very cognitive dynamics underlying people's reasoning.

While CBs are known to have a substantial impact on the work of intelligence analysts, few solutions have been proposed to reduce their negative effects. To fill such gap, the European Commission recently funded the RECOBIA (REduction of COgnitive Biases in Intelligence Analysis, http://www.recobia.eu) project, a three-year research initiative involving researchers from 9 different European organisations. Running from 2012 to 2015, RECOBIA resulted in the identification of a set of mitigation strategies pertaining to the realm of software tools, organisational measures and training. In the latter domain, the project highlighted the benefits of serious games-based training for enhancing analysts' awareness of cognitive biases and helping them to mitigate the associated negative effects.

4 SERIOUS GAMES

Serious games are tools – often digital in nature – exploiting techniques and processes typical of the entertainment sector for purposes other than entertainment [16]. Their popularity as a training tool stems from their capability to simulate real-world situations and foster the acquisition of skills otherwise difficult to develop. Compared to more traditional forms of learning, game-based learning is considered more suitable to provide dynamic, active and implicit learning modes [17]. In particular, gameplay has become highly valued as an educational tool for the possibility of teaching through experiential and declarative learning, by allowing players to fail and to try again [18].

Serious games so far have been applied to several domains, including business, military and healthcare. Over the past decade, however, the US intelligence community has demonstrated a particular interest in their use for improving the training of intelligence analysts. In 2011, the IARPA (Intelligence Advanced Research Projects Activity) launched a 10 million dollar-worth research initiative aimed at developing serious games to '*train participants and measure their proficiency in recognizing and mitigating the cognitive biases that commonly affect all types of intelligence analysis*' [19]. Known as the SIRIUS Programme, the project

resulted in the design of a set of computer games addressing various cognitive biases, like 'confirmation bias', 'projection bias', 'bias blind spot', 'anchoring bias', 'representativeness bias' and 'fundamental attribution error'. In one of those serious games, called MACBETH, the player impersonates an intelligence analyst tasked with preventing an impending terrorist attack under increasing time pressure. The game contains a specific section dedicated to mitigating the fundamental attribution error bias, in which the player must review past case files and make threat assessments on profiles of real-life individuals. As a de-biasing mechanism, the game encourages the player to rely on situational - as opposed to dispositional - cues by only allowing correct answers informed by at least 3 situational cues to be rewarded with the possibility of unlocking additional intelligence and progressing with the game [17, 20].

The same set of cognitive biases targeted by the SIRIUS programme has been the focus of another serious game developed in 2013, called 'The Mind's Lie', the game was originally designed as a table-top game, but it has now become available also in the form of an Android app, which can be freely downloaded. The game requires players to examine different real-world scenarios, spot the cognitive biases associated with each scenario and share those findings with the other players. Then, the game foresees that each player has to convince the others about the validity of his/her interpretation [21]. To mitigate cognitive biases, the game uses different pedagogical strategies, including 'peer-learning' and 'retrieval practice' [22]. The former refers to an educational approach in which learning objectives are achieved by students through interactions with other students. The latter relies instead on the idea that constantly recalling details, strategies and patterns from memory facilitates this recall over time.

5 THE LEILA PROJECT

Year 2014 saw the launch of one of the first European initiatives dedicated to the development of serious gaming solutions for improving the training of law enforcement intelligence analysts. Funded by the European Commission (EC) under the Seventh Framework Programme (FP7), the LEILA (Law Enforcement Intelligence Learning Applications, http://www.leila-project.eu) project aims to provide law enforcement agencies with an innovative training methodology based on a set of 'learning experiences' designed to improve cognitive capabilities and reasoning skills both at individual and group level. The ultimate goal of LEILA is the production of effective and innovative serious games to be deployed flexibly to security actors as well as beyond.

The LEILA project involved the following organisations:

- Center for Security Studies (KEMEA, http://www.kemea.gr): research centre of the Greek Ministry of Public Order and Citizen Protection, focused on security policies, acting as project coordinator;
- Alpha Labs (http://www.alpha-simulations.com): French spin-off company of the INSEAD's Centre for Advanced Learning Technologies (CALT), specialised in the development and distribution of advanced learning technologies and Web 2.0 tools;
- FVA (http://www.fvaweb.it): Italian company operating in the field of ICT and new media communications;
- GLOBO Technologies SA (http://www.globogr.com): Greek IT company specialised in the design and implementation of integrated advanced technological services;
- ORT France (http://www.ort.asso.fr): member of the ORT World network, it is an NGO with expertise in innovative strategies related to ICT involved in research, consulting and technology services;

- 'Carol I' National Defence University (NDU, http://www.unap.ro): highest military education institution of the Romanian Ministry of Defence, involved in research and training the area of national security and defence;
- Zanasi & Partners (Z&P, http://www.zanasi-alessandro.eu): Italian SME specialised in research, training and advisory on security, intelligence and their enabling technologies.

The LEILA consortium developed four distinct learning experiences: the 'VUCA (Volatility, Uncertainty, Complexity and Ambiguity) Challenge', the 'WhatATeam! Challenge', 'LabRint' and 'Cyberint'.

5.1 The 'VUCA (Volatility, Uncertainty, Complexity and Ambiguity) Challenge'

The 'VUCA Challenge' learning experience is designed to test the ability of participants to deal with crisis scenarios, within a context of limited time availability, by filtering through large amounts of information and interactions in order to solve a number of complex situations. In doing so, it addresses additional competencies relevant to the work of intelligence analysts, like the ability to mitigate cognitive and behavioural biases such as the 'overconfidence bias' and the 'fundamental attribution error' bias".

The VUCA Challenge begins with a game focusing on overconfidence and estimates quality. The player is asked to provide a series of estimates within 15-second time intervals before being debriefed by the instructor. This game is followed by a learning module based on a security scenario (inspired by the 2014 football World Cup in Brazil), in which players have access to a wide array of information and are tasked with demonstrating their understanding of the situation as well as assessing different types of threats emerging throughout the scenario. The following module consists in a simulation exercise (the 'WhatADay! Challenge') in which the participant has to prove his/her ability to solve three problems in parallel, operating under time pressure and dealing with large amounts of information sources and competing requests that appear in real-time. At the end of the simulation, similarly to what happens at the end of the first module (estimates game), the trainee takes part in a debriefing session focused on the analysis of his/her performance. The VUCA learning experience can also include a follow-up stage in which trainees are asked to implement, in their daily job, an individual action plan agreed with the instructors following the results achieved using the serious games. After a three-month period, the trainees report to the instructor about the effects deriving from following the action plan.

5.2 The 'WhatATeam! Challenge'

The 'WhatATeam! Challenge' learning experience focuses on the development of the key competences needed for successfully operating in diverse and distributed teams, as required by several cross-organisational and international cooperation situations that intelligence analysts face. The critical competencies addressed fall under the umbrella term 'enhanced collaboration skills'. The primary function of these skills is to enable good performance at individual and team level, as well as at organisational and inter-organisational level.

The experience is articulated into progressive learning stages. It starts with a module focused on how to identify barriers to effective collaboration when dealing with complex organisational or inter-organisational scenarios. The reference scenario addresses issues similar to those that affected US intelligence agencies before and during the 9/11 attacks.

This module is followed by a game-like team experience (the 'EagleRacing' phase) in which trainees, over a period of 7 weeks, operate as a virtual team. During this phase, participants are challenged to reach consensus using different collaboration tools, make joint risk assessments and collaborate to determine the best decision in a video-based scenario which evolves based on the teams' decisions. At the end of this simulation, two additional game-based modules help participants to gain awareness of their own natural current strengths and weaknesses as well as to identify the behaviors that may best contribute to enhance the team's effectiveness and cohesiveness.

5.3 'LabRint'

LabRint is a learning experience designed to improve the performance of intelligence analysts by targeting a set of required competencies. The game places particular emphasis on rational thinking, thinking disposition, creative attitude and open mindedness.

LabRint develops along four different stages:

1. An introductory video illustrates the reference scenario, which revolves around a security event taking place in a fictitious Middle Eastern country. At the end of the video, the analyst is presented with three possible hypotheses about the exact nature of the event, and has to choose which one is true:
   - H1. a terrorist attack;
   - H2. an armed robbery;
   - H3: a personal revenge;
2. The analyst receives a sequence of 47 pieces of information ('events'), from which he/she must select the ones that are relevant for evaluating the three hypotheses. Every time an event is presented, the analyst is asked to structure the pieces of information that the event includes into 'evidence'. To that end, the analyst has to look into six different drop-down lists, respectively dedicated to answer the "Who?", "What?", "Where?", "When?", "How?" and "Why?" questions;
3. Once the set of evidences has been created, the analyst is asked to structure it under the form of an inference scheme, the vertices of which are the evidences created and the three hypotheses, while the edges connect vertices that contradict each other. More precisely, given two vertices A and B, there will be an arrow of origin A and extremity B if and only if A being true implies that B is false;
4. The analyst has to use the inference scheme to determine which of the three hypotheses is true. LabRint returns a score based on the correctness of the inference scheme and the hypothesis being selected.

5.4 'Cyberint'

While in 'LabRint', the player is confronted with an armed attack scenario, in 'Cyberint', he/she must deal with a cyber-security scenario instead. Also in this case, the learning experience requires the player to analyse several incoming pieces of information in order to determine which of three hypotheses is correct. Cyberint develops along the same four steps into which LabRint is articulated.

During the LEILA project, all four learning experiences were subjected to test and evaluation by relevant end-users. Such process consisted of a series of pilot workshops giving

intelligence analysts, members of law enforcement agencies and other target end-users the opportunity to try out and provide feedback on the LEILA learning experiences. A first round of pilot sessions was carried out in 2015, with dedicated workshops taking place in Romania and Greece. A second pilot round was successfully completed in 2016, with the execution of pilot sessions in Greece, France, Italy and Romania.

6 LEILA'S INNOVATIONS

The LEILA project has brought some important innovations to the domain of intelligence analysis training. One of them pertains to its holistic approach, which combines insights from various disciplines. For its conceptual framework, LEILA relies on insights from the following domains:

- cognitive, psychological and cultural biases that may cause data interpretation errors;
- Bayesian approaches to decision-making under uncertainty;
- preference elicitation and inference schemes through argumentation and dialog games as well as through case-based reasoning;
- Games of Deterrence-based inference schemes as a solution to the problems raised by Bayesian approaches to decision-making [23].

At the beginning of the project, the consortium engaged in a careful study of various issues pertaining to such disciplines in order to ensure the solidity of the project's theoretical foundations. A review of existing training approaches in intelligence analysis was also carried out in an effort to highlight the core skills needed by intelligence analysts as well as existing gaps in current training programmes. This effort resulted in the identification of a set of user requirements and learning needs for intelligence analysts, from which the consortium has drawn a more basic set of abilities and soft skills (defined as 'Competence Development Enablers') to be targeted by the LEILA learning experiences. These represent the preliminary competencies an intelligence analyst must acquire in order to develop the core competencies (e.g. critical thinking) needed to perform at best.

In addition to critical thinking, the array of competencies addressed by LEILA includes rational thinking, creative attitude, collaboration and communication skills, awareness and mitigation of cognitive biases, capabilities in filtering and analysing large datasets as well as decision-making under social and time pressure. Some of these skills are likely to be particularly useful to analysts working in law enforcement and national security intelligence, but may also be beneficial to those operating in industry, economy, society, both in local and global organisations.

An important innovation introduced by LEILA is the flexibility of its proposed learning model. The methodology underlying the design of LEILA learning experiences addresses different categories of end-users by supporting the acquisition of competences at individual but also at team level and, indirectly, at organisational level. The LEILA learning experiences offer various deployment options: they may be delivered to trainees either as part of online/offline sessions or in a blended format mixing virtual and in presence interactions, with or without the support of a facilitator as well as both in real time and asynchronously. Furthermore, they can be easily tailored in terms of sequence and selection of modules, introduction of new content as well as adaptation to specific schedules and curricula. Such element of flexibility is particularly emphasised in the LabRint and Cyberint learning experiences, in which players have the opportunity to re-play the same session in order to spot possible

failures and traps, decide whether to play individually or as a team as well as customise scenarios, missions and tasks.

A further peculiarity of the LEILA learning experiences is their ability to successfully combine multiple pedagogical approaches together. Such characteristic is shared by all LEILA learning experiences, as each of them consists of separate modules addressing a specific set of competencies through different forms of learning. Some of the learning modules proposed by LEILA rely on highly interactive computer simulations, presenting trainees with complex situations and requesting them to either answer a series of verification questions or operate autonomously within the reference environment in order to complete a certain mission. Other modules are centred upon 'conceptual model reconstruction games' in which, starting from a validated conceptual model (for example, a model describing the actions to undertake in a certain situation), participants are induced to gradually 'discover' and 'build' the model themselves. To that end, the trainees have to assess a number of situations/scenarios narratives/questions, also relying on computer-based 'dialog games'. Simple game dynamics, such as challenging trainees to accomplish a mission within a clearly defined playful context, are also exploited as a way to help the participants grasping new concepts or expose them to their own level of competence in a given area.

7 CONCLUSION

Traditional training methodologies are no longer sufficient for acquiring the core competencies needed to perform good intelligence analysis in an increasingly complex, IT-dominated and rapidly changing world. With the LEILA project, the European Commission has demonstrated its willingness to explore alternative pathways for empowering law enforcement intelligence analysts to tackle the challenges associated with their modern operational environment. The learning methodology developed by the LEILA consortium, based on a set of flexible serious games integrating insights from various disciplines and extensively validated by European end-users, represents a promising solution in this respect. The maturity level of the solutions built by LEILA makes it possible for European organisations to adopt them immediately. In addition to intelligence analysts operating in the law enforcement sector, domains such as industry, economy and society could also benefit from the findings of LEILA, opening a potentially large diffusion space for its proposed learning methodologies. Further research into the educational potential of serious game technology, building upon the results of LEILA, could lead to new opportunities in the domain of law enforcement intelligence as well as in many other fields where quick and accurate information analysis is critical.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 608303.

REFERENCES

[1] Carter, D.L. & Schafer, J.A. The future of law-enforcement intelligence. *Policing 2020: exploring the future of crime, communities, and policing*, ed. Schafer, J.A., U.S. Federal Bureau of Investigation: Washington DC., pp. 226–256, 2007.

[2] Carter, D.L., *Law enforcement intelligence: a guide for state, local, and tribal law enforcement agencies.* CreateSpace Independent Publishing Platform: Lavergne, TN, 2012.

[3] Krizan, L., *Intelligence essentials for everyone*, Books for Business: Washington DC, 2003.

[4] The Intelligence Cycle; *Central intelligence agency*, available at: https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html
[5] The six steps in the intelligence cycle; U.S. Department of Homeland Security, Fusion Center, available at: http://fusioncenter.golearnportal.org/rawmedia_repository/b4e1b-56dcf572f53b00ee43a31b34223?/document.pdf
[6] Intelligence Branch; Federal Bureau of Investigation, available at: https://www.fbi.gov/about/leadership-and-structure/intelligence-branch
[7] Zanasi, A., (ed). *Text mining and its applications to intelligence, CRM and knowledge management*, WIT Press: Southampton, UK, 2007.
[8] Gill, P. & Phytian, M., *Intelligence in an insecure world*, Polity Press, Cambridge, UK, 2012.
[9] Richelson, J.T., *The US intelligence community*, Westview Press: Boulder, CO, 2011.
[10] Marrin, S., Training and educating U.S. intelligence analysts. *International Journal of Intelligence and Counter Intelligence*, **22(1)**, pp. 131–146, 2009. https://doi.org/10.1080/08850600802486986
[11] Goodman, M. & Omand, D., What analysts need to understand: the king's intelligence studies programme. *Studies in Intelligence*, **52(4)**, 2008.
[12] Johnston, R., *Analytic culture in the U.S. intelligence community. an ethnographic study*, Government Printing Office: Pittsburgh, PA, 2005.
[13] Training; IntelligenceAnalysis.net, available at: http://www.intelligenceanalysis.net/Training.htm
[14] Moore, D.T., *Critical thinking and intelligence analysis*, National Defense Intelligence College Press: Washington D.C., 2006.
[15] Heuer, R.J., *Psychology of intelligence analysis*, Books Express Publishing: Saffron Walden, UK, 2010.
[16] Libes, D. & O'Connell, T., Applying serious games to intelligence analysis. *Proceedings of SEA '07, the 11th IASTED International Conference on Software Engineering and Applications*, ACTA Press: Anaheim, CA, pp. 311–317, 2007.
[17] Dunbar, N.E., *et al.*, Implicit and explicit training in the mitigation of cognitive bias through the use of a serious game. *Computers in Human Behavior*, **37**, pp. 307–318. https://doi.org/10.1016/j.chb.2014.04.053
[18] Gee, J.P., *What video games have to teach us about learning and literacy*, St. Martin's Griffin: New York, NY, 2007.
[19] Sirius; IARPA, available at: https://www.iarpa.gov/index.php/research-programs/Sirius
[20] Dunbar, N.E., *et al.*, MACBETH: Development of a training game for the mitigation of cognitive bias. *International Journal of Game-Based Learning*, **3(4)**, pp. 7–26, 2013.
[21] Richey, M.K., The mind's lie: games-based learning for critical thinking. *The International Journal of Humanities Education*, **12(1)**, 2014.
[22] Game-Based Learning and Intelligence Analysis: Current Trends and Future Prospects; E-International Relations, available at: http://www.e-ir.info/2013/08/07/game-based-learning-and-intelligence-analysis-current-trends-and-future-prospects/
[23] Rudnianski, M., Sadana, U. & Bestougeff, H., Bayesian networks and games of deterrence. *Recent advances in game theory and applications*, eds. Petrosyan, L. & Mazalov, V., Springer Verlag, pp. 201–224, 2016.