2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

A Renewed Approach to Serious Games for Cyber Security

Alexis Le Compte
De Montfort University
Leicester, England
alexis.lecompte@dmu.ac.uk

Tim Watson
WMG
University of Warwick
Warwick, England
tw@warwick.ac.uk

David Elizondo
De Montfort University
Leicester, England
elizondo@dmu.ac.uk

Abstract: We are living in a world which is continually evolving and where modern conflicts have moved to the cyber domain. In its 2010 Strategic Concept, NATO affirmed its engagement to reinforce the defence and deterrence of its state members. In this light, it has been suggested that the gamification of training and education for cyber security will be beneficial. Although serious games have demonstrated pedagogic effectiveness in this field, they have only been used in a limited number of contexts, revealing some limitations. Thus, it is argued that serious games could be used in informal contexts while achieving similar pedagogic results. It is also argued that the use of such a serious game could potentially reach a larger audience than existing serious games, while complying with national cyber strategies. To this end, a framework for designing serious games which are aimed at raising an awareness of cyber security to those with little or no knowledge of the subject is presented. The framework, based upon existing frameworks and methodologies, is also accompanied with a set of cyber security skills, itself based upon content extracted from government sponsored awareness campaigns, and a method of integrating these skills into the framework. Finally, future research will be conducted to refine the framework and to improve the set of cyber security related skills in order to suit a larger range of players. A proof of concept will also be designed in order to collect empirical data and to validate the effectiveness of the framework.

Keywords: *serious games, framework, cyber security*

1. INTRODUCTION

The development of technology and the increasing number of cyber threats have led political and military organisations, such as NATO and its state members, to develop cyber security strategies, providing recommendations on how to improve nations' resilience and deterrence.

These strategies focus in particular on the reinforcement of infrastructures and the improvement of businesses practices, but their scope also extends to an individual level, with the objective of training cyber security elites and to educate the general population to fight more efficiently against cybercrime. From a certain perspective, it could be argued that the education of the population represents a cornerstone of the system as citizens constitute both the basis of all actors involved in the development of cyber capabilities (cyber experts, specialised industries, military organisations); and the target of various cyber threats, which needs to be protected and defended (businesses, governments, critical infrastructures, general population). A more educated nation provides better prepared individuals for organisations, but also hinders the spread of cybercrimes.

In parallel, serious games, which commonly refer to games with purposes beyond pure entertainment, have gained a lot of popularity in academia and industry over the past decade due to their pedagogical benefits. As a result, it has been proposed that games are used in information assurance and cyber security for educational and training purposes [1], [2].

However, all of the serious games for cyber security awareness, education and training developed to date have been designed to be used in formal contexts and have aimed at reproducing real life experience.

This paper aims at introducing a different approach to serious games in order to raise awareness of cyber security among the general population. Such a game would consistently fulfil cyber security strategies' objectives in terms of education and awareness. To support this approach, a comprehensive framework for designing and releasing serious games is proposed, based upon a study and a review of existing frameworks and methodologies.

The following section presents a review of serious games, in order to identify the respective strength and limitations of these games. Then, the proposed framework is described in greater detail, and finally, the next section introduces a method of integrating cyber related skills into the framework.

2. SERIOUS GAMES

A. Definition

The expression "serious games" in its modern meaning seems to have been introduced by Abt in 1970 [3] and has since been redefined by many researchers and professionals. A popular definition was given by Zyda who describes serious games as "a mental contest, played with a computer in accordance with specific rules, that uses entertainment to further government or

corporate training, education, health, public policy, and strategic communication objectives" [4]. However, the definition of the expression still arouses debate, and Sawyer, who created the Serious Games Initiative in 2002 [5], criticised the variations between existing interpretations, arguing that many authors restrict the definition of serious games based upon their own needs [6].

Although the examples used all relate to video games, the interpretation presented in this paper is not limited to video games and could extend to board games or any other type of games. Furthermore, this paper aims at emphasising the importance of the gaming aspect as a fundamental and non-negligible feature of serious games. Despite the involvement of academics or professional in the conception of serious games for training or educational purposes, serious games should be, primarily, games. This also represents the difference between serious games and gamification, with the latter applying game mechanics to real life contexts. Therefore the expression serious games will simply be defined as "games which incorporate pedagogic elements".

B. Review of Serious Games for Information Assurance and Cyber Security

Serious games have received a fair amount of attention in the field of information security and cyber security, both from academic researchers and in industry.

One of the most popular examples which can be found in the literature is the game "CyberCIEGE", created by the US Naval Postgraduate School (NPS) and sponsored by several US organisations [7], [8]. The game offers a realistic virtual world in which players have to operate and defend a computer network. From a pedagogic point of view, the game encompasses seven fundamental cyber security related topics. The game has also been the object of many academic publications and has shown good pedagogic benefits.

Other examples developed by various US military departments, universities and other organisations, are presented by Pastor *et al*. [9] in a state of the art simulation systems for information security education, training and awareness. Although the paper is focused on simulation systems, the distinction between serious games and pure simulation tools is quite blurred in this context. In particular, the paper mentions CyberCIEGE as part of the list of simulation tools, but describes it as a video game. The paper ultimately proposes a taxonomy of simulation systems, based upon topics, technical features, target audiences, didactical capabilities and so on. Nevertheless, Pastor *et al*. highlighted several limitations in the conclusion of their paper. Firstly, they suggested that more tools should be developed for anyone interested professionally in information assurance, rather than mainly targeting university students. Secondly, they remarked that these tools should allow players to practice in their own environment. Thirdly, they commented that there was very little diversity in the choice of simulations for information assurance teaching, training and awareness.

CyberCIEGE, along with other games like "CyberProtect" or "Anti-Phishing Phil" were cited as examples in a paper from Nagarajan *et al*. [10]. In this paper, the authors conducted research on game design for cyber security training emphasising particularly on a game called

"CyberNEXS". The latter contains different modes, respectively focusing on computer network, forensics and penetration testing. While the authors aimed at producing a game addressing limitations of existing training solutions, they use CyberNEXS as a basis for improvements. To this end, they elaborate on game genres and game mechanics, providing examples directly applicable to CyberNEXS.

Anti-Phishing Phil was developed at Carnegie Melon University to provide a user friendly tool to teach about phishing attacks. In this game, players have to guide a fish towards different worms that will display a genuine or a phishing link. Players then have to identify whether the link is legitimate or not by choosing to "eat" or "reject" the worm. In a paper dedicated to the game, Sheng *et al*. [11] present the methodology and the structure of the game, concluding on the results of their user study showing the best outcomes when playing the game.

Several other games can be found in industry. "Data Security", "Agent Surefire", "Cyber Awareness Challenge" and "Cyber Security Investigation (CSI) Game" are four games covering information assurance and cyber security topics. In the simulation game "Data Security", from Playgen [12], players play the role of a new employee tasked to identify security concerns. "Agent Surefire", produced by Mavi Interactive [13], [14] , is a point and click simulation in which players must catch an insider threat, identify breaches and security issues. According to Mavi Interactive, the game has been really well received in industry, receiving a total of thirty-six awards. "Cyber Awareness Challenge", developed by Carney, Inc. [15] is also a simulation. This game, which was one of the finalists of the "2012 Serious Games Showcase & Challenge", proposes mini games as a federal government agent whose purpose is to capture an unnamed hacker. The last example, "Cyber Security Investigation (CSI) Game", developed by InfoSecure [16], and which will be fully finished later this year, is a kind of puzzle game, where players have to find the right combination of events that led to an information security incident.

It is also worth citing the game "Secure Futures", released on the website "Big Ambition" [17] developed by e-skills UK, the Sector Skills Council for Business and Information Technology in UK. The game, which targets pupils, introduces cyber security careers and is accompanied with teaching guides for teachers. After registering, the game is freely available to play. After trying the game, it was found that the scenario was interesting from a technical point of view and that the website was easy to navigate. However, it could be argued that this game may be too difficult for young players which led to uncertainties about its pedagogic effectiveness. Nevertheless, without proper analysis, it is impossible to make any conclusions on this point; furthermore, the game was not designed to teach cyber security, but rather to provide an overview of careers in this field.

Finally, when looking at games from the traditional gaming industry, no example of serious games on cyber security was found. A few games on the theme of "hackers" exist, such as "Uplink" [18] or "Hacker Evolution" [19], which let players fulfil various missions as professional hackers in a virtual world, but these games are not designed to teach any specific concepts and therefore cannot be considered as serious games.

C. Observations and Suggestions

When reviewing the aforementioned academic publications and commercial products, it appears clearly that serious games present a great pedagogic potential for cyber security awareness, teaching and training, as evidenced by case studies. The large number of industry awards received by some of these games also shows that businesses approve their usefulness and effectiveness.

Nevertheless, several limitations arise from the presentation of these games:

1. In their attempt to immerse players in a realistic environment, most of these games are simulation based games, or are strongly aiming at reproducing real life scenarios. This observation is also corroborated by Connolly et al. [20] who conducted a literature review of empirical evidence on serious games which shows that simulation was the most popular game genre in their research results. However, the excess of simulation based games could lead to the potentially wrong assumption that it is the only viable game genre for serious games design. On the contrary, Nagarajan *et al*. [10] show that many different game genres could embody cyber security related concepts, based upon different game mechanics. Furthermore, different game genres would suit a wider range of players, as different players have different game preferences.
2. In most cases, the examples shown previously are designed for educational purposes for use in school or in university, or for training purposes in corporate environment. This implies that the access to most of these games is tied to a formal environment (school, university, business, etc. Marklund *et al*. [21] explained in great details the difference between formal and informal contexts), sometimes under the supervision of a learning facilitator or an instructor, and that players rarely have the possibility to play these games outside of these contexts, by their own initiative. This leads to several issues already highlighted by Nagarajan *et al*. [10], such as the lack of continual practice necessary to a better knowledge retention or too much information in too little time, among several other issues. Thus, Pastor et al. [9] argued that players should be able to play the game "in their own environment" in order to get a deeper understanding of concepts presented in games; which was confirmed by Thompson and Irvine [22] who shown in a study on CyberCIEGE that the ability to play the game on personal computers substantially improved the educational experience.
3. In a slightly similar perspective, it can observed that none of these games can be acquired through traditional distribution channels for video games such as online store or video games shops, nor are they mentioned on entertainment video games forums. Instead, these games are sometimes available from their respective official website, or on request from the organisations producing them. It appears that there exists a gap between serious games and entertainment games, and that as a result, it could be argued that serious games fail to reach large audiences and that their potential is only exploited in formal contexts. Indeed, only people aware and convinced of the benefits of serious games will promote and implement serious games in their organisation or business. To come back to the context of NATO and cyber security policies, the education and the development of competences through serious games

would mostly rely on the responsibility of a somewhat limited number of schools, universities and business.

4. From a technical perspective, a direct consequence of serious games being essentially designed for formal contexts is the added complexity in the development process and implementation. This problem is in particular illustrated by Marklund *et al*. [21] who proposed a model for balancing pedagogic and players expectations. By designing serious games for "informal" contexts, many constraints and issues listed by Nagarajan *et al*. [10] and Marklund *et al*. [21] can be removed, in particular the need for a well structured environment and supervisors. Players would just acquire the game and built their own environment in order to play the game. Also, there is a limit to how many hours serious games can be used in formal contexts, whereas this restriction virtually does not exist in informal contexts.

Based upon all these observations, it can be argued that it is technically possible to design serious games for use in informal contexts which could be pedagogically viable.

To support this theory, the game "Wii Fit", and its sequel "Wii Fit plus", from the Japanese firm Nintendo, can be used as examples. The games propose various types of fitness exercises and rely on the use of a special board. While these games achieved noticeable commercial results, with 22 millions of copies sold for "Wii Fit" and around 20 million for its sequel [23], [24], the games have also demonstrated pedagogic usefulness and effectiveness. "Wii Fit" was used in several health studies and shown positive results [25–27].

To put it in a nutshell, millions of people have played Wii Fit, in informal contexts, over variable periods of time, most likely from their own initiative and may have purchased its sequel. Although these games were primarily designed as flagships for Nintendo's console, their popularity combined to empirical evidences acquired through academic studies would suggest that the games have had a positive pedagogic impact on players. It is also unclear if these games have had an impact in the long term, but the same observation can be made for serious games used in formal contexts. Nevertheless, it appears that two different paradigms are possible, and that pedagogic outcomes can be achieved in both cases. What is more, developing serious games for cyber security teaching, training and awareness for informal contexts would open new perspectives in terms of self-education. Serious games designed for informal contexts have the potential to reach and spread across a larger and more diversified audience. It can even be imagined that well designed serious games could keep users playing over longer periods of time, increasing the frequency of practicing pedagogic concepts through the games.

3. PROPOSED FRAMEWORK

Due to the growing popularity of serious games, much research has been conducted on design methodologies for serious games, as illustrated by the publication of MSc or PhD thesis and other academic papers [28–30]. Despite this, some researchers have focused on specific aspect of serious games design, highlighting limitations and issues or suggesting new approaches, in particular in the design and evaluation of serious games.

As a basis for a comprehensive framework to design serious games aimed at informal contexts, essential steps were extracted from existing frameworks and methodologies, resulting in a generic and iterative set of steps which can be applied to most serious games. The limitations raised in the literature were also taken into account, and each step is supported by one or several concepts developed specifically to address these limitations. Finally, particular emphasis was laid on the development and deployment processes in order to make the framework more suitable for informal contexts.

Step 1: Preliminary analysis.

Poor project management and planning are responsible for more than half of IT project failure, and video games are no exceptions. This crucial step essentially consists in defining the pedagogic objectives for the game, gathering information about the target audience and analysing the technical constraints for the development of the game. The objectives of these steps are:

- Evaluating the technical resources allocated for the development of the game. This includes equipment but also time constraints, budget and technical skills of the developers. All these factors have an impact on the quality of the final game and must therefore be analysed carefully in order to maximise the success rate of the overall development process and distribution
- Defining pedagogic objectives. A set of key skills must be clearly identified. These skills will be matched against game mechanics later on
- Identifying target players and context of play (as described by the Design, Play, Experience framework (DPE) [31] and the Four Dimensional Framework (FDF) [32]). Players will have different expectations from the game depending on their cultural background or experience. Thus, understanding the players help in providing a more suitable game, adapted to the targeted players
- Defining the pedagogic and game mechanics (as described by the LM-GM framework). Pedagogic objectives can be associated to game mechanics to produce consistent gameplay. Choosing appropriate game mechanics is also essential in order to choose a game genre. A customised LM-GM map is proposed in the next section.

Step 2: Design.

The design is all about building conceptual models. The key characteristics for these models should present a balance between serious objectives and entertainment:

- From a technical point of view, models can be formalised with the help of the LM-GM [33] and the DPE framework [31]. They will ensure consistency between pedagogic mechanics and game mechanics, while concentrating on the players perspective in order to provide engaging gameplay for players
- Developers should ensure that the purposes of the game are well conveyed through the game, as explained by the SGDA framework [34]. Clear objectives not only generate a greater engagement of players, but also help them to better assimilate the pedagogic objectives
- Games should present a progressive level of difficulty, with in-game tutorials and many opportunities to practice. Gee [35] also suggests that games should provide opportunities where skills acquired in game will not be sufficient to progress,

requiring players to develop new techniques by themselves. This contributes to a more engaging gameplay but also stimulates players' creativity. It is essential that models developed at this stage incorporate the techniques used by entertainment games as they will help to build better quality games, and more engaging games. A direct consequence of this is that players will give more attention to pedagogic objectives

Step 3: Development.

The purpose of this stage is to provide technical guidance to develop the game while respecting the constraints identified during step 1. In particular this steps guides developers in the choice for a suitable approach to the development of games. The aim is to provide the best balance between time, skills and financial limitations:

- Support from a third party: Some companies, with the example of Mavi Interactive, specialise in the development of serious games, and can provide either ready to use games, or provide support for the development of customised games. This solution will come at a cost, and can be time consuming.
- Off-the-shelf game: An existing game, from an entertainment game studio or a specialised development company, can be used in a teaching or training context. In this case, learning facilitators may be involved in the deployment and use of the game, and may provide additional guidance and instructions for pedagogic objectives to fulfil, which means that players may not be able to play the game without supervision. However, from a technical point of view, this solution is efficient as it considerably simplifies the development process and removes the need for developers.
- Off-the-shelf game with modifications: Some existing games enable players and developers to customise the original game by adding additional content in game referred to as "mods", which can be used to introduce the pedagogic objectives while maintaining the integrity of the original game. This solution can be useful as players may not necessarily need to be monitored or guided by learning facilitators, and can be autonomous when playing the game. On a technical side, this solution can also be time and cost effective, as it may only require a limited amount of development.
- Assisted development: To mitigate the difficulties of video game development and improve the production ratio, assisted methodologies have been developed. These methodologies are usually accompanied with tool kits which simplify the development process. For instance, the EMERGO methodology [36] proposes a 5 step methodology, from the analysis to the evaluation, with tools assisting with the completion of each of these steps and requiring a minimum amount of programming. The end result is an interactive video based game, which can be played in web browsers. The downside with such a choice is that the options for customisations are limited and complex scenarios may be difficult to implement.
- Full development: If the development team has the appropriate knowledge, the time and financial resources, it is also possible to build a game from scratch. In this case, the development team is completely responsible for all phases of the development. The time and financial cost of the game will depend on the competence of the development team and the game to be built.

Step 4: Game assessment.

Game assessment is a crucial part of the development process and could be compared to user acceptance in software development. This step has the objective of ensuring that the game matches technical and pedagogic expectations, while maximising players' engagement and enjoyment.

- Several frameworks have been designed to evaluate serious games and players ([37], [38]). One of the most recent studies was conducted by Mayer [39], who highlighted limitations of existing frameworks and developed a comprehensive methodology, which is generic enough to be applied in numerous contexts (education, training, professional environment...).
- In the video game industry, engagement and enjoyment are usually estimated through testing phases. Players can either be recruited or they can obtain copies of prototypes to test the game before its release. Feedback from players are then collected, either via survey or directly in game, so that developers can uncover bugs, improve gameplay or even modify game mechanics if the game does not match their initial expectations. These testing phases are also important for the reputation of the game as they constitute its first public exposure, and are often accompanied with trailers or reviews of the prototype.

Step 5: Deployment.

In formal contexts, rules apply to the deployment of serious games. Most often, players are supervised by an instructor or a learning facilitator, time is limited and play sessions are framed within the pedagogic plan. In informal contexts, the constraints and requirements are different. Nevertheless, the release process is an integral part of the lifecycle of a commercial product, and the gaming industry already uses techniques to maximise sales and reach large audiences. This implies the use of marketing campaigns, supported by advertisements, demonstrations, the creation of dedicated websites and a presence on social media. These techniques should also be applied to serious games, and could in fact increase the benefits of the games. For instance, Gee [35] provided empirical evidences of the benefits of using external media such as forums, and Raybourn [40] even demonstrated that transmedia strategies is key for new learning strategies.

Step 6: Player assessment.

Finally, to determine whether games contribute to skills improvement, it is necessary to evaluate players. This can be done following Mayer's methodology [39], or game mechanics can be implemented in order to evaluate players directly while playing. Indeed, most games become increasingly difficult as players progress throughout the game. Thus, to progress, players need to master particular skills and principles [35]. If pedagogic mechanics are appropriately mapped to game mechanics, then players should acquire the expected skills when completing the game.

Tests, surveys and questionnaires could potentially be used, but would have to be implemented in a way which does not require an external intervention since the aim is to deploy serious games in informal contexts.

4. INTEGRATING CYBER SKILLS IN SERIOUS GAMES

Cyber security is a field with multiple, technically complex and ever changing aspects, and cyber threats can affect individuals as well as large organisations like businesses or governments. As a consequence, there is a real need to educate people to the most basic cyber security principles.

In the UK, for instance, the government deployed its cyber security strategy in order to provide guidance to businesses and to inform the public. This resulted in the creation of public awareness campaigns and websites such as "Get safe online" [41] or "Cyber Streetwise" [42] which cover an exhaustive list of topics such as protecting computers or users, online behaviour or safeguarding children but also guidance on physical security, backups, staff management, legal advice and so on. Although the content provided on these websites is not in as great depth as other sources such as the IISP skills framework [43] or the Skills Framework for the Information Age [44], which both emphasise on information security in businesses, the two campaigns have the advantage of being simple enough while covering the most common cyber threats. Therefore, the knowledge presented in these two websites are relevant for people with no prior or limited knowledge in cyber security, but can also be relevant to those who have already understood these basics, as a reminder. However, as Gee suggests [35], well designed video games encompass good educational practices. Thus, serious games for cyber security awareness should implement gradually complex concepts, starting with the most basic aspects of cyber security. One of the objectives of this paper is to focus on basic concepts and awareness of the general public, therefore, concepts specifically applying to businesses or requiring prior knowledge in cyber security will be avoided. More advanced sets of topics would be more suitable in the context of advanced training, for people with experience or knowledge of cyber security or for specific businesses. These topics may be integrated in a future update of this framework.

In order to fit an appropriate set of skills into the framework, relevant competences were first extracted from "Get Safe Online" and "Cyber Streetwise". This compilation of skills was then used to enhance the model presented in the "Learning Mechanics - Game Mechanics" (LM-GM) framework [33] (see Table I). To use the resulting customised LM-GM map, the learning mechanics grid should be used as a transitional layer between cyber security skills and game mechanics.

TABLE 1: CUSTOMISED LM-GM MAP WITH CYBER SECURITY SKILLS

CYBER SECURITY SKILLS		
Use of appropriate hardware	Proper hardware disposal	
	Backing up data on separate devices	
Software updates	Using appropriate encryption	Using security software (anti-virus)
	Avoiding remote access / online services	
Using strong passwords	Avoiding disclosing personal information	Avoiding untrusted / unknown networks
	Secure online payment / mobile banking	
Being able to identify potentially dangerous searches	Being able to identify social engineering	Being able to identify and react to cyber threats and cyber frauds *
Controlling and monitoring people with physical / remote access to assets	Protecting access to critical assets (machines and networks)	Establishing usage rules
	Being able to identify legal from illegal use of a computer or software	

* scams, phising, cyberbullying, cyberstalking, money mulling, blackmail, ransomware...

LEARNING MECHANICS		
Instructional	Guidance	
Demonstration	Participation	Action / Task
Generalisation / Discrimination	Observation	Feedback
	Question & Answer	
Explore	Identify	Discover
	Plan	Objectify
Hypothesis	Exeperimentation	
	Repetition	
	Reflect / Discuss	Analyse
	Imitation	Shadowing
Simulation	Modelling	
Tutorial	Assessment	
	Competition	
Motivation	Ownership	Accountability
	Responsibility	Incentive

GAME MECHANICS			
Behavioural Momentum	Role Play		
Cooperation	Collaboration	Goods / Information	
Selecting / Collecting	Tokens	Cut Scenes /Story	
	Cascading Information	Communal Discovery	
	Questions & Answers	Pareto Optimal	Appointment
Strategy / Planning	Resource Management	Infinite Gameplay	
Capture / Eliminate	Tiles / Grids	Levels	
Game Turns	Action Points	Feedback	
Time pressure	Pavlovian Interactions	Meta-game	
	Protégé effects	Simulate / Response	Realism
Design / Editing	Movement		
Tutorial	Assessment		
	Competition		
Urgent Optimism	Ownership		
Rewards / Penalties	Status	Virality	

5. CONCLUSIONS AND FUTURE WORK

This paper reviewed existing serious games for cyber security awareness, teaching and training, showing that these games have a great pedagogic potential. However, their use is most often limited to formal contexts, leading to several limitations. It was argued that these limitations could be overcome if serious games were released in informal contexts, without degrading their pedagogic virtues.

In this perspective, a framework balancing pedagogic and game mechanics has been proposed, which also suggests an approach supported by transmedia theories [40], more in line with entertainment games, for the deployment of serious games. Finally, a method of integrating cyber security related skills, based upon the LM-GM framework, has been presented.

Future work will focus on improving the set of cyber related skills, in order to provide an appropriate set of skills for different level of expertise, and therefore cover a larger range of players. Research will also be conducted on alternative methods for integrating pedagogic content in games. Finally, a proof of concept will be designed for a case study in order to refine and validate the framework.

REFERENCES

[1] J. A. Amorim, M. Hendrix, S. F. Andler, and P. M. Gustavsson, "Gamified Training for Cyber Defence: Methods and Automated Tools for Situation and Threat Assessment," in *NATO Modelling and Simulation Group (MSG) Annual Conference 2013 (MSG-111)*, 2013.

[2] "Serious Games and their Use in NATO," in *NATO Modelling and Simulation Group (MSG) Lecture series (STO-EN-MSG-115)*, 2013.

[3] D. Djaouti, J. Alvarez, J.-P. Jessel, and O. Rampnoux, "Origins of Serious Games," in *Serious Games and Edutainment Applications*, M. Ma, A. Oikonomou, and L. C. Jain, Eds. Springer London, 2011, pp. 25–43.

[4] M. Zyda, "From visual simulation to virtual reality to games," *Computer*, vol. 38, no. 9, pp. 25–32, 2005.

[5] The Serious Games Initiative, "Serious Games Initiative." [Online] http://www.seriousgames.org/ [Accessed 20/02/14].

[6] B. Sawyer and P. Smith, "Serious Games Taxonomy.", [Online] http://www.dmill.com/presentations/serious-games-taxonomy-2008.pdf? [Accessed 8/03/14], 2008.

[7] Centre for Information Systems Security Studies and Research (CISR), "Incorporating CyberCIEGE into an Introductory Cyber Security Course.", [Online] http://cisr.nps.edu/cyberciege/CyberCIEGE%20Syllabus.html [Accessed 5/12/2014], 2013.

[8] Centre for Information Systems Security Studies and Research (CISR), "Incorporating CyberCIEGE into an Introductory Cyber Security Course.", [Online] http://cisr.nps.edu/cyberciege/CyberCIEGE%20Syllabus.html [Accessed 5/12/2014], 2013.

[9] V. Pastor, G. Díaz, and M. Castro, "State-of-the-art simulation systems for information security education, training and awareness," in *Education Engineering (EDUCON), 2010 IEEE*, 2010, pp. 1907–1916.

[10] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training," in *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on*, 2012, pp. 256–262.

[11] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish," *Institute for Software Research*, 2007.

[12] Playgen, "Data Security.", [Online] http://playgen.com/play/data-security/ [Accessed 5/12/2014].

[13] Mavi Interactive, "Agent Surefire.", [Online] http://www.maviinteractive.com/agent_surefire_insider_threat.asp [Accessed 5/12/2014].

[14] E. Alhadeff, "Converting Cybersecurity Practice Into Engaging Serious Games.", [Online] http://seriousgamesmarket.blogspot.co.uk/2012/02/converting-cybersecurity-practice-into.html [Accessed 09/03/2015], 2012.

[15] E. Alhadeff, "Serious Games As Information Assurance Adventures.", [Online] http://seriousgamesmarket.blogspot.co.uk/2012/12/serious-games-as-information-assurance.html [Accessed 09/03/2015], 2012.

[16] InfoSecure, "Cyber Security Investigation Game.", [Online] http://www.infosecuregroup.com/CSI.html [Accessed 10/03/2015], 2015.

[17] Big Ambition, "Secure Futures.", [Online] http://www.bigambition.co.uk/securefutures [Accessed 5/12/2014].

[18] Introversion Software, "Uplink.", [Online] http://www.introversion.co.uk/uplink/index.html [Accessed 8/12/2014].

[19] Exosyphn Studios, "Hacker Evolution.", [Online] http://www.exosyphen.com/page_hackerevolution.html [Accessed 9/12/14].

[20] T. M. Connolly, E. A. Boyle, E. MacArthur, T. Hainey, and J. M. Boyle, "A systematic literature review of empirical evidence on computer games and serious games," *Computers & Education*, vol. 59, no. 2, pp. 661–686, 2012.

[21] B. B. Marklund, P. Backlund, and H. Engstrom, "The Practicalities of Educational Games: Challenges of Taking Games into Formal Educational Settings," in *Games and Virtual Worlds for Serious Applications (VS-GAMES), 2014 6th International Conference on*, 2014, pp. 1–8.

[22] M. Thompson and C. Irvine, "Active Learning with the CyberCIEGE Video Game," in *Proceedings of the 4th Conference on Cyber Security Experimentation and Test*, 2011, pp. 10–10.

[23] Nintendo, "It's official! Nintendo's Wii Balance Board is a record breaker!", [Online] https://www.nintendo.co.uk/News/2012/It-s-official-Nintendo-s-Wii-Balance-Board-is-a-record-breaker--253133.html [Accessed 10/12/14], 2012.

[24] Nintendo Co., Ltd., "Financial Results Briefing for Fiscal Year Ended March 2012.", [Online] http://www.nintendo.co.jp/ir/pdf/2012/120427e.pdf [Accessed 10/12/14], 2012.

[25] N. B. Herz, S. H. Mehta, K. D. Sethi, P. Jackson, P. Hall, and J. C. Morgan, "Nintendo Wii rehabilitation ('Wii-hab') provides benefits in Parkinson's disease," *Parkinsonism & Related Disorders*, vol. 19, no. 11, pp. 1039–1042, 2013.

[26] R. Mombarg, D. Jelsma, and E. Hartman, “Effect of Wii-intervention on balance of children with poor motor performance,” *Research in Developmental Disabilities*, vol. 34, no. 9, pp. 2996–3003, 2013.
[27] N. Vernadakis, A. Gioftsidou, P. Antoniou, D. Ioannidis, and M. Giannousi, “The impact of Nintendo Wii to physical education students’ balance compared to the traditional approaches,” *Computers & Education*, vol. 59, no. 2, pp. 196–205, 2012.
[28] C. Bull-Hansen, “Serious Games: Video Game Design Techniques for Academic and Commercial Communication.,” University of Oslo, 2007.
[29] D. Fitchie, “Investigating the use of Serious Games for teaching anatomy and physiology to higher education students: Research into Serious Games,” University of Huddersfield, 2011.
[30] A. Yusoff, “A Conceptual Framework for Serious Games and its Validation,” University of Southampton, 2010.
[31] B. Winn, “The design, play, and experience framework,” *Handbook of research on effective electronic gaming in education*, vol. 3, pp. 1010–1024, 2008.
[32] S. de Freitas and M. Oliver, “How can exploratory learning with games and simulations within the curriculum be most effectively evaluated?,” *Computers & Education*, vol. 46, no. 3, pp. 249–264, 2006.
[33] S. Arnab, T. Lim, M. B. Carvalho, F. Bellotti, S. de Freitas, S. Louchart, N. Suttie, R. Berta, and A. De Gloria, “Mapping learning and game mechanics for serious games analysis,” *British Journal of Educational Technology*, 2014.
[34] K. Mitgutsch and N. Alvarado, “Purposeful by Design?: A Serious Game Design Assessment Framework,” in *Proceedings of the International Conference on the Foundations of Digital Games*, 2012, pp. 121–128.
[35] J. P. Gee, *What video games have to teach us about learning and literacy*. Palgrave Macmillan, 2007.
[36] R. J. Nadolski, H. G. K. Hummel, H. J. van den Brink, R. E. Hoefakker, A. Slootmaker, H. J. Kurvers, and J. Storm, “EMERGO: A methodology and toolkit for developing serious games in higher education,” *Simulation and Gaming*, vol. 39, no. 3, pp. 338–352, 2008.
[37] T. Connolly, M. Stansfield, and T. Hainey, “Towards the Development of a Games-based Learning Evaluation Framework,” in *Games-based Learning Advancement for Multisensory Human Computer Interfaces: Techniques and Effective Practices*, Idea-Group Publishing: Hershey, 2009.
[38] A. Yusoff, R. Crowder, and L. Gilbert, “Validation of Serious Games Attributes Using the Technology Acceptance Model,” in *Games and Virtual Worlds for Serious Applications (VS-GAMES), 2010 Second International Conference on*, 2010, pp. 45–51.
[39] I. Mayer, “Towards a Comprehensive Methodology for the Research and Evaluation of Serious Games,” *Procedia Computer Science*, vol. 15, no. 0, pp. 233–247, 2012.
[40] E. M. Raybourn, “A new paradigm for serious games: Transmedia learning for more effective training and education,” *Journal of Computational Science*, vol. 5, no. 3, pp. 471–481, 2014.
[41] Get Safe Online, “Free online security advice.”, [Online] https://www.getsafeonline.org/ [accessed 20/12/2014].
[42] HM. Government, “Cyber Street, Protect your home or business from cyber crime.”, [Online] https://www.cyberstreetwise.com/ [accessed 20/12/2014] .
[43] Institute of Information Security Professionals, “Our Skills Framework.”, [Online] https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework.aspx [Accessed 17/11/2014], 2013.
[44] SFIA Foundation, “Skills Framework for the Information Age.”, [Online] http://www.sfia-online.org/ [Accessed 17/11/2014] .