



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

Christopher Herr
Dennis Allen

Carnegie Mellon University

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 01 OCT 2014		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Christopher Herr Dennis Allen				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 22	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Copyright 2014 ACM

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.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This material has been approved for public release and unlimited distribution.

DM-0001692

1 Table of Contents

2	TABLE OF CONTENTS	I
3	ABSTRACT	II
4	1 THE CYBERSECURITY WORKFORCE SHORTAGE	3
5	1.1 GREATER CYBERSECURITY EDUCATION IS NEEDED FOR PRIMARY/SECONDARY STUDENTS	3
6	2 VIDEO GAMES AS A UBIQUITOUS LEARNING TOOL	4
7	2.1 HOW VIDEO GAMES CAN BE EFFECTIVE LEARNING TOOLS.....	4
8	2.2 VIDEO GAMES REACH A LARGE AND DIVERSE AUDIENCE	5
9	2.3 THE PREVALENCE OF VIDEO GAMING	6
10	3 VIDEO GAME USE BY THE DEPARTMENT OF DEFENSE	7
11	3.1 VIDEO GAMES FACILITATE SCENARIO-BASED TRAINING.....	7
12	3.2 VIDEO GAME ORIGINS IN THE DoD.....	8
13	3.3 MARINE DOOM: A TOOL FOR PRACTICING TEAM TACTICS AND PROCEDURES.....	8
14	3.4 AMERICA’S ARMY: A VIABLE GAME-BASED TRAINING TOOL	9
15	4 GAME-BASED LEARNING FOR CYBERSECURITY	11
16	4.1 ATTRIBUTES FOR EFFECTIVE CYBERSECURITY GAMES.....	11
17	4.2 RECOMMENDATIONS.....	13
18	5 WHAT IS NEXT?	16
19	BIBLIOGRAPHY	18

20

21

22

1 **Abstract**

2 There is a global shortage of more than 1 million skilled cybersecurity professionals needed to
3 address current cybersecurity challenges (CISCO, 2014). Criminal organizations, nation-state ad-
4 versaries, hacktivists, and numerous other threat actors continuously target business, government,
5 and even critical infrastructure networks. Estimated losses from cyber crime and cyber espionage
6 amount to hundreds of billions annually (Center for Strategic and International Studies, 2013).
7 The need to build, maintain, and defend computing resources is greater than ever before.
8 A novel approach to closing the cybersecurity workforce gap is to develop cutting-edge cyberse-
9 curity video games that (1) grab the attention of young adults, (2) build a solid foundation of in-
10 formation security knowledge and skills, (3) inform players of potential career paths, and (4) es-
11 tablish a passion that drives them through higher education and professional growth. Although
12 some video games and other games do exist, no viable options are available that target high-
13 school-age students and young adults that supply both a quality gaming experience and foster the
14 gain of key cybersecurity knowledge and skills. Given the Department of Defense’s success with
15 simulations and gaming technology, its sponsorship of a cybersecurity video game could prove
16 extremely valuable in addressing the current and future needs for our next generation cyber warri-
17 ors.

18

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 Needed 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 cybersecuri-

ty workforce. An important observation was that 78% of college students decided to study Science, 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 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 Effective Learning Tools

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

1 of the games per week outside of class had a 25% increase in vocabulary and language skills and
2 a 50% increase in math skills over students who had only classroom instruction (Prensky, 2006).
3 The results from this study demonstrate the benefit of gaming beyond entertainment value.
4 Outside of games specifically aimed at education, gamers who play fast-paced action games have
5 been shown to have faster average reaction times when compared to non-gamers, and research
6 also found that this increase in reaction speed had a negligible loss of accuracy (Dye, Green, &
7 Bavelier, 2009). Studies also found that subjects playing 50 hours of the fast-paced role-playing
8 games “Call of Duty 2” and “Unreal Tournament” made accurate decisions when exposed to
9 fast-moving visual stimuli--up to 25% faster than subjects who played slower moving strategy-
10 based games (Turman, 2010). These studies have also shown that video game types, such as first
11 person shooters, have even improved cognitive skills and spatial navigation. The latter has been
12 previously linked to long-term success in STEM careers (Lubinski et al. 2010).
13 Gaming is also often seen as a way to relieve stress and exercise the mind’s more emotional side.
14 A January 2014 study published by the American Psychological Association evaluates the cogni-
15 tive, emotional, social, motivational, and mental benefits of video games. Research found that
16 players learn valuable cooperative skills by playing cooperative and challenging games with oth-
17 ers (Granic et. al., 2013). Granic and others also hypothesize that game playing can invoke moods
18 and emotions that are not only beneficial to our own mental and emotional state but also make us
19 generally more mentally healthy (2013).
20 These studies indicate that gaming can be used as a tool to train your brain and can be used to
21 teach basic quantitative and qualitative skills such as math and language. Furthermore, games can
22 also serve to enhance proper cooperative behaviors and relieve stress. These qualities are neces-
23 sary for any game that is aimed at effectively teaching future cyber warriors.

24 **2.2 Video Games Reach a Large and Diverse Audience**

25 The makeup of the gamer population has evolved to a more heterogeneous constituency, strength-
26 ening 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 has also grown to a \$5-billion-a-year industry and is expected to double by 2014 (Rosenburg, 2011). 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).

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, 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 cost 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,

1 1994; Mead, 2011). Marine Lieutenant Scott Barnett and Sergeant Dan Snyder began the effort of
2 combing through the existing war video game library for candidates. The only game that allowed
3 for shareware and actually encouraged user modification was Doom. As a result, Marine Doom
4 was produced in 1995 for the \$49 cost of the game, \$25,000 in development costs, and six months
5 of effort (Mead, 2011). A new “skin” put players in forest and urban settings with three other
6 teammates, all working towards a collective mission objective. The team used realistic U.S. mili-
7 tary weapons, such as the M-16 rifle and M-249 squad automatic weapon, and a team leader
8 would lead the team through its objectives, drilling on small team tactics and procedures. The
9 game was so popular with the Marines on base that they were literally coming in at night and
10 waiting outside in the hall to get a chance to play (Mead, 2011).

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

19 **3.4 America’s Army: A Viable Game-Based Training Tool**

20 America’s Army is a multiplayer, tactical shooter game where the player acts as a soldier in the
21 U.S. Army. The U.S. Army released the game in 2002 as a recruiting tool, which quickly gained
22 popularity and acclaim for its realism (Mead, 2011). Although the game was primarily a recruit-
23 ment tool, it also provided potential soldiers with some knowledge and virtual experience of what
24 a soldier learns in basic training. The initial development cost of the game was slated at around
25 \$7.6 million and the average cost to recruit a soldier was around \$15,000 at the time of its release.
26 Colonel Wardynski states that if the Army could bring in 300 to 400 new recruits because of

1 America's Army, then the cost would be worthwhile (Kennedy, 2002). Not only did the game
2 serve as a recruitment vehicle, but it also gave new recruits knowledge prior to arriving at Basic
3 Combat Training, or BCT. It was Colonel Wardynski's hope that exposure to the information
4 available in America's Army would reduce the number of washouts, due to a lack of information
5 prior to signing up, and help more recruits complete basic training and move ahead to their indi-
6 vidual skill training and on to their parent units (Kennedy, 2002). The game enables new recruits
7 to get a virtual feel for what training is like and provides incoming recruits with insight on what to
8 expect.

9 America's Army has since gone through a few makeovers, with various versions coming out over
10 the years. As a testament to the game's realism and playability, America's Army has won several
11 awards and accolades. Congress lauded America's Army as one of the most effective contact
12 mechanisms in the recruiting arsenal, and a study by MIT found that 30 percent of Americans age
13 16-24 had a more positive view of the Army as a result of the game (Singer, 2009). America's
14 Army boasts more than 11 million registered users over the years and is one of the most down-
15 loaded war games of all time.

16 The Army created an accidental training tool in America's Army by teaching recruits details
17 about weapons, rank structure, military terms, and basic tactics and procedures. America's Army
18 paved the way for a new generation of virtual combat training simulators that evolved in the wake
19 of America's Army and the Iraq and Afghanistan wars. The Virtual Combat Convey Trainer and
20 numerous firearms training simulators grew in response for a need to train troops for war. Simu-
21 lated training has even expanded to other applications such as field medic training, with Engineer-
22 ing and Computer Simulations' vMedic trainer, which places trainees in an America's-Army-type
23 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 that may have moral or ethical consequences

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

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

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

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

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

23 **Whether:** The *Where* of the player also ties into how players make decisions. In any case, players
24 would typically want to confirm or report their findings and actions to some authority figure be-
25 fore enacting a plan of attack. If a Fortune 500 company website is under attack, and your mitiga-
26 tion strategy is to simply power it off, you might have thousands of angry customers who can no

1 longer access important information or services. A player's feeling of stress, joy, or even remorse
2 over a decision can also be used to help prepare them for future real-world experiences. Further-
3 more, assessing consequences and interacting with other players in leadership roles should be a
4 part of any effective cybersecurity training exercise. Making decisions that will solve the problem
5 but also have the least impact on critical services is always paramount for any cybersecurity pro-
6 fessional.

7 **4.2 Recommendations**

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

14 Below are several additional ideas and recommendations that could be incorporated into a new
15 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 has 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.

The DoD should invest in game-based, cybersecurity training 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 a difference. With the funding and development of a realistic and effective cybersecurity game, the DoD has an

1 opportunity to make a large impact on the nation. The video game could then become one of our
2 best tools in improving information security awareness and building the next generation of cyber
3 warriors.

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

- 1 [https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-](https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf)
2 [Security-Profession-GISWS-Subreport.pdf](https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf)
- 3 **[Granic 2013]**
4 Granic, I., Lobel, A., & Engels, R. C. (2013). The benefits of playing video games.
- 5 **[Kennedy 2002]**
6 Kennedy, B. (2002, July 11). "Uncle Sam Wants You (To Play This Game)." New York Times.
7 <http://www.nytimes.com/2002/07/11/technology/uncle-sam-wants-you-to-play-this-game.html>
- 8 **[Libicki 2014]**
9 Libicki, M., Senry, D., & Julia, P. (2014). Hackers Wanted: an examination of the cybersecurity
10 labor market. RAND.
- 11 **[Lubinski 2010]**
12 Lubinski, W., Bendow, C.P., & Steiger, J. H. (2010). Accomplishment in science, technology, en-
13 gineering, and mathematics (STEM) and its relation to STEM educational dose: A 25-year longi-
14 tudinal study. *Journal of Educational Psychology*. 102, 860-871. Doi: 10.1037/a0019454.
- 15 **[McGonigal 2011]**
16 McGonigal, J. (2011). *Reality is Broken: Why Games Make Us Better and How They Can*
17 *Change the World*. London: Penguin.
- 18 **[Mead 2011]**
19 Mead, C. (2011). *War Play: Video Games and the Future of Armed Conflict*. New York: Hough-
20 ton Mifflin Harcourt.
- 21 **[Merel 2011]**
22 Merel, T. (2011, July 6). The Big V: The great games market split. Retrieved from
23 <http://venturebeat.com/2011/07/06/the-big-v-the-great-games-market-split/>.
- 24 **[Prensky 2006]**
25 Prensky, M. (2006). "Don't Bother Me Mom – I'm Learning." Sat. Paul: Paragon House.
- 26 **[Raytheon 2013]**
27 Raytheon. (2013). *Preparing Millennials to Lead in Cyberspace*. [PDF Document] Retrieved
28 from [http://www.raytheon.com/capabilities/rtnwcm/groups/gallery/documents/digitalasset/rtn_158](http://www.raytheon.com/capabilities/rtnwcm/groups/gallery/documents/digitalasset/rtn_158203.pdf)
29 [203.pdf](http://www.raytheon.com/capabilities/rtnwcm/groups/gallery/documents/digitalasset/rtn_158203.pdf).
- 30 **[Riddell 1994]**
31 Riddell, R. (1994, April). *Doom Goes to War*. Wired 5.4 Retrieved from
32 http://archive.wired.com/wired/archive/5.04/ff_doom_pr.html
- 33 **[Rosenberg 2010]**
34 Rosenberg, D. (2010, May 26). Mobile-gaming revenue to hit \$11.4 billion in 2014. Retrieved
35 from <http://www.cnet.com/news/mobile-gaming-revenue-to-hit-11-4-billion-in-2014/>.

- 1 **[Singer 2009]**
2 Singer, P. (2009, Nov 17). Video Games Veterans and the New American Politics. Washington
3 Examiner. Retrieved from [http://washingtonexaminer.com/video-game-veterans-and-the-new-](http://washingtonexaminer.com/video-game-veterans-and-the-new-american-politics/article/20385)
4 american-politics/article/20385
- 5 **[Turman 2010]**
6 Turman, L. (Sep 27, 2010). "Action video games speed up decision-making process." Washington
7 Post. Retrieved from [http://washingtonpost.com/wp-](http://washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092705244.html)
8 dyn/content/article/2010/09/27/AR2010092705244.html.
- 9 **[US GAO 2013]**
10 United States Government Accountability Office. (Sep 2013). DHS Recruiting and Hiring: DHS
11 is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Re-
12 cruiting Efforts. [PDF Document]. Retrieved from <http://www.gao.gov/assets/660/657902.pdf>.