Gamified Training for Cyber Defence: Methods and Automated Tools for Situation and Threat Assessment

Joni A. Amorim, Dr.
University of Skövde - HiS
Kanikegränd 3, Box 408, SE-541 28, Skövde
SWEDEN

joni.amorim@gmail.com

Maurice Hendrix, Dr.
The Serious Games Institute, Coventry University
Coventry University Technology Park, Cheetah Road, Coventry CV1 2TL
UNITED KINGDOM

maurice@mauricehendrix.co.uk

Sten F. Andler, Dr.
University of Skövde - HiS
Kanikegränd 3, Box 408, SE-541 28, Skövde
SWEDEN

sten.f.andler@his.se

Per M. Gustavsson, Dr.
Swedish National Defence College - Försvarshögskolan
Drottning Kristinas väg 37, 115 93, Stockholm
SWEDEN

per.m.gustavsson@fhs.se

ABSTRACT

This work considers training needs for cyber defence and discus the gamification of training. The use of game play mechanics will be considered with a special emphasis on strategies to encourage users to engage in desired secure behaviours. The use of games and game play mechanics has been shown to be able to make the training more engaging. Serious games may as well help increase motivation amongst learners. A possible design of a gamified training system for cyber security that complies with these requirements is introduced. Based on these analyses, the paper concludes for the feasibility of the approach overall.

1.0 INTRODUCTION

The word “cyber” was extracted from “cybernetics”, which was coined by the mathematician Norbert Wiener (1894-1964), from the Greek word “kybernetes” for “steersman” and possibly based on the French word “cybernétique” for “the art of governing”. “Cybernetics” traditionally means the control of mechanical and electronic systems designed by humans. A “cyber environment” includes “users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks” (ITU, 2008). The term “cyber space” is often used to “describe systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks” (ITU, 2011).

The frequency of cybercrimes and cyber-attacks is increasing, as has been recognised by the Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization (NATO, 2010), adopted by Heads of State and Government in a NATO Summit in 2010. This Strategic Concept document from NATO presents fundamental security tasks and identifies the central features of the new security environment. The document specifies the elements of the Alliance's approach to security while providing guidelines for the adaptation of its military forces. The document indicates the following: "Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks."

The Strategic Concept document also stresses that, in order to ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security, it is essential to "develop further our ability to prevent, detect, defend against and recover from cyber attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations" (NATO, 2010). Training of key personnel in many different capacities across the NATO is essential, as a way to develop and enhance the different abilities needed to prevent, detect, defend against and recover from cyber-attacks. Different strategies may be used for training, which include more traditional methods such as face-to-face lectures, digital texts and videos, but also emerging training technologies such as simulators and serious games.

This paper focuses on the gamification (ALDRICH, 2009; SCHELL, 2008) of training for cyber security, considering the protection of communication and information systems. Put simply, gamification is the use of game mechanics and game thinking to engage users in solving problems. The training content and/or the exercises of courses may be gamified, in this way resulting in a serious game. In the case of cyber security, a motivating scenario would have, for example, somebody who practices unsafe behaviour and would need to engage in the appropriate training to change this behaviour. The process of gamefication of training could consider using game strategies to train users as a way to help an organization to prevent this unsafe behaviour. In a concrete setting, government workers could be using their electronic mail unsafely. In a gamefied training, the students would receive points that would go on a leaderboard. In this case, a leaderboard may be understood as a board displaying the names and current scores of the leading competitors, in the same way it happens in a golf tournament, for example. The leaderboard could be a physical one but it could also be presented in a webpage. Different rewards could be given to the students according to their performance during the training. An important question for the human resources department would be: Are there any other rewards besides "looking good" on the leaderboard? Having rewards like days off, money, training, etc. could motivate even more these government workers, or students in this specific case, to excel in the gamefied training.

Within this perspective of the gamification of training on cyber security and related topics, the use of methods and automated tools for situation and threat assessment are considered while having the information fusion theory as a theoretical framework. In the sequence, we analyse training needs for cyber defence and discus its gamification. A possible design of a gamified training system for cyber security that complies with these requirements is introduced. Based on these analyses, the paper concludes for the feasibility of the approach overall.

2.0 THREATS AND CYBER WARFARE

A threat may be understood as a declaration of an intention or determination to inflict injury in retaliation for, or conditionally upon, some action or course.; it is an indication or warning of probable trouble. A cyber threat may originate externally or internally; it is a potential cyber event that may cause unwanted outcomes, in this way harming systems and organizations. According to a recent report on cyber threats, "cyber espionage and cyber sabotage are already a reality" (SYMANTEC, 2013). The same report notices an expansion of traditional threats into new forums like social media and mobile devices.

According to the NATO National Cyber Security Framework Manual (KLIMBURG, 2012), “governments, businesses, and citizens know intuitively that cyberspace is man-made and an ever-expanding environment, and that therefore the definitions are also constantly changing”. This Manual confirms that different terms related to the protection and preservation of confidentiality, integrity and availability of information are often used interchangeably. In the case of the term “cyber security”, the document indicates that it encompasses “information security” and “ICT security”. Despite the many varying definitions, the Manual stresses the importance of cyber security: protecting the critical infrastructures, protect government secrets and enable national defence.

A well-known definition for “cyber security” follows (ITU, 2008): “Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality”.

Since security features tend to increase the cost of systems while most often turning them more difficult to use, it may be a good practice to conduct a threat assessment in order to identify the relevant threats against which protection is needed. After listing the assets that require protection, a threat analysis must happen with at least the following steps being considered (ITU, 2008): "a) identifying the vulnerabilities of the system; b) analysing the likelihood of threats aimed at exploiting these vulnerabilities; c) assessing the consequences if each threat were to be successfully carried out; d) estimating the cost of each attack; e) costing out potential countermeasures; and f) selecting the security mechanisms that are justified (possibly by using cost benefit analysis)”. The threat analysis is also important to subsidise the definition of the training needs for all stakeholders involved.

Cyber threats are now relevant not only to organizations and individuals, but also to nations considering the many serious security challenges perceived in a continuously changing “threatscape” (ANDRESS & WINTERFELD, 2011). As a consequence, the traditional war-fighting domains of land, air, sea and space are no longer the only ones to be considered by nations. With the increase of the use of networks like the Internet for different applications, a fifth war-fighting domain is defined: the cyber world. In this way, it is essential to prepare the twenty-first century workforce of every country through high quality training and education aimed at dealing with the persistent cyber threats.

This brings about the need to investigate better ways to educate in Science, Technology, Engineering, and Mathematics (STEM) and also to train in cyber security. This twenty-first century workforce will have to develop competencies to defend their countries in the new World Wide Web’s Wild West (W5): the cyber world. While discussing cyber warfare, ANDRESS & WINTERFELD (2011) suggest that the Internet nowadays could be portrayed like the Wild West is in American movies: “Indian attacks, Mexican ‘banditos’, bad weather, criminals from our own community, and Mexican Army invasions”. In other words,

the W5 would have guerrilla warfare, non-state actors with possible informal support from their host nation, noise in the system making things unpredictable, threats to the community requiring aid from state or federal government, and cyber military invasions. In the past, an enemy nation would try to steal weapon system design documentation using infiltrated spies, for example; nowadays, it would be preferable to break into the servers that are storing the documentation.

This "threatscape" drives countries into the elaboration of national cyber security strategies. The elements of cyber security programmes should include the following, according to the ITU National Strategy Guide for cyber security (ITU, 2011): (1) top government cyber security accountability so that leaders would be accountable; (2) national cyber security coordinator to oversee activities; (3) national cyber security focal point for activities dealing with the protection against all types of cyber threats; (4) legal measures; (5) national cyber security framework with security requirements; (6) computer incident response team to analyse cyber threat trends, coordinate response and disseminate information; (7) cyber security awareness and education to raise awareness about cyber threats; (8) public-private sector cyber security partnership; (9) cyber security skills and training programs for cyber security professionals; and (10) international cooperation in order to better consider the transnational nature of cyber threats. The need for cyber security awareness and education programs is evident.

3.0 THREATS AND INFORMATION FUSION

The use of methods and automated tools for situation and threat assessment may be considered while having information fusion theory as a theoretical framework. In this way, this section presents some fundamental concepts related to information fusion before discussing some of the main threats considered to be relevant to the research presented in this paper. Many of these threats are directly related to information fusion, as shown in the literature (LLINAS, 2013).

Information is sometimes used as another word for data. Alternatively, information may be viewed as the meaning given to data by the way in which it is interpreted. The rapid evolution of technology drives a continuous reshaping of definitions of both data fusion and information fusion (BLASCH & STEINBERG, 2013; DAS, 2013; STEINBERG, 2013). The following paragraphs present some usual definitions.

In this text, "data fusion" may be understood as a "process to organize, combine and interpret data and information from various sensors and sources (e.g., databases, reports) that may contain a number of objects and events, conflicting reports, cluttered backgrounds, degrees of error, deception, and ambiguities about events and behaviours" (KESSLER & WHITE, 2008).

On the other hand, "information fusion" is understood as the "the synergistic integration of information from different sources about the behaviour of a particular system, to support decisions and actions relating to the system" (ANDLER & BROHEDE, 2008).

In this perspective, information fusion involves gathering information, fusing this information and interpreting the result. It is necessary to merge information for the subsequent manipulation and treatment. The combination of raw data from different sources with available information, tends to provide a better understanding of various phenomena of interest. Accordingly, it is essential to use methods to transform and identify potential sources of information, to automate the merging process, to understand the effects of certain information in different situations related to decision-making, and to better develop information systems that make use of fusion (ANDLER & BROHEDE, 2008). Methods and automated tools for situation and threat assessment may be developed using information fusion theories. Despite this, it is important to first identify the most relevant threats.

A report on security (FORWARD CONSORTIUM, 2010) identifies twenty-eight threats while presenting a risk assessment for each one of them based on severity and likelihood. They are the following, with 1 representing the first one in the rank, and so on: (1) threats due to parallelism; (2) threats due to scale; (3) underground economy support structures; (4) mobile device malware; (5) threats related to social networks; (6) routing infrastructure; (7) denial of service; (8) wireless communication; (9) unforeseen cascading effects; (10) false sensor data; (11) privacy and ubiquitous sensors; (12) user interface; (13) the insider threat; (14) system maintainability and verifiability; (15) hidden functionality; (16) new vectors to reach victims; (17) sensors and RFID; (18) advanced malware; (19) virtualization and cloud computing; (20) retrofitting security to legacy systems; (21) next generation networks; (22) IPv6 and direct reachability of hosts; (23) naming (DNS) and registrars; (24) online games; (25) safety takes priority over security; (26) targeted attacks; (27) malicious hardware; and (28) use of COTS components. Many of these threats are directly related to information fusion, like false sensor data, sensors and RFID; the literature on information fusion presents additional evidence of this link (GIACINTO, ROLI & SANSONE, 2009).

4.0 ANALYSIS OF TRAINING NEEDS

The training needs for cyber defence would include the typical cyber security skills. They may be grouped in three categories, according to the International Telecommunication Union (ITU, 2011): managerial, information assurance and technical. For the managerial category, we have: cyber security strategy; legal and regulatory; cyber security business case formulation; IT base skills; staff management skills and/or leadership skills; personnel security; multi-disciplinary skills related to technology, people and others; communication skills; cybercriminal psychology; and cyber ethics skills. For the information assurance category, we have: cyber security policies, standards and procedures; risk management; system accreditation; compliance checking; audit and monitoring; user rights and responsibilities; incident management; process design; assurance, trust and confidence mechanisms. For the technical category, we have: IT technical skills related to security management; IT technical skills related to security deployment; security design principles like zoning; resilient infrastructure; data protection and/or system administration; cryptographic and applied crypto skills; data custodianship; operational security; and incident management.

Other perspectives for cyber security skills exist. In the case of IISSCC (2013), a certifying body that meets the requirements of ANSI/ISO/IEC Standard 17024, different credentials and certifications exist, each one asking for different skills and experience: Associate of $(ISC)^2$; SSCP; CAP; CSSLP; CISSP; CISSP Concentrations; CCFP; and HCISPP. As an example, for the CISSP, or Certified Information Systems Security Professional (CISSP) certification, an exam is based on the following ten domains: (1) Access Control; (2) Telecommunications and Network Security; (3) Information Security Governance and Risk Management; (4) Software Development Security; (5) Cryptography; (6) Security Architecture and Design; (7) Operations Security; (8) Business Continuity and Disaster Recovery Planning; (9) Legal, Regulations, Investigations and Compliance; and (10) Physical (Environmental) Security. The CISSP relates to job functions like Security Consultant, Security Manager IT Director/Manager, Security Auditor, Security Architect, Security Analyst, Security Systems Engineer, Chief Information Security Officer, Director of Security and Network Architect.

A third perspective would derive from the Department of Homeland Security's Essential Body of Knowledge (EBK) for IT Security (SHOEMAKER & CONKLIN, 2011). In connection with the EBK, the National Cyber Security Workforce Framework outlines 31 functional work specialties within the cyber security field. The Framework also identifies knowledge, skills, and abilities associated with each specialty area. The areas of expertise required for successful performance of a role would be the following 65: Capacity Management; Computer Forensics; Computer Languages; Computer Network Defence; Computer Skills; Computers and Electronics; Configuration Management; Contracting/Procurement; Criminal Law; Cryptography; Data Management; Database Administration; Database Management Systems; Embedded Computers; Encryption; Enterprise Architecture; External Awareness; Forensics; Hardware; Hardware Engineering; Human Factors;

Identity Management; Incident Management; Information Assurance; Information Management; Information Systems Security Certification; Information Systems/Network Security; Information Technology Architecture; Information Technology Performance Assessment; Infrastructure Design; Internal Controls; Knowledge Management; Legal, Government, and Jurisprudence; Logical Systems Design; Mathematical Reasoning; Modelling and Simulation; Multimedia Technologies; Network Management; Object Technology; Operating Systems; Oral Communication; Organizational Awareness; Personnel Safety and Security; Political Savvy; Project Management; Public Safety and Security; Quality Assurance; Reasoning; Requirements Analysis; Risk Management; Security; Software Development; Software Engineering; Software Testing and Evaluation; Surveillance; Systems Integration; Systems Life Cycle; Systems Testing and Evaluation; Teaching Others; Technical Documentation Technology Awareness; Telecommunications; Vulnerabilities Assessment; Web Technology; and Writing.

A more in-depth discussion on training needs for cyber security may be found in AMORIM et al. (2013), where the authors discuss training needs with a focus on privacy and security by design. ANDRESS & WINTERFELD (2011), on the other hand, present a categorization of cyberspace challenges by resources required and level of complexity before discussing the necessary skills involved and threat/risk awareness aspects related to people. Anyway, the three perspectives briefly presented in this section demonstrate the high complexity of training development for cyber security content.

5.0 GAMIFICATION AS A NEW APPROACH

People generally learn and remember best what they study when they "do the real things" by themselves or, at least, when they are simulating that they are doing. Serious games could provide an environment where the learner may simulate actions in a more engaging way. In fact, it has been shown that serious games can be effective learning materials (BACKLUND & HENDRIX, 2013). With that in mind, the training should be designed in a way that the students function as active participants as occurs in simulations and serious games. In this section, we discuss gamification as a new approach.

In a way, it is still more common to have training with simulators (CHUNG, 2003) nowadays, which is the "traditional" approach. But the use of gamefied training tends to grow in importance with time. Various different technologies have been used over the years in training and education. Defence related training has traditionally relied heavily on practical exercises in a simulated environment. When it comes to cyber defence most of practical exercises are based on digital simulations. A recent trend sees the use of computer games for serious purposes in so called serious games (ZYDA, 2005). One of the most well-known serious games is indeed the defence training/recruitment game America's Army (AGS, 2013). These serious games have been shown to be able to provide a fun and effective learning environments (BACKLUND & HENDRIX, 2013).

Gamification is now emerging as a new trend, where instead of creating spate computer games for training, game mechanics are incorporated in systems people use in their normal everyday practice and these mechanics are then used to incentivise desirable behaviour. Game mechanics used range from stars, badges and points to social status in social networks. A recent trend is the gamification of mobile entertainment games, where small in-game upgrades can be had for a small financial fee, motivating players in this case to get their credit card out for a game that they have already paid for or may even be free. These mechanics can also be leveraged for training purposes, or to promote desirable behaviours. For example, good behaviours can lead to gaining points that can be used to "buy" things. These things can be anything that has at least a perceived value to the individual.

The gamification management may happen in different ways (KAPP, 2012) but two methods prevail for developing gamification efforts: the ADDIE process and the Scrum approach. It is also possible to use a hybrid of the two models that should be modified accordingly to each project: determine outcome of the

learning, determine the type of content to be taught, develop a rough storyline, create the gamification design document, create a paper mockup of the game and play it, create storyboards and concept art, test the storyboards and concept art by showing it to focus groups, have play-tests and daily meeting during the development, and so on. In the next section, a possible design of a gamified training system is presented.

6.0 A NEW APPROACH FOR THE DEVELOPMENT OF TRAINING

The Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization (NATO, 2010) suggests that NATO should continue fulfilling effectively three essential core tasks: collective defence, crisis management and cooperative security. This section will consider mainly crisis management in the perspective presented by the Strategic Concept: "NATO has a unique and robust set of political and military capabilities to address the full spectrum of crises – before, during and after conflicts. NATO will actively employ an appropriate mix of those political and military tools to help manage developing crises that have the potential to affect Alliance security, before they escalate into conflicts; to stop ongoing conflicts where they affect Alliance security; and to help consolidate stability in post-conflict situations where that contributes to Euro-Atlantic security". More specifically, we shall consider Cyber Crisis Management.

The Strategic Concept document (NATO, 2010) confirms the importance of training as a way to be effective across the crisis management spectrum. In this case, the document suggests that it is relevant to enhance intelligence sharing within NATO, to further develop doctrine and military capabilities, to form an appropriate civilian crisis management capability, to enhance integrated civilian-military planning throughout the crisis spectrum, to develop the capability to train and develop local forces in crisis zones, to identify and train civilian specialists from member states, and to broaden and intensify the political consultations among Allies and with partners.

Different approaches may be used for the development of training. In this research, we focus our discussion on Cyber Crisis Management while considering which design paradigm is more appropriate for a training course, which learning materials should be used, which training system would provide the best support for both emergency management exercises and on demand training and which method should be applied to properly use the portfolio of learning objects to be allocated to each student undertaking the training.

In one of many points of view, cyber refers to the set of technologies associated with computers and communication infrastructures like the Internet. Cyber Crisis Management refers to the administration of different situations involving computers and communication infrastructures in a "threatscape" that continues to evolve. In the next paragraphs, a new approach to training that considers this dynamic is presented.

The development of intelligent human computer systems for crisis response and management continues to be a challenge for different reasons. In the specific case of cyber crisis, an additional challenge involves training appropriately the stakeholders for a scenario where new threats appear in a daily basis. The more traditional approach to training development would focus on identifying training needs, preparing the training and offering such training. As an example, training on cyber security threats could be considered based on the previously mentioned report on security (FORWARD CONSORTIUM, 2010) that identifies a total of 28 threats while presenting a risk assessment for each one of them based on severity and likelihood. The immediate problem of the traditional approach would be that, even if all the 28 identified threats would be properly contemplated in a specific course, there would still be a reasonable chance that the training would be considered outdated or incomplete in a short time frame. The main reason would be the dynamics of the cyber world where, due to its continuous and rapid evolution, presents a nebulous domain to be dealt with.

In this perspective, it turns to be essential to investigate new approaches for training development and implementation. More specifically, in the case of Cyber Crisis Management, there exists as well a need to

better identify training needs based on demands that may be identified during emergencies. This need asks for a performance support system that may trace back previous training from stakeholders in order to provide appropriate new learning objects with multimedia content for training "on demand". The new training content may be a set of learning objects like a video from an expert explaining how to deal with a new specific threat, a text file with technical information and an animation explaining how to proceed step-by-step to solve a specific problem. This new training content would possibly be used immediately by some of the stakeholders but others would lack enough background and, due to this, could benefit from having a performance support system suggesting additional content to be learnt. In this context, the application of agile methods could be successful.

The research briefly presented here intended to answer the following four questions for Cyber Crisis Management training: (A) Which design paradigm is more appropriate for a training course?; (B) Which learning materials should be used?; (C) Which training system would provide the best support for both emergency management exercises and on demand training?; and (D) Which method should be applied to create a portfolio of learning objects to be automatically allocated to each stakeholder based on his or her specific profile and previous training? The results follow and are summarized in the form of answers to these questions.

For the first question, the chosen design paradigm presents similarities to software development models like the Agile (ALLEN & SITES, 2012). The growing importance of Agile methods and philosophy is noticeable, from the creation of specific certifications (SMITH JR., MANGANO & MANGANO, 2012) to the creation of new standards and of extensions to standards like the BABOK (IIBA, 2013), and from applications ranging from software development (LEFFINGWELL, 2011) to the enterprise management (KREBS, 2008).

For the second question, it is considered that doing "the real thing" or simulating that you do it would be preferable for the perceived training needs. The learning materials that tend to fit this need are serious games and simulations, which drives the research on training systems that apply the concept of "gamification" (KAPP, 2012).

For the third question, the chosen approach would involve the incorporation of the characteristics of Performance Support Systems (PSS) to the Cyber Crisis Management training system to be developed. A PSS offers to the user the necessary information, guidance and learning experiences. A PSS usually has four components: an advisory component, an information component, a training component and the user interface component (DESROSIERS & HARMON, 1996).

For the fourth question, it is relevant to present to the stakeholders the best selection of learning objects in a portfolio (KAY & KNAACK, 2008; KAY & KNAACK, 2007). The transformation of that need into a system, in this case the product or service that provides for the need, involves using both computational simulations and qualitative information for multi-criteria optimization of the portfolio as a way to provide the expected "training value".

7.0 CONCLUSION

This paper presented a possible design of a gamified training system for cyber security that intends to comply with the many relevant requirements while considering new approaches for the development of training. This approach to be used for the development of training is based on Agile methods and its work philosophy since threats change continuously and new content must be added every time in the form of new texts, new videos, new parts of a serious game, etc. In this way, this paper advocates in favour of gamification and concludes for the feasibility of the approach. As future work, the development of the system and/or the development of a mock-up with prototyping software will be considered.

8.0 REFERENCES

[1] AGS (2013). America's Army PC game fact sheet. America's Army first person action PC game series. Army Game Studio (AGS). AMRDEC Software Engineering Directorate at Redstone Arsenal. Huntsville, Alabama, USA. Retrieved August 19, 2013 from http://www.americasarmy.com

[2] ALDRICH, C. (2009). The Complete Guide to Simulations and Serious Games: How the Most Valuable Content Will be Created in the Age Beyond Gutenberg to Google. Pfeiffer. ISBN 0470462736.

[3] ALLEN, M. W.; SITES, R. (2012). Leaving Addie for SAM: An Agile Model for Developing the Best Learning Experiences. ASTD Press: 1st edition (September 26, 2012). ISBN 1562867113.

[4] AMORIM, J. A.; ÅHLFELDT, R.; GUSTAVSSON, P. M.; ANDLER, S. F. (2013). Privacy and Security in Cyberspace: Training Perspectives on the Personal Data Ecosystem. European Intelligence and Security Informatics Conference (EISIC). Proceedings CD. August 12-14, 2013. Information Technology Center ITC at Uppsala University. Uppsala, Sweden. http://www.eisic.eu/

[5] ANDLER, S.; BROHEDE, M. (2008). Information Fusion Research Program - Proposal. University of Skövde. November 24, 2008. Retrieved June 30, 2013 from http://www.his.se/english/research/infofusion/research/proposal/

[6] ANDRESS, J.; WINTERFELD, S. (2011). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Waltham, USA: Syngress; 1 edition (June 1, 2011). ISBN 1597496375.

[7] BACKLUND, P.; HENDRIX, M. (2013). Educational Games - Are They Worth The Effort?, Fifth International Conference on Games and Virtual Worlds for Serious Applications (VS-Games). UK.

[8] BLASCH, E.; STEINBERG, A. (2013). Situation/Threat Assessment and Higher Level Fusion. Tutorial 15. 16th International Conference on Information Fusion. July 9-12, 2013. Istanbul, Turkey. International Society of Information Fusion (ISIF). Retrieved July 12, 2013 from http://www.fusion2013.org/

[9] CHUNG, C. A. (Ed.) (2003). Simulation Modelling Handbook: A Practical Approach. CRC Press; 1 edition (July 15, 2003). ISBN 0849312418.

[10] DAS, S. (2013). Big Data Fusion and Analytics. Tutorial 10. 16th International Conference on Information Fusion. July 9-12, 2013. Istanbul, Turkey. International Society of Information Fusion (ISIF). Retrieved July 12, 2013 from http://www.fusion2013.org/

[11] DESROSIERS, S.; HARMON, S. W. (1996). Performance Support Systems for Education and Training: Could This be the Next Generation?. Research Repository. Georgia State University. http://www2.gsu.edu/~wwwitr/docs/nextgen/

[12] FORWARD CONSORTIUM. (2010). Forward - Managing Emerging Threats in ICT Infrastructures. D3.1 - White book: Emerging ICT threats. Seventh Framework Programme. Technical University of Vienna Coordinator, Austria. 17/01/2010. Retrieved June 30, 2013 from http://www.ict-forward.eu/media/publications/forward-whitebook.pdf

[13] GIACINTO, G.; ROLI, F.; SANSONE, C. (2009). Special Issue on Information Fusion in Computer Security. Information Fusion. Elsevier. Edited by Giorgio Giacinto, Fabio Roli and Carlo Sansone. Volume 10, Issue 4, Pages 271-368 (October 2009). Retrieved July 12, 2013 from http://www.sciencedirect.com/science/journal/15662535/10/4

[14] IIBA (2013). Agile Extension to the BABOK Guide. Paul Stapleton (Editor). July 1, 2013. Retrieved July 12, 2013 from http://www.iiba.org/BABOK-Guide/Agile-Extension-to-the-BABOK-Guide-IIBA.aspx

[15] IISSCC. (2013). Certification Programs. International Information Systems Security Certification Consortium - (ISC)^2. Retrieved September 2, 2013 from https://www.isc2.org/credentials/default.aspx

[16] ITU (2008). Recommendation ITU-T X.1205. ITU-T X-Series Recommendations. Data Networks, Open System Communications and Security. Telecommunication Standardization Sector of ITU. International Telecommunication Union (ITU). United Nations. 04/2008. Retrieved July 12, 2013 from www.itu.int

[17] ITU (2011). ITU National Cybersecurity Strategy Guide. Dr. Frederick Wamala (Editor). International Telecommunication Union (ITU). United Nations. Switzerland, Geneva. Retrieved July 12, 2013 from http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx

[18] KAPP, K. M. (2012). The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education. Pfeiffer; 1st edition (May 1, 2012). ISBN 1118096347.

[19] KAY, R. H.; KNAACK, L. (2007). A systematic evaluation of learning objects for secondary school students. Journal of Educational Technology Systems, 35 (4), 411-448.

[20] KAY, R. H.; KNAACK, L. (2008). A multi-component model for assessing learning objects: The learning object evaluation metric (LOEM). Australasian Journal of Educational Technology. 2008, 24(5), 574-591.

[21] KESSLER, O.; WHITE, F. (2008). Data Fusion Perspectives and Its Role in Information Processing. In: Handbook of Multisensor Data Fusion: Theory and Practice, Second Edition. Electrical Engineering & Applied Signal Processing Series. Martin Liggins II (Editor), David Hall (Editor), James Llinas (Editor). CRC Press. 2nd edition. September 26, 2008. ISBN 1420053086.

[22] KLIMBURG, A. (ED.). (2012). National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia: NATO CCD COE Publication. ISBN 978-9949-9211-2-6. Retrieved August 19, 2013 from www.ccdcoe.org

[23] KREBS, J. (2008). Agile Portfolio Management. Microsoft Press; 1 edition (June 30, 2008). ISBN 0735625670.

[24] LEFFINGWELL, D. (2011). Agile Software Requirements: Lean Requirements Practices for Teams, Programs, and the Enterprise. Addison-Wesley Professional; 1 edition (January 6, 2011). ISBN 0321635841.

[25] LLINAS, J. (2013). Challenges in Information Fusion Technology Capabilities for Modern Intelligence and Security Problems. European Intelligence and Security Informatics Conference (EISIC). August 12-14, 2013. Uppsala, Sweden.

[26] MCINTYRE, A. (2011). iPad and Beyond: What the Future of Computing Holds. Gartner. 30 September 2011. Retrieved June 30, 2013 from http://www.gartner.com/id=1812319

[27] NATO (2010). Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. Adopted by Heads of State and Government at the NATO Summit in Lisbon, 19-20 November 2010. NATO Public Diplomacy Division 1110, Brussels - Belgium. Retrieved June 30, 2013 from www.nato.int/ebookshop

[28] SCHELL, J. (2008). The Art of Game Design: A book of lenses. CRC Press. ISBN 0123694965.

[29] SHOEMAKER, D.; CONKLIN, W. A. (2011). Cybersecurity: The Essential Body of Knowledge. Cengage Learning. ISBN 1435481690.

[30] SMITH JR., A.; MANGANO, V. S.; MANGANO, V. (2012). PMI Agile Certified Practitioner (PMI-ACP) Exam Preparation Self-Study Courseware. CreateSpace Independent Publishing Platform (March 9, 2012). ISBN 146996418X.

[31] STEINBERG, A. (2013). Fundamentals of Data Fusion. Tutorial 4. 16th International Conference on Information Fusion. July 9-12, 2013. Istanbul, Turkey. International Society of Information Fusion (ISIF). Retrieved July 12, 2013 from http://www.fusion2013.org/

[32] SYMANTEC. (2013). Internet Security Threat Report – ISTR 2013. Volume 18. Symantec Corporation. Retrieved August 22, 2013 from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

[33] ZYDA, M. (2005). From Visual Simulation to Virtual Reality to Games. Computer. 38, 9 (September 2005), 25-32. DOI=10.1109/MC.2005.297. Retrieved August 19, 2013 from http://dx.doi.org/10.1109/MC.2005.297