

13



unicri
advancing security, serving justice,
building peace



MAX-PLANCK-GESELLSCHAFT

GOVERNANCE
BASEL INSTITUTE ON GOVERNANCE

freedom from fear

www.freedomfromfearmagazine.org

SPECIAL ISSUE

CYBERCRIMES

Looking for Safer Spaces?



**Hackers Profiling:
Who Are the
Attackers?**

Raoul Chiesa



**Terrorist use of
the Internet and
Legal Response**

Marco Gercke
Daniel Thelesklaf



**Cyberwar:
Myth or Reality?**

Bruce Schneier

Award notification

Congratulations your identity has been sold!

*All our lauded technological progress -- our very civilization -
is like the axe in the hand of the pathological criminal.*

(Albert Einstein)

Over the last years we have witnessed changes as we analyzed criminal trends and elaborated new strategies to confront crime. New scenarios have emerged, which have obliged us to improve knowledge and to rethink strategies. These changes are the direct consequences of a wired world driven by global markets where frontiers are abolished mainly in the name of economics. This new world, dominated by new information and communication technologies, has also redefined the criminals' profile and their modus operandi.

Most of the criminal phenomena we are fighting today are transnational. The network woven by organized crime has also become part of our daily life, it has infiltrated the new information and communication technologies (ICT) and, the more we depend on these, the more we are potential victims. ICTs have expanded our possibilities, but they have also enabled a wide spectrum of offences, and the magnitude of these violations can reach impressive levels through the Internet.

Nowadays, security is no longer just an issue in the real world: it is a virtual matter as well. Therefore, trying to be on the safe side today also means having a good firewall, a strong program to detect viruses, avoid answering messages from unknown senders or sharing sensitive information on unprotected channels, and so on.

As it turns out, the likelihood of suffering from a real crime, like being robbed in the street, is actually smaller than the possibility of suffering a virtual crime, such as an on-line identity theft or a credit card fraud. Committing cybercrimes is much more profitable, significantly less risky and strictly linked to market logic and trends. Moreover, many of them no longer require a high level of expertise or sophisticated techniques.

Internet abuses may originate anywhere in the world, no matter where the target happens to be. How we defend ourselves from crime has changed, but we should consider that organized crime is becoming faster and more aggressive in exploiting new technologies and in sharing their know-how with the hacker community.

However, none of us can deny that the impressive changes that information technology has brought to our societies have also allowed for the development of countries and democracies, and for the improvement of people's life standards.

According to the International Telecommunication Union (ITU), in 2009 an estimated 26 percent of the world's population (or 1.7 billion people) were using Internet. This means that one out of four persons

The views and opinions expressed in the Magazine do not necessarily reflect those of the United Nations, UNICRI, and the Max Planck Institute. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the publishing institutions.

Freedom from Fear

www.freedomfromfearmagazine.org

UNICRI
United Nations
Interregional Crime and Justice Research
Institute

Viale Maestri del Lavoro, 10
10127 Turin, Italy

Telephone

(+39) 011 653 71 11

Telefax

(+39) 011 631 33 68

E-Mail

unicri@unicri.it

Web

www.unicri.it

MAX PLANCK INSTITUTE
for Foreign and International Criminal Law
(MPI)

Guenterstalstrasse 73,
79100 Freiburg, Germany

Teleph one

(+49) 761 708 10

Telefax

(+49) 761 7081 294

E-Mail

info@mpicc.de

Web

www.mpicc.de

**BASEL INSTITUTE
ON GOVERNANCE**

Steinenring 60
4052 Basel, Switzerland

Telephone

+41 (0)61 205 55 11

Telefax

+41 (0)61 205 55 19

E-Mail

info@baselgovernance.org

Web

www.baselgovernance.org



has opened a window to the rest of the world: they can avail themselves of the amazing opportunities offered by the Internet, but, at the same time, they can also become a victim of cybercrime.

We can now exchange data, information and know-how from one side of the world to another in just a few seconds. The accessibility of information combined with the fact that all aspects of our life are electronically stored are the two aspects that contribute to our socio-economic development, our possibility to enjoy the freedom of a world simultaneously connected to us, but also to our vulnerability to cybercrime. The Internet breakthrough and its widespread accessibility are the technical factors that have allowed the emergence of cybercrime: phishing, pharming, credit card fraud, identity theft, computer espionage, hacking, the elaboration and diffusion of viruses and worms, just to mention a few, are now part of our common dictionary.

Think about it. One of the articles here included mentions that, considering 1995 as “year 0” (the last year before the Internet boom erupted in many countries), Interpol knew of only 4,000 child abuse images; today it totals around 1,000,000, and the number of children abused to make them runs in the tens of thousands. And this is but one of the many facets of crime in the Internet Era. A bot herder can remotely control thousands of victim computers at once, including yours, and launch a systematic and widespread attack with just the click of a mouse. The UN estimates that identity theft alone can account for around 1.5 million victims, with an estimated annual value of 1 billion USD.

Furthermore, we are speaking about a world that right now is still only partially connected. Africa: is going to be the latest Internet-connected continent, also thanks to the recent FIFA World Cup, which this year has doubled the continent’s Internet links capacities. In a region where the hardware platforms and the operating systems are outdated, security issues, mass-worms and botnets could spread through Africa. This could mean a new wave of targeted attacks that may have a serious impact on African financial institutions and national critical infrastructures, such as oil and gas pipelines.

In this landscape, cybercrime represents a real challenge to governments’ security: militaries have been working for years on issues like cyber espionage and cyber war scenarios, just to mention few. Let’s imagine the consequences of a cyber attack to a crucial infrastructure: the outbreaks of violence, looting, plunder and destruction that occurred during the 1977 blackout in New York would fade in comparison.

From the evolution of cybercrimes, to terrorist use of information technology, to the main offences committed through the Internet, this issue of the Magazine aims to improve our knowledge of phenomena that could potentially affect or are already having an effect on each of us: cybercrime. This issue includes several perspectives on cybercrimes and suggestions to reduce our vulnerability and on how to prevent them.

The fight against cybercrime is not a journey towards the unknown (although it is almost impossible to identify the offenders): it is actually a matter of creating a collective strategy to avoid criminals from taking advantage of the weakest links of the chain (lack of legislation, of technical expertise and statistics, poor coordination across borders and sectors) and to exploit to its utmost the global market opportunities driven by new technologies.

The world we know today is not capable of surviving a collapse of the system of information technology. But, on the other side of the coin, our increased vulnerability should not be neglected.

Doris Buddenberg
UNICRI Officer-in-Charge

Contents



Editorial board

UNICRI

Doris Buddenberg
Kristiina Kangaspunta
Amaury Aubrée-Dauchez
Marina Mazzini

Max-Planck Institute

Hans-Joerg Albrecht
Ulrike Auerbach
Michael Kilchling

Basel Institute on Governance

Daniel Thelesklaf

Editorial team

Olivia Jung
Fatima Zahra Habib Eddine

Proofreading & translation

Olivia Jung

Graphics and layout

Manuela Flamini

Columns

60 Focus on
Cybernetics and Law
Javier Livas

64 Insight
The New Convergence between International
Criminal Law, Nuclear Non-Proliferation
and Maritime Security
Stefano Betti

66 Close up
Reporting in Times of War
Francesca Caferri

68 In the Spotlight
Humankind's: Suffering is Not Something One
Can Get Used to
Laura Boldrini - *Op-ed*

2 That Was then, This Is Now:
A Concise Look Back on the Hacker Subculture
Ioan Landry

4 Hackers Profiling: Who Are the Attackers?
Raoul Chiesa

5 Interview with a Hacker: Chronicles of a Black Hat
Interview conducted by Raoul Chiesa

8 The State of Cybercrimes
Levi Gundert

16 Cyber Crime and Organized Crime
Tatiana Tropina

18 Terrorist Use of the Internet and Legal Response
Marco Gercke, Daniel Thelesklaf

22 Defending Quality of Life through
Critical Infrastructure Protection
Marco Carbonelli, Luisa Franchina, Laura Gratta,
Fabio Guasconi, Daniele Perucchini

26 Online Crimes against Children
John Carr

29 Estimating and Interpreting the Prevalence of E-fraud
across the World
Jan Van Dijk

32 Avoid Becoming a Victim of Cybercrime
Scot Huntsberry

35 From Encryption to Failure of Traditional Investigation
Instruments: the Challenges of Fighting Cybercrime
Marco Gercke

38 Global Cybersecurity Agenda
ITU (International Telecommunication Union)

43 The Internet: Anonymous Forever
Bruce Schneier

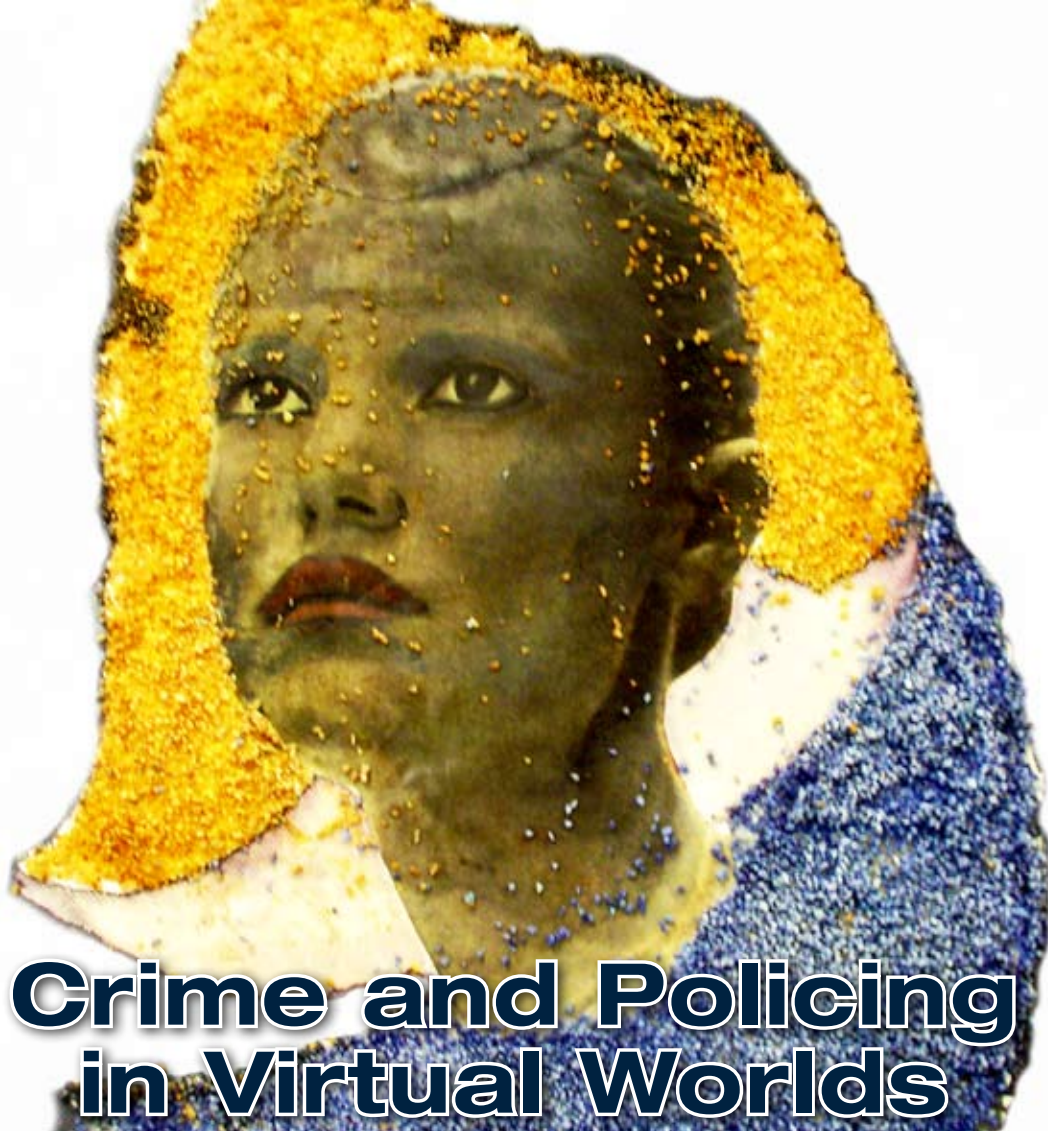
46 Privacy vs. Security? A Dilemma of the Digital Era
Giuseppe Vaciego

49 Cyberwar: Myth or Reality?
Bruce Schneier

52 Crime and Policing in Virtual Worlds:
On the Ever-Evolving Nature of Cybercrime
Marc Goodman

70 On the International Agenda

72 Challenging Ideas for Challenging Times



Crime and Policing in Virtual Worlds

On the Ever-Evolving Nature of Cybercrime

* Marc Goodman

The rapidly changing nature of information and communications technologies suggests that as soon as new hardware, software or other applications are introduced, they will be exploited in some form or fashion by international criminal organisations. The speed at which criminals can exploit these technologies is truly remarkable. Unfortunately, law enforcement and the criminal justice system, bound by limited budgets, finite training, and traditional legal regimes are much slower in their abilities to respond.

Cybercrime has, and will continue, to evolve overtime. From the early days of phone *phreaking* and the hacking of Bulletin Board Systems (BBS's), information technology crime has transformed itself to include a much broader spectrum of criminal activities comprising previously unimagined technical forms of malfeasance, such as computer viruses, worms and Trojans; *hacktivism*, *phishing*, *botnets*, critical information infrastructure attacks and even cyber-terrorism.

Given the significant advances in computer processing power and the growing number of Internet users around the world, it should come as no surprise that newer forms of criminal conduct in cyberspace are surfacing, to include crime and disorder in "virtual worlds" as well.

What are virtual worlds?

The concept of "virtual reality" is new to law enforcement agencies around the world. Yet every day, millions of people connect in these 3-D worlds to socialise, shop and learn. Unfortunately, lawbreakers have also joined these virtual worlds and the full range of criminal activities is now also present. Common "real world" crimes are occurring every day in virtual worlds, including money-laundering, theft of intellectual property, exchange of child abuse images and even suspected terrorist activities. For these reasons, new virtual worlds and communities pose a unique set of challenges for the criminal justice system. Moreover, the near total lack of requisite jurisprudence means that criminals are often free to act with impunity.

Features of Virtual Worlds

Virtual Worlds can often be classified according to their specific features. The most commonly seen types of virtual worlds break down into two general categories: game-playing and community-based, although they often share some characteristics of the other. One of the interesting developments with certain Virtual Worlds is the possibility of transforming gains generated within these online spaces into real world money.

As a result, a whole new breed of entrepreneurs has developed and several “virtual industrialists” have turned virtual world activities into real world profits. Perhaps the most famous of these virtual world entrepreneurs is an individual whose Second Life character is known as Ailin Graef, but in reality is controlled by Chinese national Anshe Chung. Chung created a real estate company within Second Life and as a result became the first “real world” millionaire based solely upon her activities in virtual worlds.²

In short, “virtual worlds” create an alternative reality where users can represent themselves as they wish, in just about any format they desire through their “avatars.” Men can become women, women men, adults may become children and human beings may transform themselves into animals, superheroes or monsters.

Virtual worlds often contain elements common to other types of online activities, such as MMORPGs (Massive Multiplayer Online Role-Playing Games). MMORPG’s are videogames that allow thousands of players to simultaneously enter a virtual world and interact with one another. Players can run their own “cities and countries,” stand up armies to win battles and go on any variety of “quests” with their own avatars. These avatars are completely customizable. Within MMORPG’s participants may communicate with each other through a variety of means, including text chat or real time voice communication, using technologies such as VOIP to carry their messages.

Common Virtual Worlds

There are dozens, if not hundreds, of virtual worlds and MMORPG’s in existence today, with new ones emerging increasingly frequently. Perhaps one of the most popular virtual worlds is Second Life (SL), which was established by Linden Labs in 2003. SL has grown significantly over the past years and has an international reputation as one of the preeminent non-game based virtual reality worlds.

Among MMORPG’s, the World of Warcraft (WoW) is perhaps the most popular worldwide. Players control a character/ avatar within the game world, exploring the landscape, fighting monsters, completing quests and interacting with Non-Player Characters (NPCs) or with other players.

Other common virtual worlds and MMORPG’s include Club Penguin, Lineage II, Habbo, HiPiHi, Runescape, Entropia Universe, Gaia Online and IMVU. The number of users in virtual worlds is impressive, with tens of millions of individuals visiting these spaces every month. Blizzard Entertainment’s World of Warcraft alone has over 11 million active subscribers:³ if WoW were it’s own country, it would be the 75th largest in the world, surpassing Belgium, Portugal, Sweden, Austria and Switzerland in terms of population size.

Psychology of Virtual Worlds

To many that live in the “First World,” the concept of a Second or Virtual World may not make much sense at all. Many criminal justice officials may be asking themselves why individuals would spend so much time in these simulated environments. The answers are complex and are not yet fully understood by psychologists. To many,

virtual worlds offer not just a form of entertainment, but also a means of escapism, a way of creating an alternative environment that is much more attuned to the user’s liking. The fantasy lives permitted via these virtual worlds create almost unlimited opportunities for escapism, starting from the fact that an avatar does not need to have any verisimilitude to how one appears or behaves in real life.

In order for any investigator to understand virtual worlds, the crimes that take place therein, and the suffering of victims of “virtual crimes,” it is critical that the investigator gain insight into the mindset of virtual spaces’ “inhabitants.” Many of them sincerely see their “second lives” as “first lives,” to the extent that, for the more extreme participants (about 20% of MMORPG gamers), the real world (a.k.a. “meatspace”) is nothing more than a secondary home in which to eat and sleep, while the virtual world clearly represents in their minds their first place of residence and interaction.⁴

Until one fully grasps the how real the “reality” in virtual worlds is to its participants, it will be impossible to successfully understand the mindset of both the criminals and the victims who participate in these new virtual communities. Only by understanding this mindset can one begin to comprehend why somebody might show up at their police station to report a virtual rape, a virtual assault, a virtual burglary or a virtual suicide.

Economics

Millions and millions of euros are spent each year in various online virtual worlds. While the idea of a “virtual economy” versus a real world economy might sound strange at first, most virtual worlds allow for some exchange of goods and services, either through bartering systems, or by overcoming various game challenges or through the use of “virtual currency.”

While previously many of these economies were strictly virtual, recently there has been a cross over between virtual worlds’ economies and real world economies. Some virtual worlds actu-

ally have currency exchange rates with real world currencies such as dollars, pounds, RMB and euros. That means it is possible to buy Linden Dollars or Entropian dollars with Swedish krona or Brazilian reals. Often virtual currencies trade with or without authorization in a booming secondary market, which operates without any regulations, opening the door to further criminal opportunities.

Real Crimes in Virtual Worlds

Many police officials, including seasoned and experienced cybercrime investigators, may not have yet investigated a case involving a virtual world or MMORPG. Faced with already overwhelming caseloads from traditional forms of cybercrime, such as hacking, Internet fraud and online child abuse images, few investigators want additional work from virtual cases. That said, we believe that virtual world crimes merit further examination given their inevitable emergency into the daily workload of cybercrime investigators around the world.

While it might be tempting to ignore MMORPG crimes as being purely virtual in nature, and thus not “real,” the vast majority of virtual crimes have real world victims. While one can certainly argue whether “virtual rape” indeed constitutes “real rape,” let there be no doubt about the economic or psychological effect of these crimes on their victims, since these virtual spaces are every bit as real to their inhabitants as is the physical world to most investigators.

Economic Crimes

Given the size of virtual world economies, it should not be surprising that many of the crimes committed in virtual spaces involve financial fraud or other nefarious activities for criminal economic gain. Virtual World economist Edward Castronova has estimated the value of all the goods and services produced in virtual worlds to be between 7-12 billion US dollars per annum. He further noted the economic transfer of at least 1 billion dollars in virtual cur-

rencies per annum as of May 2009.⁵ As such, the virtual economy dwarfs the “real world” economy of dozens of countries around the world.

The proliferation of virtual currencies, such as Linden Dollars, WoW gold, QQ coins and so many others, has created an attractive economic target for international organised crime groups. Long gone are the days where hackers engaged in criminal activities merely for the “fun” or “challenge” of the matter. Modern organised crime seeks first and foremost financial gain and the amount of money in MMORPG’s poses an incredibly enticing target for them and the millions of MMORPG users can become to organised crime a readily accessible victim-base. The emergence of some dominant companies in the MMORPG field, such as Second Life and World of Warcraft, has meant that criminals can now create computer malware and social engineering scams to specifically locate and target large numbers of potential victims.

Financial Frauds

There are several tried and tested ways of committing financial fraud in virtual worlds, including social engineering, exploiting or hacking MMORPG servers and the introduction of malicious computer code into an individual’s virtual world environment.⁶ Social engineering attacks occur when cyber criminals enter an MMORPG or an associated, but independent, gaming forum where they search out users and offer them help or various bonuses to help “improve” their user experience or increase their gaming level. In exchange they solicit user names and passwords so that they can carry out the purported helpful work.

The Role of Malware

These malicious programs or computer Trojans enable a wide variety of criminal activities in MMORPG’s, including the theft of virtual goods and money. The number of malware programs specifically directed at virtual worlds and online gaming has increased dramatically over the past few years. In fact, according to computer security company Kaspersky Laboratories, over 30,000

new malicious programs specifically targeting online games were introduced in 2008.⁷

Money laundering

Over the past decade, a number of new alternative forms of payment have been introduced throughout the world to keep up the growing volume of electronic commerce. The most famous of these companies is PayPal, which became a wholly owned subsidiary of eBay in 2003. PayPal made it easier for payments to be made through the Internet and serves as an electronic alternative to traditional paper money, checks or bank money orders. It can be very useful for the vast majority of the planet’s inhabitants that do have access to a credit card. Of course alternative payment systems also open up the doors to alternative forms of money laundering. While PayPal was certainly revolutionary in its approach, it always settled transactions in well-established forms of national currency, such as dollars, yen or euros. Over the past few years however, a number of virtual worlds have begun to issue their own forms of currency. With names like the Linden Dollar (used by Linden Lab’s Second Life), World of Warcraft Gold (from Blizzard Entertainment) or QQ Coins (by Tencent Limited), these virtual currencies are being used by literally tens of millions of people worldwide. There have been various estimates of the size of the virtual world economy, but some estimates have placed it in the billions of (US) dollars.

Given the vast sums of money being transferred among parties around the world, it should not be surprising of course that criminals would want to take advantage of this money flow. With little if any regulation, virtual world economies are ripe for exploitation by organized crime, terrorists and others who wish to launder large sums of money.

While virtual world money laundering has theoretically been a possibility for some time, the following case clearly shows that theory has now been put into practice, to the tune of \$38 million US dollars. As the Seoul Metropolitan

Police Agency (SMPA) demonstrated, a group of Chinese and Korean criminals were able to successfully defraud Korean game players and then launder the funds through a number of business front companies back in mainland China.

Extortion

In further evidence demonstrating the growing value of virtual world goods, a court in China handed down a 3-year prison sentence in mid-2009 to a known gang member for extorting virtual goods. According to Chinese officials, three suspects cornered the victim in a cyber café and noticed he had a particularly large balance of virtual goods in his QQ-Tencent account. An assault ensued and the victim was forced to turn over the equivalent of nearly 100,000 RMB of the virtual currency QQ coins.⁸ This case is interesting in that it shows that virtual goods must be of value in order for the arrest and prosecution to have occurred. As virtual goods proliferate, more and more individuals could become victims of virtual thefts and extortions.

Possession of Child Abuse Images

By the very nature of their entertainment value, virtual worlds and MMORPGs are attractive to people of all ages, and in particular to young people. The enticing cartoon-like graphics, the gaming potential and the entertainment value all make virtual worlds of interest to a younger audience. Of course this is not to say that children are the only ones using virtual worlds. In fact, across the board, most users in MMORPG's are in the 20's and 30's, but average ages vary greatly from game to game. Second Life tends to draw an older crowd than Disney's Club Penguin for example, which targets children from 6 to 14 years of age.

Many virtual worlds allow for outside connections and communications: text chats, real-time voice over internet protocol (VOIP) conversations, exchanges of photographic and video images with one another. While friends might want to do this for legitimate purposes, there

certainly could be criminal implications as well.

For example, a number of paedophiles could create avatars in Second Life providing false identification details. They could meet each other in various chat rooms/islands dedicated to "child love" or "Lolita" or any other such keyword and begin socializing with each other. One of the paedophiles (represented by his avatar) could readily build a movie theatre on the island of his choice and show whatever streaming video file he chooses. So in effect, it would be entirely possible to have a virtual room full of paedophiles watching real child abuse images (photos, videos, etc) of real children.

Age Play

While few would argue that the exchange of real child abuse images, whether done in person, on IRC (Internet-relay chat) or in a virtual world should be a criminal matter, the depiction of virtual children engaging in sexual activity proves much more difficult. For example, in Second Life, you can choose and dress you avatar as you wish, thus a 56 year old man could inhabit the avatar of a 12 year old girl and could then script that avatar to engage in various sexual activities. To those observing in Second Life, it would look as if the "12 year old girl" was engaging in sexual activities, while in reality it is the older man using the avatar for his own sexual purposes.

Should such activities be a crime? Across the world, government legislatures are answering this question differently. In Germany, Ireland and many other European countries the possession of "virtual child pornography" is considered the legal equivalent of possessing "real" child pornography and is equally punishable by law. In the United States the courts have ruled that "virtual" child sex depictions are a form of fantasy and, as such, they do not constitute criminal behaviour because no actual child was ever abused or photographed in the production of those virtual child abuse images. Others have argued that only somebody predisposed to abusing a real world child would want to act

out sexually as a virtual child. Those in opposition responded that democratic societies should not have "thought police" and that a fantasy life that does not cross the threshold into harming others should not be criminalized.

One of the largest and most infamous cases of age play occurred in Second Life in an area known as "Wonderland." There, young "children" avatars were offering sex in a playground environment. The young children were in this context not real children, but graphical representations, the so-called avatars, and the playground was a virtual playground created with computer software. The case created a strong rebuke from law enforcement authorities and prosecutors in Germany opened a criminal case in the matter. Another such case was investigated by the British police.

Rape/Sexual Assault

Perhaps no other form of virtual world crime endangers quite as much passion amongst participants as the discussion of "virtual rape." To some, it is very much a crime as "real" world rape. Doubters dismiss the possibility outright, noting that rape is impossible without a human victim who has been physically attacked or violated. Despite the differences, more and more police agencies around the world are having victims of these types of crimes present themselves and demanding police redress.

A "virtual rape" occurs when one person's avatar is forced into a sexual situation against his/her desire. To be clear, this type of crime is different from consenting adults acting out a fantasy version of rape for whatever reasons. Virtual world rape is alleged when one of the participants is an unwilling participant in the act. Graphics in MMORPG's and virtual worlds have progressed enormously, to the point that they can accurately represent real world scenarios fairly well. As such, an involuntary sexual assault could be perceived as having verisimilitude to the actual real world act. While many virtual worlds such as Second Life have built-in technical protections to prevent such activities from occurring, they can occur elsewhere through the introduc-

tion of malicious code that forces an avatar to do something against its will. Again a review of the psychology of virtual worlds is critical here. To an individual who spends 12 hours a day inside a MMORPG living through their avatar, any activity that occurs to that avatar against its owner's will can be troubling. For some seeing one's avatar undergo a graphic representation of a violent sexual attack clearly would have a negative impact to the psyche of the avatar's owner. Whether this harm is as serious as a "real world rape" is very much debated openly and is beyond the scope of this report. That said, many such cases are occurring and are being reported to law enforcement around the world.

In Belgium recently, federal prosecutors asked the Belgian Federal Computer Crime Unit to travel to the scene of a crime in Second Life for the purpose of investigating a "virtual rape" involving a Belgian victim.⁹ This type of activity has been around for a very long period of time. The first most widely reported case of virtual rape was documented in 1993, long before today's MMORPG's existed.

Despite how police may or may not feel about such cases, one thing is certain, they will be increasingly reported to police. As such, law enforcement should have a plan in place to deal with them and to secure any potential crime scene in search of evidence of criminal activity.

Stalking/Griefing

One of the most common complaints and potential criminal activities in virtual worlds/MMORPG's is that of harassment, intimidation or stalking. This often occurs when an individual becomes the subject of unwanted attention or focus by another person (avatar) or group of them. In virtual worlds, this type of activity is commonly referred to as "griefing."

Perhaps it is not surprising that all the petty grievances, insults, arguments and disorders that occur in the "real world" also occur in "virtual world" spaces. A griever is not playing an online game or inhabiting an MMORPG for any useful purpose, except to harass or intimidate

others. They may have uncovered undocumented technical aspects of the virtual world software and exploit these glitches or features to purely harass other players or inhabitants. For those victimized by such behaviour, it can be extremely annoying and it could feel like the real world equivalent of stalking or harassment.

Prostitution

Prostitution is certainly common in virtual worlds and MMORPGs, but one must be careful about how one defines the term. Some individuals are willing to pay for their avatar to engage in simulated sexual conduct with another avatar for money (virtual currency or real). While this may or may not violate the terms of service of the virtual world itself, it would not be a criminal offense in many jurisdictions, assuming all parties were consenting adults. In other jurisdictions, even simulated sexual contact in exchange for money would be criminal.

While most police forces might not pursue strictly virtual prostitution between adults (especially when all activities were purely online within the MMORPG), there are many overlapping technologies that can make this type of activity a hybrid cross between the virtual and the real. For example, many virtual worlds allow users to incorporate VOIP communication into the MMORPG environment. Thus the addition of voice communication as part of the prostitution scenario might further push the boundaries of what is legal in some jurisdiction.

In other cases, pure acts of prostitution in the real world have taken on a virtual world component. In one of the most famous cases known as the "Epic Mount" case, a woman offered sexual encounters in the real world in exchange for money: 5,000 pieces of World of Warcraft gold. The woman claimed she needed the money to purchase her "epic flying mount." Since WoW gold can be exchanged for real world currency (euros, dollars or yen) it has a real world value based on market conditions, and given the exchange of said currency for a real-world sexual

act, that woman could be punishable in many jurisdictions.

Riots/Public Disorder

Though it might seem odd to talk about riots or public disorder issues in virtual worlds, they are in fact, not that uncommon. For example, during the most recent round of elections in Spain, most politicians had established a virtual presence in Second Life. Some politicians had even established their own avatars, which in turn campaigned, held rallies and put up election posters in virtual spaces. While things worked well for a while, politicians from one party were quickly overwhelmed with grieving by opposition supporters.

This is of course not the first time such a thing has happened. During a recent political rally by a far-right French politician, his posters were defaced, he had "exploding virtual pigs" hurled at him and Nazi swastikas were painted on campaign headquarters.¹⁰

Surely when incidents as these occur, especially when they involve high-level politicians, law enforcement will be contacted. Whether or not police are able to respond to such matters under national law is another question. The fact is, however, that the public will increasingly expect their police service to handle incidents such as these.





Conclusions

The evolving nature of modern science portends that as new information and communications technology tools are introduced, so too will criminal exploits for these technologies. The aforementioned focus on virtual world crime was provided to highlight how a simple new technology can be utilized by criminals to commit a wide variety of offenses. As has been noted, almost any crime that can occur in the real world can also be committed in virtual spaces. From child abuse to terrorist attacks, police will increasingly encounter a plethora of offences in virtual spaces. In order to keep these virtual spaces safe and crime free, criminal justice professions should continue to work with industry and academia to ensure the greatest possible cooperation in trying to minimise any

social harm resulting from these technological developments. The size of the financial gain to be made by modern criminals will ensure that virtual worlds continue to be targeted for illicit purposes. Moreover, as human social interactions increasingly migrate from “real space” to virtual space, so too will the panoply of social ills and harms. Given the complexity of the issues involved, now is the time to begin thinking about and responding to these concerns before the virtual crime wave spills over into the real world.

* **Marc Goodman** is a visiting researcher at the University College Dublin's Centre for Cybercrime Investigation. He also serves as a Senior Advisor to Interpol's Steering Committee on Information Technology Crime, where he chairs the organisation's working group on Next Generation Cyber Threats.

- 1 A virtual world is a type of online community that often takes the form of a computer-based simulated environment, through which users can interact with one another and use and create objects, often in 3D virtual environments. In virtual worlds, users often take the form of avatars visible to others as graphical representation of the users.
- 2 According to: www.el-universal.com.mx/articulos/36445.html. See also Business Week Magazine's feature article on Chung: http://www.businessweek.com/magazine/content/06_18/b3982001.htm
- 3 http://en.wikipedia.org/wiki/World_of_Warcraft
- 4 <http://motherjones.com/politics/2007/05/even-better-real-thing>
- 5 <http://edition.cnn.com/2009/TECH/05/19/online.currency/index.html>
- 6 For a good overview of fraud in online gaming environments, see the white paper by Kaspersky Labs entitled “Online games and fraud: a source of easy money,” available at: http://www.kaspersky.com/au/reading_room?chapter=207716493
- 7 http://www.kaspersky.com/au/reading_room?chapter=207716493
- 8 <http://www.virtualgoodsnews.com/2009/05/chinese-man-faces-three-year-sentence-for-virtual-currency-extortion.html>
- 9 Source: <http://virtuallyblind.com/2007/04/24/open-roundtable-allegations-of-virtual-rape-bring-belgian-police-to-second-life/>
- 10 <http://www.guardian.co.uk/technology/2007/jan/20/news.france>

A NEW AND ADDICTIVE DRUG



CORRUPTION

The phenomenon of corruption has always existed, nonetheless it is only in recent years that **awareness of it has grown at the international level.**

Corruption is a phenomenon that is not limited by politics or geography. It exists in rich countries and in poor countries.

The economic impact of corruption is difficult to establish with precision; in fact, **available data is often inconsistent.**

On the international level, the fight against corruption requires that **people work together** to increase transparency in economic and financial transactions and to enact within different countries **uniform legislation in this area.**



The European Law Students' Association

INTERNATIONAL LEGAL RESEARCH GROUP

Call for Applicants

Applications are invited from all ELSA members, coming from the Mediterranean Countries, whether new or experienced.

However, you will need to show evidence of commitment to the values and goals of ELSA.

Applicants must also have sufficient knowledge and interest in the topic, but no specific area of Law is privileged, as the corruption phenomenon can involve any legal field.

Evidence of previous dissertations or researches will also help your application.

Participants are expected to work on the issue from December 2010 to July 2011.

They will need regular access to e-mail and the internet; it is advised to keep a good communication flow, exchanging emails on a regular basis.

REGISTRATION DEADLINE: 20TH NOVEMBER 2010
Fill in the Application Form (www.elsa.org)

Send it to your Local VP AA

For further information:

preventcorruption@elsa.org & www.elsa.org



unieri

advancing security, serving justice,
building peace

Would you risk
such a bloody trip?



Total Cost*

€ 60.000 debt to be repaid to the traveller's smuggler

€ 20.000: value of the fake passport

€ 5.000 per month: value of the confiscated 'salary'

* The Carrier declines any liability for death or injury during the desert crossing or any part of the trip.

We are all citizens of the same World
Please stand up for justice and equality

United Nations Campus in Turin
November 2010 - July 2011



Università degli Studi di Torino
Faculty of Law



unicri

advancing security, serving justice,
building peace

Master of Laws (LL.M.) in International Crime and Justice

Areas of Study

- Activities and policies of the United Nations and the international tribunals
- Transnational organised crime, emerging crimes and terrorism
- Crimes against humanity, genocide and war crimes
- International Criminal Law

Programme Details

- Integration of theory and practice: lectures, seminars, mock trial, practical exercises and up-to-date analysis of United Nations activities
- Lecturers composed of international experts of theory and practice
- Programme intended for:
 - University Graduates in Law, Political Science, International Relations, Criminology, or equivalent disciplines
 - Young professionals in governmental institutions, local authorities, international organisations or NGOs seeking to specialise in international criminal justice
- Course taught in English
- Lectures held at the United Nations Campus in Turin, Italy

LL.M. Certificate

- Upon successful completion of the programme, students are awarded an LL.M. degree from the University of Turin, Faculty of Law (60 ECTS)



For further information, please contact:
Tel: +39 011 6537 111 - Fax: +39 011 6313 368
E-mail: llm@unicri.it

Application Deadline: 23 AUGUST 2010
www.unicri.it



MAX-PLANCK-GESELLSCHAFT

Max Planck Institute for Foreign and International Criminal Law

Department of Criminology

Director: Prof. Dr. Dr. h.c. Hans-Joerg Albrecht
hjalbrecht@mpicc.de

Additional contacts:
Dr. Michael Kilchling
m.kilchling@mpicc.de
Ulrike Auerbach
u.auerbach@mpicc.de

Postal address: Guenterstr. 73, D - 79100 Freiburg, Germany
Telephone: +49-761-7081-0

For further information please visit our website at www.mpicc.de