Virtual worlds and online gaming communities are fast becoming the predominant entertainment medium in the world. Collectively, they are projected to generate $112 billion in sales revenues annually by 2015 from hundreds of millions of individuals worldwide who subscribe to them. Millions of users enjoy these “digital playgrounds” every day, and very rarely is their experience interrupted by inappropriate or criminal behavior.

Unfortunately, as more people subscribe to virtual worlds, and as the number of online games increase, the opportunities for socially and economically harmful crime will correspondingly rise. The law enforcement community must, consequently, begin to develop a capacity to address criminal activities in virtual and online gaming communities in their efforts to police cyberspace and to protect the jurisdictions they serve.

Over the past two years, the Bureau of Justice Assistance (BJA), in partnership with Drakontas and Drexel University, has been investigating the rise of crime in virtual worlds and online gaming communities, and its impact on the people that subscribe to and play them. This document is designed to help raise awareness about the kinds of crimes being committed in virtual and online gaming worlds, and to provide an overview on the methods of social interaction that occur within these worlds and what law enforcement and the broader criminal justice community can do to respond to and mitigate future incidents.
According to a recent report\textsuperscript{2} from Interpol, the International Criminal Police Organization headquartered in Lyon, France, virtual worlds can often be classified according to their specific features. The most commonly seen types of virtual worlds fall into two general categories: game playing and community-based. Both of these types of virtual worlds are created to provide entertainment, first and foremost, while some also provide social engagement and interaction, as well as monetary benefits to their users. In the game-playing category, social interaction is not only encouraged, but is required, as players will only be able to advance so far and accomplish set-goals within a game before they will need to call upon others to assist them.

Community-based virtual worlds, on the other hand, have no specific purpose from the players’ perspective, aside from fostering social interaction and providing entertainment. Any person can explore community-based virtual worlds without the assistance of other players that is required in game-based virtual worlds.

No matter what type of virtual world or online gaming world one plays, there are inherent risks associated with each of them, as the people one encounters along the way may have ulterior, criminal motives. The criminal opportunities that exist within virtual worlds, and the subsequent call to action, that is required by law enforcement and crime prevention communities, will be addressed in the following pages.

In his book, *Virtual Justice: The New Laws of Online Worlds*, Dr. Greg Lastowka of Rutgers University defines virtual worlds and online gaming communities as “Internet-based simulated environments that feature software-animated objects and events.”
Today’s digital playgrounds and online communities have been created, as highlighted above, for children and adults as vehicles for social engagement, entertainment, diversion, and, on occasion, as places to make money by selling and buying digital goods and services.

However, just like playgrounds in the real world, digital playgrounds offer myriad new locations and opportunities for criminals to prey on unsuspecting individuals and to commit traditional “real-world” crimes, like theft, money laundering, bullying, and stalking. The companies behind these new gaming environments certainly did not intend to create virtual worlds that facilitate criminal behaviors, and most companies actively protect the safety and security of their users. Nonetheless, these measures have not prevented criminals from exploiting vulnerabilities in gaming platforms and systems.

For instance, the major gaming systems on the market today each have embedded communications features and provide access to social networking platforms. Additionally, many have internet browsing capabilities, allowing users to access any number of social media sites where they can meet friends or seek to establish new relationships.

One of the major challenges in these virtual environments, however, is being able to identify the person on the other end of the internet with whom one is communicating. Due to the fact that many of these virtual and online gaming worlds are often free or very inexpensive to use, a person can easily register for a particular game and provide false information. For example, a person can indicate on a virtual world registration page that she is a 14-year old girl, when “she” is, in reality, a 35-year old man. Here, the communications capabilities – chat, voice, text messaging – all become potential means by which criminals can exploit and target an unsuspecting victim.
This is especially troubling if a young person is unaware of the dangers inherent in virtual worlds and online gaming worlds and is not monitored while playing in a digital playground. Complicating the issue even further is that many of these virtual worlds are built on the need for social interaction in order to advance to new levels within a particular game. Communication with other players is often paramount to one’s success within a game and this fact further increases the opportunity and likelihood for social or economic harms.

These same social capabilities have been used by criminals to oversee and monitor prostitution rings and by drug dealers to coordinate the exchange of illicit goods. They use the gaming system as a communications platform in order to evade wiretaps, as this is a channel that law enforcement is not as likely to monitor.

Each gaming platform also has some form of storage capacity and, much like a traditional personal computer, these can be locations for storing pictures and videos. This provides a child pornographer with another location to hide illicit images, and the file sharing permitted by these systems and embedded into the virtual worlds and online gaming communities accessed via the gaming consoles offer new potential distribution mechanisms for these illegal materials.

Many of these virtual worlds and online gaming communities are accessible via handheld gaming devices or even via smartphones. The gaming companies are seeking to ensure the gaming experience is accessible wherever cellular networks can connect users to the games.

Sometimes, the games are even designed to combine real world and virtual world interactions, where users know the physical location of other participants so that they can meet or receive offers for special deals from retailers that are near their location. This same information can be intercepted and used as a beacon for a cyberstalker, or offer targets for child exploitation.

There are also vulnerabilities arising from the economic systems built to support virtual worlds and online gaming communities. Many virtual worlds have their own currency, Threats and Vulnerabilities (Continued)

Below are several kinds of socially harmful illegal activities occurring in and/or inadvertently facilitated by virtual worlds and online gaming communities:

• **Online Solicitation of a Minor:** Using communication tools (e.g., email, video chat, audio chat, text chat, and instant messaging) in a gaming environment or virtual world to engage in sexually explicit conversations with a minor or for the purposes of arranging a sexual encounter in the physical world.

• **Child Pornography:** Storage and distribution of images or videos via a gaming console that contains people under the age of 18 in a sexual situation.

• **Harassment, Bullying, and Stalking:** Using communication tools (e.g., email, video chat, audio chat, text chat, and instant messaging) in a gaming environment or virtual world to threaten, annoy, or alarm other players.
so that people playing the game can buy and sell objects. For the gaming company, this is another way of making money from the game; estimates are that revenues from virtual goods will exceed $14 billion by 2014.\(^3\)

Most of these revenues come from “micro-transactions”—small purchases of less than $1 that make up the bulk of consumer purchases of virtual goods. The process is very simple: a person plays a game for which he or she pays a nominal monthly subscription fee. In addition, the user has the option of customizing an avatar—the user’s digital character within a virtual world or online gaming world—or purchasing additional items to increase the avatar’s strength or weaponry. Each of these items, sometimes referred to as add-ons, can be purchased for a small fee. These purchases can add up to a sizable sum of money over time. Considering there are many virtual worlds with hundreds of thousands of subscribers, the companies behind these games stand to reap significant revenues from these micro-transactions.

In some cases, a virtual world company will blur the lines between the real world and the virtual world in order to maximize its profits for a particular brand. Imagine a virtual world created for children, wherein a parent can spend a few pennies to purchase a piece of digital jewelry for his or her child’s virtual doll. This “virtual” jewelry just so happens to look exactly like the jewelry the parent also purchases in the physical world for the child’s “real” doll, allowing the company to maximize the amount of time a child interacts with its brand in both the real and virtual worlds, thereby increasing its bottom line.

Generating profits in the real and virtual worlds isn’t a crime. However, with the increasing complexities involving real and virtual currency transactions, there is a correspondingly rising likelihood that fraud and other crimes will be perpetrated in these environments. Law enforcement needs to be aware of and familiar with these payment systems so that they are prepared to respond accordingly.

There are millions upon millions of small transactions like this, happening every day, crossing credit card platforms, banking systems, and payment systems.
services throughout the world. It is the kind of playground where criminals can make money if they know how to intercept those transactions.

The sheer volume of transactions and sums of money involved make virtual worlds and online games inviting targets for fraud, identity theft, and other economically harmful crimes. Gaming companies have become the new targets for cybercriminals looking to steal credit card information or intellectual property associated with the games themselves.

Phishing schemes, where computer users are tricked into entering user names, passwords, and credit card information into websites that appear to be legitimate, are just as likely to target gaming brands as they are to exploit large banking institutions. This is, in great part, due to the fact that many gaming companies store both personally identifiable information and financial data of their members on servers across the globe. Criminals gaining access to this information, using phishing schemes or other nefarious methods, can easily reap millions of dollars.

Additionally, many gaming companies have created digital currencies that are meant to facilitate transactions within the virtual world. Some companies even contemplated that their virtual currencies would be transferrable into real world currencies. There are even currency exchange platforms that allow users to trade in and out of virtual currencies in the same way they could trade foreign currencies in the real world. Individuals provide virtual goods and services – everything from new dresses for an avatar to virtual prostitution – and money paid for these goods and services can be transferred into U.S. dollars through the currency exchange. However, unlike traditional “real” world banks, these virtual exchanges and operations are not subject to the same regulatory oversight.

This trend is likely to expand further in the coming years, as gaming companies seek to maximize the consumer’s engagement with the gaming platform on a daily basis. There was even one gaming company several years ago that had registered for and received a banking license, which allowed gamers to transfer currency in and out of the game readily through ATMs or a “real-world” bank branch. This creates a parallel banking system, where the potential exists for money laundering and the illicit transfer of goods. There are also criminal organizations that use these virtual currencies to earn real money, selling illegally obtained virtual goods to game players interested in obtaining a powerful sword or special potion so they can advance to the next level of the game.

For people who have never played one of these games, this may seem a bit farfetched. Yet, these social and economic harms are very real and have been documented in the articles and news stories included as an appendix to this document. The list we provide represents the tip of the iceberg – an increasing threat that law enforcement must address now.
Law enforcement is constantly required to adapt its strategies and tactics to combat the rise of new criminal behavior. The increase of socially and economically harmful activity in virtual worlds and online gaming communities requires a unified response from law enforcement and other key stakeholders, some of which will come from refocusing existing policies, procedures, and capabilities to match this new threat.

Nevertheless, new capabilities are required to ensure law enforcement has sufficient capacity and tools at their disposal to respond effectively. Some of these are outlined below.

**INCREASED AWARENESS**
First and foremost, it is imperative that awareness be raised among the criminal justice community regarding the threats posed by crimes in virtual worlds and online gaming communities. The Symposium held in Philadelphia, pictured above - along with the training sessions conducted by Drakontas LLC and Drexel University, as part of BJA’s program - represent a first step in helping law enforcement better understand the challenges.

**UPDATED POLICIES AND PROCEDURES**
Second, existing policies and procedures need to be refined given the nature of the investigatory process. For instance, as gaming technologies and digital storage devices evolve and are increasingly adopted around the world, the potential locations for digital evidence also increases. Information is now being stored on machines and devices located in other countries.
on other continents far away from a particular user’s gaming system.

This greatly complicates an investigator’s work. An investigator needs to search for evidence on local devices (i.e., a computer or gaming system), but they also must reach out to Internet Service Providers (ISPs) and the gaming companies, as well as the third party payment services that often serve as the marketplace for the exchange of digital goods and services. Each has vital information that law enforcement will want to use during an investigation, but it can be very difficult and time consuming to collect all of the relevant information for a particular case involving gaming systems. Law enforcement must piece together the various technologies involved that facilitate the connection between an offender and a victim. They must also familiarize themselves with the data storage and retention practices of virtual world companies, as they begin investigating game-related cases for the first time.

NEW FORENSICS TOOLS

Finally, there are few tools available to automate the process of examining the gaming devices and platforms used as gateways to these virtual worlds and online gaming communities. Law enforcement has had success over the years in conducting digital forensics investigations on traditional computing devices, such as personal computers and laptops; however, the pace at which video game consoles and handheld electronic devices have emerged and been adopted by consumers has presented a number of pressing issues for law enforcement and private industry.

Video game consoles have different proprietary operating systems and other restrictions that present numerous technical hurdles for forensics tool manufacturers; as a result, it is very difficult, if not impossible, to automate a sound forensic examination of these platforms and extract evidence for an investigation. Forensic experts, therefore, are often required to employ manual techniques, such as a scroll analysis through various menus and data storage locations, which can be time consuming and potentially subject to courtroom challenges, if not properly documented.

Fortunately, there are resources available to law enforcement to help combat this rising challenge. These include:

• Training Programs:
  BJA has made available funding for training as part of a broader effort to raise awareness for law enforcement, probation and parole, and other facets of the criminal justice community about crimes in virtual worlds and online gaming communities. BJA has partnered with a company, Drakontas LLC, to provide this training, details for which can be requested via email at training@drakontas.com, or from BJA at www.bja.gov.

• Specialized Technical Assistance:
  BJA funds partner organizations to assist state and local law enforcement with technical challenges associated with cybercrime, in general, as well as with the specific issues described in this document. For more information, contact BJA at www.bja.gov.
• Publications:
Over the coming months, Drakontas will publish more documents that address key policy issues in virtual worlds and online gaming communities. The goal is to build further awareness of the challenges that exist in these digital playgrounds and help to define the best tactics for responding to criminal activities.

The crimes discussed in this document are not new – unfortunately, crimes like child pornography, cyberbullying, online enticement, and identity theft existed long before these new digital playgrounds were built. What is new are the techniques and methods used by criminals in virtual worlds. They are able to take advantage of both technological and social vulnerabilities, and unintended consequences inherent in game play.

This document represents a resource for addressing crime in virtual worlds, the subsequent challenges facing the criminal justice community, and the broad-based response required to stem the tide of this rising criminal threat.

CONTRIBUTORS:
Dr. Brian Regli, Drakontas LLC
Michael Mitkus, Drakontas LLC
Dr. Robert D’Ovidio, Drexel University

Disclaimer
This project was supported by Grant No. 2009-D2-BX-K005 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

ENDNOTES:


CONTACT INFORMATION:
Drakontas LLC
200 Federal Street, Suite 300
Camden, New Jersey 08103
(215) 887-5570
training@drakontas.com

Drakontas (www.drakontas.com) develops mobile collaboration software and provides training and technical assistance that increase the safety and operational capacity of law enforcement, emergency response, and security personnel. The company was founded in partnership with Drexel University in 2004 to transition technologies developed at the Applied Communications and Information Networking (ACIN) Center for the Department of Defense to commercial, civilian and homeland security uses.

ADDITIONAL RESOURCES:
Bureau of Justice Assistance
http://www.bja.gov/

International Association of Chiefs of Police (IACP) Center for Social Media
http://www.iacpsocialmedia.org

Internet Crime Complaint Center (IC3)
http://www.ic3.gov/

National White Collar Crime Center (NW3C)
http://www.nw3c.org/

Regional Computer Forensics Laboratory (RCFL)
http://www.rcfl.gov/
Related Articles:


