Software Engineering Institute

Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors

Christopher Herr
Dennis M. Allen

July 2015

Cyber Workforce Development (CWD)

Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0002631

Table of Contents

Abstract

There is a global shortage of more than 1 million skilled cybersecurity professionals needed to address current cybersecurity challenges (CISCO, 2014). Criminal organizations, nation-state adversaries, hacktavists, and numerous other threat actors continuously target business, government, and even critical infrastructure networks. Estimated losses from cyber crime and cyber espionage amount to hundreds of billions annually (Center for Strategic and International Studies, 2013). The need to build, maintain, and defend computing resources is greater than ever before.

A novel approach to closing the cybersecurity workforce gap is to develop cutting-edge cybersecurity video games that (1) grab the attention of young adults, (2) build a solid foundation of information security knowledge and skills, (3) inform players of potential career paths, and (4) establish a passion that drives them through higher education and professional growth. Although some video games and other games do exist, no viable options are available that target high-school-age students and young adults that supply both a quality gaming experience and foster the gain of key cybersecurity knowledge and skills. Given the Department of Defense's success with simulations and gaming technology, its sponsorship of a cybersecurity video game could prove extremely valuable in addressing the current and future needs for our next generation cyber warriors.

The characteristics of a potential cybersecurity video game are presented in this paper. Several current cybersecurity games were reviewed and key attributes and shortcomings of these games were identified. Additionally, a small sampling of students, trainers, educators, security professionals, and non-security occupations were interviewed and surveyed to identify some of the essential requirements. Feedback from these efforts is included to establish a foundation for additional research and future video game development.

1 The Cybersecurity Workforce Shortage

Several U.S. organizations, including the Department of Defense (DoD), the Department of Homeland Security (DHS), Government Accountability Office (GAO), and the Bureau of Labor Statistics have identified a substantial need for cybersecurity professionals. Leading information technology and security organizations have also researched and validated this critical need. The most common statistics cited relate to the number of currently filled positions, percentage of vacancies, and estimated growth:

- Cisco Systems, Inc. estimates a shortage of over 1 million global cybersecurity professionals in 2014 (CISCO, 2014).
- Employment of information security analysts is projected to grow much faster than other occupations at a rate of 37% from 2012 to 2022 (Bureau of Labor Statistics, 2014).
- In the (ISC)² 2013 Global Information Security Workforce Study (Frost and Sullivan, 2013a)
  - 53% of the 12,000 respondents believe there is a cybersecurity workforce shortage
  - 61% of the U.S. government respondents believe their agency has too few workers to handle their current information security threats
- U.S. Cyber Command is expected to grow beyond 6,000 employees in 2016 compared to an estimate of 1,800 by the end of 2014 (Baldor et al. 2014).
- The GAO reported a 22% vacancy rate in cybersecurity positions for DHS's National Protection and Programs Directorate (NPPD) citing lower pay compared to industry, difficulty in obtaining security clearances, and lack of clearly defined roles and responsibilities (United States Government Accountability Office, 2013).

1.1 Greater Cybersecurity Education is in Need for Primary/Secondary Students

In June 2014, RAND Corporation released a comprehensive analysis of the cybersecurity labor market. Among other factors, they identified the role education plays in preparing the cybersecurity workforce. An important observation was that 78% of college students decided to study Science, Technology, Engineering, and Math (STEM) in high school or earlier (Libicki et al., 2014). Unfortunately, the efforts of the National Initiative for Cybersecurity Education (NICE) to integrate cybersecurity into STEM curricula have not gained enough traction at the high school level. An October 2013 study by U.S. government defense contractor Raytheon found that 82% of millennials said, "no high school teacher or guidance counselor ever mentioned to them the idea of a career in cybersecurity," and only 24% were interested in a career as a cybersecurity professional (Raytheon, 2013).

Although federal programs such as STEM and NICE have been initiated to help address this shortage, the thousands of qualified individuals required are simply not available. More solutions are needed to establish the fundamental knowledge in computing technologies and information security concepts and to spark the desire for cybersecurity careers.

2 Video Games as a Ubiquitous Learning Tool

Traditional cybersecurity training occurs in the classroom, through reading, watching hands-on demonstrations and videos, or practicing at home. However, cybersecurity training also lends itself well to a game-based environment—an environment where players must react to incoming realistic cyber attacks in real time, and make decisions based on their current skills, knowledge, or experience. While traditional learning can take place in several forms, it is only with the game or simulation that cybersecurity professionals can truly put their skills to the test and prepare themselves for events in the real world, without risking real-world assets.

2.1 How Video Games Can Be an Effective Learning Tool

Several studies have focused on the effectiveness of game-based learning and shown that playing video games can improve motor skills, spatial reasoning, and decision-making abilities as well as reduce stress. In the 1990's, a group known as the Lightspan Partnership created several PlayStation video games geared towards imparting actual curriculum-based knowledge to elementary-age children. As a result of the study, Lightspan found that children who played a few hours of the games per week outside of class had a 25% increase in vocabulary and language skills and a 50% increase in math skills over students who had only classroom instruction (Prensky, 2006). The results from this study demonstrate the benefit of gaming beyond entertainment value.

Outside of games specifically aimed at education, gamers who play fast-paced action games have been shown to have faster average reaction times when compared to non-gamers, and research also found that this increase in reaction speed had a negligible loss of accuracy (Dye, Green, & Bavelier, 2009). Studies also found that subjects playing 50 hours of the fast-paced role-playing games "Call of Duty 2'' and "Unreal Tournament'' made accurate decisions when exposed to fast-moving visual stimuli--up to 25% faster than subjects who played slower moving strategy-based games (Turman, 2010). These studies have also shown that video game types, such as first person shooters, have even improved cognitive skills and spatial navigation. The latter has been previously linked to long-term success in STEM careers (Lubinski et al. 2010).

Gaming is also often seen as a way to relieve stress and exercise the mind's more emotional side. A January 2014 study published by the American Psychological Association evaluates the cognitive, emotional, social, motivational, and mental benefits of video games. Research found that players learn valuable cooperative skills by playing cooperative and challenging games with others (Granic et. al., 2013). Granic and others also hypothesize that game playing can invoke moods and emotions that are not only beneficial to our own mental and emotional state but also make us generally more mentally healthy (2013).

These studies indicate that gaming can be used as a tool to train your brain and can be used to teach basic quantitative and qualitative skills such as math and language. Furthermore, games can also serve to enhance proper cooperative behaviors and relieve stress. These qualities are necessary for any game that is aimed at effectively teaching future cyber warriors.

2.2 Video Games Reach a Large and Diverse Audience

The makeup of the gamer population has evolved to a more heterogeneous constituency, strengthening the need for a cybersecurity game that reaches a large and diverse audience. One common misconception is that only teenaged and early twenties males are the ones playing video games. There are over 175 million gamers in the United States alone, and recent trends have proven that not only are there far more female gamers than previously thought, but that the average age of gamers is rapidly increasing (McGonigal, 2011). The generation who grew up with the Atari or the first Nintendo Entertainment System are now in their 30's or 40's, and the average age of gamers today is still around 35 years old, not the adolescent age one might expect (McGonigal, 2011). Forty percent of gamers are women and one out of every four gamers is over the age of 50 (McGonigal, 2011). In other words, there is no single target audience or demographic when it comes to gaming.

Perhaps the most valuable trend previously mentioned pertains to the female gamer. Women accounted for almost 47% of the total U.S. labor force in 2012 and just over 45% in the European Union. However, only 11% of the 306,000 global information security workforce that year was composed of women (Frost and Sullivan, 2013b). With almost half of today's gamers being female, it is feasible that cutting-edge video games will not only help cultivate interest and inject talent into the cybersecurity pipeline early, but they may actually do so by reaching a female demographic that is greatly underrepresented within the industry.

2.3 The Prevalence of Video Gaming

Video games are a very lucrative industry, with games being played often and everywhere. While software and hardware sales have fluctuated over the years, gaming is still an $80-billion-a-year industry-- a 30% increase over the last few years (Merel, 2011). The method by which we play has changed as well. Mobile gaming grew to a $5.6-billion-a-year industry in 2010 and was estimated at over $25 billion in 2014 (Rosenburg, 2011; Pearson, 2015). McGonigal states that the average gamer may play up to 20 hours a week (2011). Gamers are playing online at staggering amounts as well. Activision claims that gamers spend a combined estimate of 1900 years per day playing some version of their Call of Duty franchise games online (Activision & Blizzard, 2014; Dyer, 2013).

2.4 The Lack of Adequate Cybersecurity Games

Appendix A highlights a number of cybersecurity games that exist today. Although each one does introduce some relevant concepts, none of those reviewed are comprehensive enough to set the appropriate foundation required for a cybersecurity professional. Furthermore, even though some are designed for a multi-player experience, even those do not provide the opportunity to effectively work in a team-based environment. This is a huge gap area. Teamwork is a critical skill in cybersecurity as organizations often are made up of tens or even hundreds of information technology/security members. Collaboration is required for incident handling, digital investigation, implementing technical controls, enforcing policies, and so many other responsibilities required of a cybersecurity professional.

3 Video Game Use by the Department of Defense

In order to understand how game-based learning can be applied to cybersecurity training, it is important to understand how game-based learning and simulations have evolved over the years and how they have been used successfully in the past. One of the largest entities in need of trained cybersecurity professionals is the government and, more specifically, the Department of Defense. The military is no stranger to simulation and game-based training, as we will discuss in the following section. In fact, the military is directly responsible for the invention of the modern-day video games and still sponsors much of the research and enhancements in simulation and game-based training today.

3.1 Video Games Facilitate Scenario-Based Training

Live fire training takes time to coordinate and a lot of resources to accomplish the task, while virtual or game-based training allows for fast and easy repetition and improvement of cognitive processes. Lieutenant Colonel Michael Newell is quoted as saying,

> "gaming provides an ability to actually put yourself in the scenario, go through it and see it. Back up, change the scenario, go through it a different way. Back up, do it again. There are an infinite number of scenarios I can run through, because it's not about *doing* it per se, it's about having *thought* through it." "When you actually get the dirt time, I can throw anything at you I want to, because you've seen it already" (Mead, 2011, p.69)

Several military trainers and leaders feel that virtual and game-based training would be a cost effective way to put soldiers' skills to the test and improve thought processes on the battlefield, before ever putting soldiers in a live fire scenario. The wrong time to learn how to shoot, move, and communicate is on the battlefield where real bullets are flying and lives are at stake. If soldiers can learn small team tactics through virtualized training, then the same methodology could be applied to cybersecurity. A video game provides a cybersecurity professional a virtual environment in which to learn skills, practice techniques, and gain confidence, instead of waiting until critical systems and sensitive data are on the line.

3.2 Video Game Origins in the DoD

The origins of militaristic gaming can be traced back to 1962 when the Pentagon funded MIT to develop the game *Spacewar!* The game consisted of two ships, dots on an oscilloscope screen that could maneuver and fire missiles at each other, both with limited fuel and time. While visually lackluster, this first attempt paved the way for gaming and battle simulation. With the invention of the Atari in the mid 1970's, combat based games began to emerge. *Battlezone* was one of the first games to offer a three-dimensional world and first-person perspective as a tank gunner. Soon afterwards, the Army hired Atari to help modify the game for use as a training implement for the then-new Bradley vehicle, which eventually went on to become known as the Bradley Trainer (Mead, 2011).

The advancements made through games such as the Bradley trainer and *Spacewar!* gained enough notice and attention that the DoD decided to create its own simulation network, known as SIMNET. Many simulators to date were geared towards piloting vehicles. Jack Thorpe, an Air Force captain in 1982, envisioned a network where hundreds or thousands of simulators could be connected to train collectively. While individuals may have been able to pilot a jet or drive a tank in a simulator, groups had never been able to simulate training together. In many cases, the first time pilots flew as a group was in live training exercise or in combat, where the costs of failure could also costs lives (Mead, 2011). By the early 1990's, SIMNET was online and used in preparation for the invasion of Iraq during the first Gulf War, using the Army's Close Combat Tactical Trainer (CCTT). Because of the success of tank missions during the Gulf War, actual engagement data was collected to be used in future simulations. The Army continues to use varying modifications and versions of the CCTT to this day for mounted and dismounted combat training.

3.3 Marine Doom: A Tool for Practicing Team Tactics and Procedures

With a budget hovering around 4% of the total DoD budget, the annual General Officers Symposium issued a mandate to the Marine Corps Modeling and Simulation Office in 1993, to find war games that might be suitable for training and teaching critical decision-making skills (Riddel, 1994; Mead, 2011). Marine Lieutenant Scott Barnett and Sergeant Dan Snyder began the effort of combing through the existing war video game library for candidates. The only game that allowed for shareware and actually encouraged user modification was Doom. As a result, Marine Doom was produced in 1995 for the $49 cost of the game, $25,000 in development costs, and six months of effort (Mead, 2011). A new "skin" put players in forest and urban settings with three other teammates, all working towards a collective mission objective. The team used realistic U.S. military weapons, such as the M-16 rifle and M-249 squad automatic weapon, and a team leader would lead the team through its objectives, drilling on small team tactics and procedures. The game was so popular with the Marines on base that they were literally coming in at night and waiting outside in the hall to get a chance to play (Mead, 2011).

Marine Doom was well received by players, and the numerous reasons for which Marine Doom was developed carried forward into the future of game-based training. The generation entering military service in the 1990's had been living with increased exposure to technology, video games, and computers. The use of game-based training is just one way to keep newer recruits interested and engaged, as well as a method to capitalize on their increased knowledge of technology. Using game-based training can also help reduce costs. While DARPA's SIMNET costs upwards of $140 million over ten years, Marine Doom was produced in a fraction of the time at less than one thousandth of the cost (Mead, 2011).

3.4 America's Army: A Viable Game-Based Training Tool

America's Army is a multiplayer, tactical shooter game where the player acts as a soldier in the U.S. Army. The U.S. Army released the game in 2002 as a recruiting tool, which quickly gained popularity and acclaim for its realism (Mead, 2011). Although the game was primarily a recruitment tool, it also provided potential soldiers with some knowledge and a virtual experience of what a soldier learns in basic training. The initial development cost of the game was slated at around $7.6 million and the average cost to recruit a soldier was around $15,000 at the time of its release. Colonel Wardynski states that if the Army could bring in 300 to 400 new recruits because of America’s Army, then the cost would be worthwhile (Kennedy, 2002). Not only did the game serve as a recruitment vehicle, but it also gave new recruits knowledge prior to arriving at Basic Combat Training, or BCT. It was Colonel Wardynski’s hope that exposure to the information available in America’s Army would reduce the number of washouts, due to a lack of information prior to signing up, and help more recruits complete basic training and move ahead to their individual skill training and their parent units (Kennedy, 2002). The game enables new recruits to get a virtual feel for what training is like and provides incoming recruits with insight on what to expect.

America’s Army has since gone through a few makeovers, with various versions coming out over the years. As a testament to the game’s realism and playability, America’s Army has won several awards and accolades. Congress lauded America’s Army as one of the most effective contact mechanisms in the recruiting arsenal, and a study by MIT found that 30 percent of Americans age 16-24 had a more positive view of the Army as a result of the game (Singer, 2009). America’s Army boasts more than 11 million registered users over the years and is one of the most downloaded war games of all time.

The Army created an accidental training tool in America’s Army by teaching recruits details about weapons, rank structure, military terms, and basic tactics and procedures. America’s Army paved the way for a new generation of virtual combat training simulators that evolved in the wake of America’s Army and the Iraq and Afghanistan wars. The Virtual Combat Convey Trainer and numerous firearms training simulators grew in response for a need to train troops for war. Simulated training has even expanded to other applications such as field medic training, with Engineering and Computer Simulations’ vMedic trainer, which places trainees in an America’s-Army-type environment, but with realistic and time-sensitive combat life-saving objectives.

4 Game-Based Learning for Cybersecurity

4.1 Attributes for Effective Cybersecurity Games

Taking the lessons of previous combat games and simulators, we can apply them to the field of cybersecurity to provide game-based training that incorporates realistic scenarios with live fire events that require players to react in real time. Based on experience of the games and simulations used by the DoD, we have identified the following qualities and characteristics that game-based training should incorporate:

- Game/scenarios need to be as realistic as possible, but also must keep the player's interest.
- Games must reinforce key concepts and skills through repetition and learning from past mistakes.
- Games must be complex enough to keep the player engaged, but at the same time be easy enough to understand so the player does not give up.
- Goals and learning objectives should be clear, even if the way to reach said goal is not 100% explicit. These goals also must be worthwhile in the eyes of the player. A good game might include goals defined by the developers but also leave several smaller goals left up to players to determine, based on what they know they need to accomplish in the long term (Prensky, 2006).

Additionally, Prensky describes five levels of learning in video games (2006), which should be incorporated into cybersecurity game-based training. While these levels were derived from game-based learning for children, they can still be applied to young adults and cybersecurity training.

How	How to play the game; what are the controls and abilities; how can those abilities be used to achieve goals and objectives
What	The rules of the game; what you can and cannot do as well as what the consequences of certain actions are for negative actions
Why	Why certain actions should be performed in a certain way to succeed
Where	The world, culture and environment of the game; your role may dictate what you can and can't do as well as your abilities (e.g. are you a wizard in a medieval castle or a Samurai warrior in Japan)
Whether	The decision making process of the player; decisions create outcomes which may have moral or ethical consequences

The following examples demonstrate how a cybersecurity game can embody these five levels of learning.

How: At a high level, players placed in a cybersecurity situation may learn how to successfully defend a network or system. At a lower level, they may also learn skills such as how to create a security policy, monitor for a certain type of activity, or configure a device.

What: Players should be given a list of rules to follow. The best games have rules that are based in reality and cannot be broken without consequences. In a military game, these might be called rules of engagement. In a cybersecurity training situation, these rules might limit the systems available to the player or may dictate what the player can and cannot change due to other requirements. For example, players may be allowed to write a firewall rule to block or defend against some type of malicious activity, but they cannot simply disconnect the network to prevent all traffic from flowing.

Why: Players learn why they need to make decisions based on trial and error and real-world experience. There may be several different ways to prevent a virus from reaching a system, but trial and error in the game will teach the players which methods are the most effective and the least time consuming. For example, writing one type of firewall rule may accidentally block a legitimate service. Therefore, the player must adjust and then come up with a more efficient way to solve the problem.

Where: The where of the game is very applicable in the cybersecurity setting. Players may have to request information from other virtual locations to complete their objectives. Also, knowing whether the player is working on a government or Fortune 500 company network may impact the decisions made to achieve their objectives. The role each player has on that organization’s team can also dictate his or her actions. Whether the player is the team lead, analyst, or technician may require different types of access and/or limit the actions that they can perform.

Whether: The *Where* of the player also ties into how players make decisions. In any case, players would typically want to confirm or report their findings and actions to some authority figure before enacting a plan of attack. If a Fortune 500 company website is under attack, and your mitigation strategy is to simply power it off, you might have thousands of angry customers who can no longer access important information or services causing loss of revenue. A player’s feeling of stress, joy, or even remorse over a decision can also be used to help prepare them for future real-world experiences. Furthermore, assessing consequences and interacting with other players in leadership roles should be a part of any effective cybersecurity training exercise. Making decisions that will solve the problem, but also have the least impact on critical services, is always paramount for any cybersecurity professional.

4.2 Recommendations

A cybersecurity video game must be fun, engaging, and entertaining. It must attract young adults and keep their attention. They have to be excited for the challenges ahead and in their quest to resolve them. In doing so, they will obtain a better understanding and appreciation for cybersecurity. Those who do not go on to become cybersecurity professionals will have a better understanding of threats, mitigations, and impact on the mission or business. Those who pursue formal education, certification, and careers will have a solid foundation of knowledge and skills.

Listed are several additional ideas and recommendations that could be incorporated into a new cybersecurity video game:

Achievements	Accomplishments must be tied to key cybersecurity learning objectives. Certifications: Obtaining badges for basic understanding of certain operating systems or even for achieving key learning objectives from industry certifications, such as A+, Network+, or Security+. Career Growth: Obtaining badges for system administration, network administration, writing your first script, or even configuring a firewall. For example, these could help career progression from a Systems Administrator to a Network Admin and then to a Security Admin. Item acquisition: The requirement that a gamer achieve certain items before performing a certain task is a great motivator. One sample scenario would require the gamer to obtain an SSL certificate before securely configuring and enabling his or her web server. The understanding of this dependency and its impact on the security posture of a solution can be taught along the way. Similarly, players must acquire items along the way to configure firewalls, intrusion detection systems, routers, and so on. Leaderboard: Inclusion of a leaderboard allows individuals to see who has accomplished certain missions, achieved specific goals, and gained expert knowledge in an area. Building a safe communication mechanism into the game also provides a way to share this knowledge in a peer-to-peer teaching and learning model.
Character Customization and Growth	Gamers need to identify with the characters within the game. The ability to customize their starting attributes and improve their skills, toolsets, and other items along the way helps build a relationship with their character, other players, and with the game itself. Avatar: The ability to choose and configure gender, race, style, and other characteristics of gamers helps them feel as if they are indeed part of the game. Sidekick: Consider including mascot or partner characters who provide hints/help or increase specific attributes. This idea is based on the concept that not all characters within the game space are actual people. There could and should be teachers or helpers throughout the game to guide learning and gameplay. These characters could be acquired, lost, or even traded throughout the gaming experience to help with certain missions. Cyber Characteristics: Integrate cybersecurity concepts into character selection. For example, the game could start with characters or attributes from white-, black-, or grey-hat security professionals: White Hat: help desk, system administrator, network administrator, forensic analyst, malware analyst, incident handling specialist Grey Hat: bug bounty hunter, penetration tester, security assessment professional Black Hat: script kiddie, bot master, malware developer, military adversary

Challenging	Gamers need to participate in difficult, but achievable missions. To support learning objectives, tie these to relevant cybersecurity activities. Real Life: Incorporate actual cybersecurity issues that can be addressed and experience that can be translated to real-world use. For example, • use Open Web Application Security Project (OWASP) Top 10 issues to create challenges and/or achievements (e.g., attack/defend SQL injection, cross-site scripting) • use a social networking attack/defend challenge that takes advantage of trust relationships Other current attacks, such as those on well-known retailers, can be incorporated into challenges to highlight the importance of good defense-in-depth controls. Boss Fight: Provide an escalation of adversaries. For example, a system administrator may face a less sophisticated adversary conducting a phishing attack, but later be targeted by a more advanced persistent threat that requires collaboration with other individuals and teams within the game to detect, respond, and mitigate the attack.
Collaboration	Teamwork and cooperative play is an integral part in many of today's most popular video games. It supports peer-to-peer learning and fosters comradery and a sense of responsibility. Players must be able to post questions and expect responses from other players, team/ guild members, and professional moderators. Real-time chat and other communications are essential to the peer-to-peer learning process and the social aspect of the game. Both virtual and real-person interactions are important. There must be a place or individual that a gamer can turn to for help on-demand that always available.
Educational	To address the critical need to develop future cybersecurity professionals, it is imperative that a video game address key knowledge, skills, and abilities in numerous disciplines. The most important rationale for offering a video game is to prepare our next-generation cybersecurity professionals. Teaching the fundamental concepts and providing the opportunity to obtain advanced knowledge is critical to a game's success. Gameplay must support the ability to obtain knowledge or assistance from a subject matter expert: a lecture, demonstration, or directions from a guru or game master. The video game should provide easy access to a glossary and other reference material for those looking for direct and specific details on topics.
Fun & Relevant	To increase the appeal and "fun" aspects of the video game, it should leverage pop culture, to connect with and engage its audience. It should also replicate relevant real-world processes for obtaining tools and equipment. Movie quotes, tools, and situations from popular fictional movies (e.g., Hackers, The Net, Sneakers, The Matrix, War Games) could increase appeal and help connect with the game's audience. Incorporate popular internet memes or historical events into background events or storylines. Include stores for shopping-- for mascots, gear, and tools to help with missions (e.g., a virtual computer store or marketplace that sells systems, tools, or applications.)

5 What is Next?

We have shown how there is a desperate need for more cybersecurity professionals in our country and the world in general. As expressed previously, there is a need for more than 1 million positions worldwide and billions of dollars in revenue, infrastructure, and intellectual property at stake. Every year young adults are choosing career paths, and the cybersecurity field needs a way to draw the masses. A cybersecurity based game has the potential to make a difference in their choice. Video games have proven to improve cognitive skills, such as reaction time, and the skills taught in the game itself. Games are also valuable teaching tools because they can immerse the player in a realistic environment that is both challenging and rewarding. Additionally, games can provide a virtual proving ground for cybersecurity professionals—cybersecurity is a field where you do not want to experience an attack for the first time on live infrastructure where data and money are on the line. The DoD, U.S. Government, and businesses have much to lose. Our national security, technological secrets, and infrastructure must be protected at all times. The DoD and military have used game-based training and simulation-based training for years. The military was the pioneer in game-based training for aviation and vehicles. Now those games and simulators are being turned to other lifesaving skills such as firearms training, convey operations, and medical response.

It is time for the DoD to invest in a cybersecurity training video game that can be used to prepare our next-generation cyber warriors and information security professionals. We have seen from other examples what a good game requires to be successful. While traditional methods may have positive results, a cybersecurity game could greatly enhance the effectiveness of the DoD's cybersecurity recruiting and training needs. A game very similar to America's Army could teach cyber warriors valuable skills before they step foot on the production floor. It could give individuals an opportunity to take chances, to test, fail, and retest on their technical skills. Additionally, it could validate individuals' self-assurance that they chose the correct field and can make an impact. With the proper funding and development of a highly realistic and effective cybersecurity game, the DoD has an opportunity to make a large impact on the country and our national security. Training related games could also be produced to encompass numerous other disciplines within the IT field, such as networking, digital forensics, or programming. In this way, training-based video games could become one of our best tools for improving information security awareness and building the next generation of cyber warriors.

Appendix A Current Cybersecurity Game Review

The Carnegie Cadets: MySecureCyberspace

This interactive game is designed for fourth and fifth graders and teaches internet safety and computer security in a safe, fun setting. Topics include cyber bullying, recognizing email threats (Spam), fighting malware, and protecting personally identifiable information. MySecureCyberspace was created by Carnegie Mellon's Information Networking Institute and Carnegie Mellon CyLab. The game is freely available for download and roughly 175MB – 225MB depending on the Operating System and most recent updates. The downloaded application requires web access to login with a unique account and maintain user progress records.

MySecureCyberspace is an immersive, interactive, learning experience for young kids. They are exposed to cybersecurity topics in a format that most are familiar with, games. They also have the opportunity to interact with other characters throughout the environment. Although these characters are part of the system, they *do* create a team-based experience for the gamer, even in non-group mode. MySecureCyberspace has a significant teaching and learning component as well. Lesson plans and comprehensive educator guides are available in addition to companion materials for parents to help maximize the learning experience for children.

MySecureCyberspace incorporates numerous popular game elements. These include:

- Good and bad characters with unique traits and capabilities
- Maps to aid navigation of the game space
- Inventory of collectable items and achievements
- Cyberpedia / glossary (that grows as you grow)
- Multiple levels and progression paths
- Customizable characters and/or rooms
- Links to additional internet resources (news, information, more games!)
- Ability to unlocking new quests

Although MySecureCyberspace does provide an engaging and immersive learning experience, the intended audience is younger than our key demographic. Also, the topics presented only skim the surface of cybersecurity and the learners have little opportunity to develop hands-on skills that they can later apply. The requirement to download and install the application may also be considered a barrier.

MySecureCyberspace is available at, http://www.carnegiecyberacademy.com/

CyberCIEGE

CyberCIEGE uses computer gaming technologies and techniques similar to SimCity™. A virtual world is presented to the learner where they can purchase and configure workstations, servers, applications, and network devices. Although specific command syntax and operating systems are not utilized, there is enough detail provided to enhance understanding of numerous cybersecurity concepts. There is a wide range of scenarios available that include tasks to configure strong password policies, or even implement physical security controls and biometrics. Users must spend virtual money on tools, training, or equipment to enhance their security posture and address the current mission objectives. In its longer scenarios, users advance through a series of stages and must protect increasingly valuable corporate assets against escalating attacks.

CyberCIEGE provides learners the opportunity to try, fail, and try again to determine the best cyber protection strategies for a give threat. Learning to manage budgets and return on investment to accomplish the mission is a valuable skill for any cybersecurity professional or manager. The use of 3-D, SIMS-style may be familiar to experienced gamers, and certainly brings the experience a bit closer to reality over 2-D Flash games. In CyberCIEGE gamers get to select the computers and networks they need to work on. They have the opportunity to select, and configure, appropriate cybersecurity controls. Throughout this experience there is exposure to a plethora of concepts including access controls, security logging, authentication options, and even Public Key Infrastructure (PKI) cryptography. More advanced campaigns and scenarios include levels to progress through and users have the opportunity to grow their overall status from “Just Starting” to “Expert” by completing all of the missions. Although there is no set order for accomplishing each scenario, specific instructions on how to do so are readily available.

CyberCIEGE includes more cybersecurity concepts than the other games that we have evaluated. It leverages more advanced gaming technologies to present a real-world environment, and does provide an active learning experience. However, interactions with characters are scripted, and in most cases the gamer is observing/reading these, not participating. There are no opportunities to interact with “real” people and achievements are based on the ability to simply accomplish the mission. Spending more or less virtual money is not a significant contributor to scoring or advancement. Running the game also requires download and installation on a Windows system with Microsoft DirectX.

CyberCIEGE is available at, http://cisr.nps.edu/cyberciege/

Control-Alt-Hack

Control-Alt-Hack is a computer security card game where you, playing the role of a White Hat hacker, have an opportunity to advance within your fictional organization by increasing your “hacker cred”. The game provides detailed scenarios that introduce cybersecurity concepts and terminology. Control-Alt-Hack is also designed to be interesting and enjoyable for a broad demographic including young adults, information security professionals, educators, and just about anyone looking for a brief walk in the shoes of a computer hacker. Players have a choice between sixteen different character cards that can be used within the game. Each has a different rating for hacker skills like Software Wizardry, Cryptanalysis, Social Engineering, and Hardware Hacking. Supplemental skills such as being an expert Barista may even come in handy if your mission requires a Social Engineering activity with you and your coffee cart! Each mission has a subset of tasks that require evaluation of the hacker’s skill, die role, and success value for that challenge. The details provided on the Mission, Character, and Entropy cards come together to form a unique scenario each time the game is played. This helps gamers visualize real-life threat scenarios and better understand how current security practices can help or hinder a malicious adversary.

There are many aspects to Control-Alt-Hack that make this game an excellent introduction to cybersecurity. The target age group of 14+ hits the key demographic that requires exposure to these topics. Results will be varied each time depending on the character, mission, and entropy combinations drawn during gameplay. Implicit learning occurs as players are exposed to different concepts and they visualize how their character's skills could be used to complete a specific challenge. What may seem to be complex topics, like cryptography, are introduced in an easy to digest computer security context. Having a physical game provides an opportunity for face-to-face interactions between gamers of different knowledge and skill levels, peer learning, and social bonding.

Unfortunately one of Control-Alt-Hacks advantages is also the biggest disadvantage. Requiring gamers to be in the same physical location limits opportunities, interactions, and does not take advantage of the mobile computing devices that are always on, and always available to the target demographic. An online video game version of Control-Alt-Hack would greatly increase the availability of this learning experience. Another drawback is the requirement for 3-6 players. A popular aspect of many video games today is that they can be played in both solo and cooperative (team) modes. Adding this capability also increases the playing opportunities, and therefore the chances to learn. Although there are a variety of characters to choose from, Control-Alt-Hack does not provide opportunities for each to grow or be customized by the player. The Entropy cards provide some variability with the opportunity to leverage their "Bag of Tricks" to perhaps go "Dumpster Diving", but the lack of character customization and growth can still be seen as a limiting factor. Finally, the depth of knowledge can be seen as a weakness. Although the game is not intended to be a deep-dive, hands-on, computer security experience, there exists an opportunity to build upon the current model to add more technical details and missions in order to attract players with an existing knowledge of cybersecurity fundamentals.

More information about Control-Alt-Hack is available at, http://www.controlalthack.com.

Cyber Awareness Challenge

The DoD requires all users of federal computer systems to complete Information Assurance Awareness (IA) training. In October 2012 they introduced the CyberAwareness Challenge to meet this requirement. Through this game, users learn security concepts and best practices for their daily work routine. They need to make situational decisions and are introduced to real-world threats such as phishing, malicious code, and spyware. The training takes about 1 hour to complete and leverages Adobe Flash and JavaScript technologies within a web browser. This game exposes everyone to cybersecurity best practices, not just information security professionals. It also combines several elements that make games and game based learning more engaging:

- Personal score tracking, and also an adversary score comparison
- Clear task lists and levels
- Accomplishments and trophies for exceptional decision making
- Realistic computer screen images, videos, and state of the art computer graphics
- Additional features like transcript downloads and captioning options
- Downloadable PDF and DOC takeaways
- Easy access to, and navigation of a glossary of relevant terms

Although this solution provides unique, cutting-edge IA awareness training, it does not target the specific areas required for a cybersecurity professionals. As per design, gameplay is relatively consistent each time. There are limited opportunities to interact with subject matter experts and these experiences are scripted. Learning is limited, in most cases, to binary decisions; one example being the choice to delete or not delete an e-mail message. Although having good judgment and the ability to recognize threats is critical to cybersecurity professionals, the actions taken to prevent, identify, and mitigate threats are often more diverse and very dependent upon unique scenarios. This solution is good for one-time use, or even annual refresher training, but not appropriate as a continuous learning solution.

Cyber Awareness Challenge is available at,http://iase.disa.mil/eta/cyberchallenge/launchPage.htm

Cyber Protect

Sponsored by the U.S. Department of Defense, this web-based game leverages Adobe Flash and JavaScript to introduce learners to various cybersecurity controls. Individuals must manage budgets, requisition tools such as firewalls, anti-virus, access controls, and others. Then, they are required to place the tools appropriately. The effectiveness of their controls is assessed through simulated attacks, in which the controls do or do not block that event. Details of the malicious activities are then presented.

This is a simple, easily accessible game, which introduces many cybersecurity concepts. Participants have the opportunity to learn the various defense-in-depth controls, where to place them, and most importantly, what types of cyber attacks they would defeat. The use of the attack scenarios is a great way to highlight the importance of a specific control and the impact of having, or not having it in place. Other good learning tools include the in-game glossary and ability to print completion certificates and a comprehensive score sheet.

Including Cyber Protect as part of a larger game-set would be useful. The current version would allow mastery to be accomplished in a short period of time (1-2 hours). Although there is some replay value, and perhaps some incentive to obtain a better score, there are no opportunities to collaborate with friends, colleagues, or adversaries. There are limited personal achievements such as levels, rewards, badges, etc., and none that can be compared within the game to other players. An escalation of adversaries, or a diversity of adversaries with each play, would increase replay value.

Cyber Protect is available at, http://iase.disa.mil/eta/cyber-protect/launchpage.htm/

OnGuardOnline.gov

OnGuardOnline.gov is a federal government website managed by the Federal Trade Commission (FTC). It is designed to help individuals be more safe, secure, and responsible online. OnGuardOnline.gov works in partnership with the Stop Think Connect campaign, led by DHS, and is part of the National Initiative for Cybersecurity Education. Numerous resources are available to help people avoid scams, secure their home computers, protect children online, and implement safe online practices. These resources include articles, videos, and even games. OnGuardOnline.gov is a great place to get introduced to cybersecurity, understand online threats, and learn best practices. There are numerous media types available. If individuals learn better through reading, a wide variety of topics are covered in detail with very specific examples provided. Others may prefer to watch professionally developed videos and tutorials. Also, Flash based games are available that combine simple challenges with important lessons. For example, “The Case of the Cyber Criminal” game has a threat actor that must be identified and requires a call to action, “Click on the hacker to stop him in his tracks.” They are then presented with a multiple-choice question to teach important topics like how to safeguard personally identifiable information. If answered correctly, you can select your reward, a tool to eliminate from the hacker’s arsenal. OnGuardOnline also provides downloadable documents, videos, and even games, for offline use.

OnGuardOnline.gov does not target the future cybersecurity professional. There are a number of useful topics that can support awareness, enhance interest, and even provide baseline knowledge on key subjects. For example, there is a very nice video on Wireless Security. However, in most videos, games, and articles the topics are not covered in any depth and they do not address how the numerous technologies and best practices come together to form a sound defense-in-depth strategy. The key shortcoming of OnGuardOnline.gov in the cybersecurity game context is that the resources are individually available. Although they are easy to find on the website, and some topics are presented in “games”, the scope of the content and lessons available are not integrated as one single game or immersive learning experience.

Watchdogs

It should be noted that Watchdogs is by no means a training or education-based game. Watchdogs is a third person free-roam action game, with a grey hat hacker as the protagonist, released in May of 2014 for the Playstation, Xbox, and PC platforms. The game takes place in a fictional Chicago, where the CenTral Operation System, or ctOS, monitors the city via security cameras, and stores personal information on all citizens. ctOS was built in response to the great blackout of 2003, an actual historical event, which was caused by software bug in GE’s management system. In the game, the blackout is fictionally caused by a hacker who was able to breach systems due to the lack of a demilitarized zone in the electrical grid’s network. The protagonist uses his cell phone to hack security cameras, ctOS transmission towers, homes, cell phones, and laptops to achieve his missions. The game does well to portray a hacker as a vigilante trying to bring justice to the city and expose corrupt ctOS leaders for storing secrets on the citizens of Chicago. The game also maintains accuracy when referring to concepts and terms in the hacking and cyber-security domains. What Watchdogs does best regarding the cyber security workforce is perhaps gaining the attention of the younger audience. If a high production value game like Watchdogs can get their feet in the door, than it may provide some benefit to the industry as a whole.

While the game is exciting, fun to play, and may hype up the concept of grey hat hacking and a need for greater cyber-security, it is not meant to be a training game. Hacking sequences are performed by simple button sequences or puzzles, and generally happen instantly. The game plays more like an action game, than a hacking game, and there are many distractions that will have the player driving and shooting their way all over the city. Even though the protagonist of the game is a hacker, hacking is only a small part of the game as a whole. The violence and language in the game makes it unsuitable as a training tool, and may also alienate part of the gaming audience.

Appendix B – Cybersecurity/Game Survey

Age was the first question asked. Roughly 1/3 of the respondents were from each of the three age groups surveyed: under 25, 25-34, and 35 or older. The primary purpose for asking age, education, and profession was to characterize other responses such as technical proficiency areas or preferred video game genres.

The cross section of respondents was also split into thirds regarding education level. Roughly 1/3 had graduate degrees, another 1/3 with 4-year bachelor degrees, and the last third having graduated high school with perhaps some college. Again, the distribution of education levels can be somewhat related to age, as it would be less likely, though not impossible, for most individuals under the age of 25 to have higher levels of education.

In addition to having a diverse survey set of ages and education, it was also intended to sample numerous disciplines and not just information security professionals. 31% of the respondents identified themselves as non-IT/IS professionals. 25% considered themselves students or educators, and over 50% were from the information technology and security sector (note: multiple selections were possible).

The first gaming question was intended to identify which platforms were the most popular among respondents. Overwhelmingly, more than 71% of respondents had played games on a smart phone or tablet within the last 30 days. Although most respondents had also played games on consoles (e.g. Xbox, PlayStation, Wii, etc.) and laptop or desktop computers, the ubiquity of mobile computing devices provides an “always on, always available” medium for accessing games and game based learning.

The next gaming question presented respondents the opportunity to identify which popular games they had spent significant time playing. Of course, not every game on every platform could be listed. The game options within the survey were carefully chosen to help identify the characteristics that could perhaps be valuable inclusions within a future cybersecurity video game. For example, 3 of the top 4 games that respondents spent over 100 hours on could be played individually or with a team (Madden NFL, Call of Duty, or World of Warcraft). Respondent comments also confirmed the value in working with friends, building characters, and working out strategies.

Although some characteristics could be implied by the identification of popular games, the next question asked respondents to specifically identify what they found most important to their gaming experience. The top two video game traits were, “Challenges are difficult but obtainable,” and, “Character growth – achievements, items, abilities.”

The next question in the survey was intended to identify what respondents believe to be their current proficiency level in certain technical areas. Of the technologies listed, computer applications (e.g. MS Office) and mobile devices (e.g. iPhone, iPad, Droid phone/tablet) had the highest scores for participants having pretty good skills. Defense in depth concepts, network protocols, and social engineering topped the list of limited knowledge topics.

When filtering these answers by respondent age there was a noticeable jump in social media knowledge and skills. However, the survey did not differentiate between security and privacy issues within social networking. With the increased use of applications like Twitter and Facebook among young adults, and over 87% of the under 25 respondents believing they have a good understanding of mobile computing devices, the increase in believed proficiency with social media was as expected. Most within the younger age group had some familiarity with network devices, wireless security, computer components, and operating systems. However, the limited skills and experience in these areas confirm conclusions that the foundational building blocks of security professionals are under developed for this age group.

The next question asked respondents to identify key areas that should be taught at the high school level. Not surprisingly these included Computers (Hard drives, RAM, CPU, etc.) and Operating Systems. Over 65% of respondents also indicated that personal privacy issues on the internet, computer applications (e.g. MS Office), social networking best practices, network devices, and security applications like anti-virus and anti-spam should absolutely be taught in high school.

Survey respondents from the 18-21 age group provided the most input for a new cybersecurity video game. Inspired by games like Runescape (http://www.runescape.com), World of Warcraft, (http://us.battle.net/wow/en/), Adventure Quest Worlds (http://www.battleon.com), and numerous others, they were able to communicate what keeps them actively engaged throughout their online experience. Many of these suggestions have been incorporated into the current list of recommendations.

For 18-21 year olds it is important to relate cybersecurity concepts to other more identifiable and relatable topics. For example, when describing defense-in-depth controls we often use the analogy of a castle. A moat, drawbridge, archers, inner walls, and numerous other characteristics of medieval defenses can be matched to a cybersecurity posture. Relating these concepts to firewalls, intrusion detection/prevention systems and other defenses is pretty easy for anyone to understand, not just high school students. In addition to relatable analogies, this group also recognized the need for better understanding of fundamental concepts. For example, what are the different operating systems available and the strengths and use-cases for each? They often knew that command line functionality existed, but have limited-to-no experience with the fundamental commands used to navigate the directory structure, perform file management, or obtain system information. Cybersecurity terminology should also be introduced. Advanced details are not required, but broad exposure to terms and topics like firewall, intrusion detection, signatures, defense-in-depth, WiFi security settings, TCP/IP fundamentals, basic PC and network hardware, etc. could provide a better overall picture early on that would aid future understanding of more in-depth learning.

Non-cybersecurity professionals had similar responses to those from the 18-21 group. There was a strong desire to better understand Operating Systems and command line fundamentals, but they raised some very specific questions:

- “If there is a network firewall at work, why do I need one on my computer?”
- “What are the free tools available and why would I pay for something else?”
- “What is A/V, Anti-Malware, and all of the other security software?”
- “How can I do stuff for friends, family, and work to help”

These questions highlight that the more established professionals have a better idea of, “knowing what they don’t know,” versus the younger audience that, in general, has very few ideas where and how to get started in cybersecurity.

As expected, the cybersecurity trainers, educators, and professionals provided far more detailed list of topics and concepts that should be presented to a high school audience. These included:

- Although awareness tools, sites, and games are available, it is still necessary to present threats and vulnerabilities such as phishing, protecting personally identifiable information, and the dangers of social networking.
- Rarely is home cybersecurity addressed and the need to understand and properly configure home protections (e.g. WiFi passwords, XBOX Live accounts, password policies)
- Awareness of social engineering tools, techniques, and objectives should also be presented
- A general understanding of how the internet works is critical (e.g. browsers, DNS, TCP/IP, Networks, etc.)
- An introduction to internet browser security would be extremely valuable (e.g. SSL certificates, good/bad browser add-ons, cookies, malicious scripts)
- Defense in depth concepts and tools (e.g. firewalls, IDS, AV, patching, etc.)
- Understanding a threat surface and how it expands/contracts based on protections in place (e.g. What is “hardening”)
- What are the various industry certifications available, and how can they be used to improve individual knowledge, skills, and career opportunities
- Identify cybersecurity jobs and key roles/responsibilities of each
  - Correlating with NICE, DoD 8570, others
  - Correlating with certifications
  - Correlating with Salary ranges
  - Correlating with real-world threats, news stories, other examples
- Introduce computer programming concepts
  - Languages and what each is used for (e.g. Python, Ruby, Java, C)
  - Fundamental concepts (e.g. loops, functions, variables)
- Wireless security fundamentals (e.g. protecting SSIDs and passwords, using strongest authentication possible)
- Network device fundamentals (e.g. hardware address, IP address, routing, switches versus hubs and routers)
- IP protocol fundamentals (e.g. addresses, subnet masks, routing)
- Introduce buzz words and topics such as BYOD, “the Cloud” and how those concepts relate to cybersecurity
- Emphasize understanding what “normal” looks like on a network, and how detect differences, anomalies, or other indicators of malicious activity

References/Bibliography

URLs are valid as of the publication date of this document.

[Activision 2014]

Activision & Blizzard. (2014). First Quarter 2014 Results [PDF Document]. Retrieved from http://investor.activision.com/events.cfm.

[Baldor 2014]

Baldor, Lolita C. & Jelinek, Pauline (March 2014). “Pentagon to triple cyber staff to thwart attacks”. Associated Press. Retrieved from http://kfwbam.com/2014/03/28/pentagon-to-triple-cyber-staff-to-thwart-attacks

[Bureau of Labor Statistics 2014]

Bureau of Labor Statistics. (Jan 8, 2014).Occupational Outlook Handbook: Information Security Analysts. Retrieved from http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[Center for Strategic and International Studies 2013]

Center for Strategic and International Studies. (2013).The Economic Impact of Cybercrime and Cyber Espionage. [PDF Document] Retrieved from http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

[CISCO 2014]

CISCO. (2014). CISCO 2014 Annual Security Report. [PDF Document] Retrieved from http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

[Dye 2009]

Dye, M. W., Green, C. S., & Bavelier, D. (2009). Increasing speed of processing with action video games. Current Directions in Psychological Science, 18(6), 321-326.

[Dyer 2013]

Dyer, M. (2013, Nov 4). People Play 1900 Years of Call of Duty Multiplayer Every Day. Retrieved from http://www.ign.com/articles/2013/11/04/people-play-1900-years-of-call-of-duty-multiplayer-every-day.

[Frost 2013a]

Frost and Sullivan. (2013). The 2013 (ISC)^2 Global Information Security Workforce Study. [PDF Document] Retrieved from https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf.

[Frost 2013b]
Frost and Sullivan. (2013). Agents of Change: Women in the Information Security Profession, The (ISC)2 Global Information Security Workforce Subreport. [PDF Document] Retrieved from https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf

[Granic 2013]
Granic, I., Lobel, A., & Engels, R. C. (2013). The benefits of playing video games.

[Kennedy 2002]
Kennedy, B. (2002, July 11). "Uncle Sam Wants You (To Play This Game)." New York Times. http://www.nytimes.com/2002/07/11/technology/uncle-sam-wants-you-to-play-this-game.html

[Libicki 2014]
Libicki, M., Senry, D., & Julia, P. (2014). Hackers Wanted: an examination of the cybersecurity labor market. RAND.

[Lubinski 2010]
Lubinski, W., Bendow, C.P, & Steiger, J. H. (2010). Accomplishment in science, technology, engineering, and mathematics (STEM) and its relation to STEM educational dose: A 25-year longitudinal study. Journal of Educational Psychology. 102, 860-871. Doi: 10.1037/a0019454.

[McGonigal 2011]
McGonigal, J. (2011). Reality is Broken: Why Games Make Us Better and How They Can Change the World. London: Penguin.

[Mead 2011]
Mead, C. (2011). War Play: Video Games and the Future of Armed Conflict. New York: Houghton Mifflin Harcourt.

[Merel 2011]
Merel, T. (2011, July 6). The Big V: The great games market split. Retrieved from http://venturebeat.com/2011/07/06/the-big-v-the-great-games-market-split/.

[Pearson 2015]
Pearson, D. (2014). Report: Mobile gaming to become gaming's biggest market by 2015. Retrieved from http://www.gamesindustry.biz/articles/2014-10-22-report- mobile-to-become-gamings-biggest-market-by-2015.

[Prensky 2006]
Prensky, M. (2006). "Don't Bother Me Mom – I'm Learning." Sat. Paul: Paragon House.

[Raytheon 2013]
Raytheon. (2013). Preparing Millennials to Lead in Cyberspace. [PDF Document] Retrieved fromhttp://www.raytheon.com/capabilities/rtnwcm/groups/gallery/documents/digitalasset/rtn_158203.pdf.

[Riddel 1994]
Riddell, R. (1994, April). Doom Goes to War. Wired 5.4 Retrieved from http://archive.wired.com/wired/archive/5.04/ff_doom_pr.html

[Rosenberg 2010]
Rosenberg, D. (2010, May 26). Mobile-gaming revenue to hit $11.4 billion in 2014. Retrieved from http://www.cnet.com/news/mobile-gaming-revenue-to-hit-11-4-billion-in-2014/.

[Singer 2009]
Singer, P. (2009, Nov 17). Video Games Veterans and the New American Politics. Washington Examiner. Retrieved from http://washingtonexaminer.com/video-game-veterans-and-the-new-american-politics/article/20385

[Turman 2010]
Turman, L. (Sep 27, 2010). "Action video games speed up decision-making process." Washington Post. Retrieved from http://washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092705244.html.

[US GAO 2013]
United States Government Accountability Office. (Sep 2013). DHS Recruiting and Hiring: DHS is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts. [PDF Document]. Retrieved from http://www.gao.gov/assets/660/657902.pdf.