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

Looking for Safer Spaces?
GOVERNANCE
BASIL INSTITUTE ON GOVERNANCE

Asset Recovery EXPERTS NETWORK

Get connected*

AREN is a service of the International Centre for Asset Recovery (ICAR). The ICAR provides training and technical assistance to developing countries to build their capacity in investigating corruption cases to identify, trace and repatriate stolen assets. ICAR is part of the Basel Institute on Governance, an independent and non-profit institute founded 2003 in Basel, Switzerland

Connect with Asset Recovery professionals

AREN is a special interest community focussing on Asset Recovery. Connect with asset recovery practitioners around the world, find experts in the various fields of the asset recovery process and get access to exclusive expertise.

Create, upload and share content

Create your own content using AREN and share it with other users. Upload and share photos, videos and documents of conference talks, panels, meetings, trainings, etc. Share websites with other members of AREN and see the favourite websites of other users.

Create your own groups

Create your own groups and invite people to join them. Put documents in your group’s workspace, share photos, videos and websites. Use the group’s bulletin board to discuss with other members of the group.

Join now:
http://aren.assetrecovery.org

* The Asset Recovery Experts Network (AREN) is an informal online forum for professionals, who are involved in processes of recovering stolen assets, to connect, network, communicate and exchange information, at all times, on issues associated and related to asset recovery.
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...
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

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 Vaciago

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
There is no argument that since the Internet’s widespread commercialization roughly twenty years ago, it has exponentially improved, automated and streamlined much of our lifestyle with every passing year. The advantages of living in a wired (or, wireless) world are apparent, but not without risks: the media is rife with speculation on hackers and every week a new phishing ring is busted or a massive data breach is reported. But who are these much-maligned hackers, and where do they come from?

The Hacker Profiling Project has successfully identified the generations of the hacker subculture, but we are going to focus here on the tentative links between criminal or “cybercriminal” links to this world. An understanding of what is unique or overlapping in each of them is crucial to understand where we are headed, and why criminal elements are going digital.

The first generation of hacking - comprising the 1960 all the way to the 1980s - was very much academic, with students at universities putting together various programs for the new mainframes being installed on campus, as well as early forays into the telephony system. The ethics of this era focused on shared ownership of data and information, as well as promoting the contribution of all those involved in the hacker culture.

The second “hacker era” characterizing the early ‘80s, was driven by curiosity, and the motivation to hack into external targets was often driven by the scarcity of technology: the mainframes and the unique operating systems running on them would cost vast sums of money and technology was not yet a common utility: even a PC was beyond reach for many, and dialling into modems half-way across the globe could result in exorbitant monthly phone bills.

The next wave of hacking covers a larger timeframe - from 1985 until the mid to late ‘90s - and was a very active period, especially with the commoditization of the Internet in the later half. This was an extremely prolific period for the culture and many “hacker periodicals,” such as 2600 (1984) and Phrack (1985), began their publication in these years. The motives of hackers from this era were as eclectic as their geographical distribution and background, but even in this period there were very few economically motivated black-hat-hackers. Interestingly, the diffusion of “crimeware” and increases in frauds both rose as the ‘90s progressed, leading us to the next era of hacking.

The current wave of hacking is just as convoluted as the previous, but it is marked by a worrying trend: the monetization of hacking. In the past couple of decades, there has been a shift from hobbyist hacking primarily driven by ego and “the thrill of the chase” to malicious and financially motivated crime conducted over the Internet. One only needs to research the stark contrast between the early hacker crew known as L0pht Heavy Industries (1992-2000) and the recent cases of the Russian Business Network (RBN), Innovative Marketing Ukraine, or the Shadowcrew fraudster forums (2002-2004) to see the devolution of ethics and ideals in the hacker subculture.

The “infiltration” or usurpation of hobbyist hacking by outright criminal elements is a relatively recent phenomenon, but one all too natural given the open-nature and naivety of the subculture, as well as the adoption en masse of the Internet for key sectors such as finance or the management of PII (Personally Identifiable Information). In fact, some early hackers were prophetic enough to predict a hijacking of their beloved lifestyle by organized crime or loosely affiliated criminal bands.

But when did we reach the threshold or boiling point, which led to the rise in financially motivated attacks launched over the Internet? It is difficult to say exactly when online criminals organized themselves for profit-driven attacks, but we began spotting large-scale attacks against financial institutions and gambling websites just before the turn of the Millennium. Not coincidentally, this is also the same period when so-called “crimeware” became marketable among the cybercriminal underground. These kits are sold to aspiring black-hats to automate and streamline their criminal operations, allowing them to work with corporate-like efficiency.
The purpose of distinguishing between the modes and motives of hackers throughout the years is not to whitewash the second and third abovementioned waves of hacking as purely innocent or without consequence: crimes were in fact being committed, and even as early as 1991 there were cases of individuals peripherally related to the then-booming hacker scene being investigated and arrested for toll fraud or “carding” (using stolen credit card information to purchase items or services). However, even a cursory glance at the literature and archived timelines of those days would show us that the majority of the players involved tended to be uniform in their disdain of the outright criminal elements in their midst, such as virus writers and carders.

However, even today the monetization of hacking is being pursued by small, flexible and tight-knit criminal bands which, despite their size, have a considerable impact on the online ecosphere: an Anti-Phishing Working Group report states that 66% of all phishing attacks in the second half of 2009 were perpetrated by a single group known as “Avalanche.” The only good news one could possibly extrapolate from this statistic would be that the skilled criminal groups operating online are perhaps less numerous than previously anticipated, but, as always, there is no lack of “script kiddies” and newcomers to the “underground economy” waiting for their turn at the table.

And where are the black-hat hackers going now? Wherever the money is. It is no secret that since the dawn of civilization criminals have sought out the “low-hanging fruit,” and we have already seen them shift away from targeted attacks on financial institutions or e-commerce with server-side attacks, to phishing scams and particularly virulent blended threats targeting end-users and consumers who don’t have the luxury of an annual security budget ranging in the millions of dollars.

We speculate that the prime target will remain the end-user for the near future, with an increase in sophisticated XSS (Cross-Site Scripting) attacks targeting social networking sites and a constant focus on subverting the web browser. An example of this, offering a glimpse of the next generation of phishing attacks, would be the devious tabnabbing exploit: it subverts an open, idle and otherwise innocent browser tab to redirect itself to a hostile page of the attacker’s choice once the user’s attention is elsewhere, fooling the user into providing sensitive data in the fraudulent page (i.e. a spoof page of Gmail or Facebook asking for log-in and password).

As always, there is no technological or legislative “silver-bullet” solution to tackling the increase in cybercrime: these criminals conducting online abuses and frauds have already shown their capacity to defeat IT security measures, and an indifference to national or international laws focusing on them. As long as their activities remain profitable the miscreants will continue, and as long as technology advances they will keep on adapting.

<table>
<thead>
<tr>
<th>THEN</th>
<th>NOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>L0pht Heavy Industries was the original “hacker think tank.” They initially supported themselves by selling used hardware at local flea markets, offering UNIX shell accounts and archives of files and texts. They eventually created the famous password recovery suite “L0phtCrack,” and they offered their skills as developers of secure code to the corporate sector. The origin of the name, pronounced “loft,” most likely relates to the fact that many members shared a common apartment in Boston. After years of unique contributions to the hacker subculture (and years of barely breaking even), L0pht merged with security firm @stake in 2000, which was subsequently purchased by Symantec in 2004.</td>
<td>The RBN, or was, based in Saint Petersburg (Russia) and operated as a host or Internet Service Provider for illicit services such as child pornography, malware distribution, etc. Their 2006-2007 revenue is estimated at $150 million. Their main areas of criminal activities include spam (estimated to have been actively involved with up to 50% of worldwide spam distribution at their height), malware, phishing scams (estimated to have been behind up to 50% of phishing spams throughout 2007), all the while providing hosting services for other criminal activities, such as the dissemination of child pornography, identity theft, credit card fraud, etc. The RBN is alleged to have dispersed (but not suspended) its activities as of 2008, due to increasing attention from international security vendors, media, and law enforcement.</td>
</tr>
</tbody>
</table>

* Ioan Landry is a UNICRI consultant on cybercrimes.
Who is attacking you? “We don’t know…”

When talking about attackers and hacking it often happens that I ask people working at customer’s sites “who is scaring you?” Most of the time the answer I hear is not “Well, you know... I’m scared by script kids, playing with those couple of unpatched machines I have,” nor is it “I’m really scared about industrial spies.” Rather, 98% of the time the answer is “I don’t know.”

The hacking world has changed dramatically in the last 30 years, and the somehow “romantic” figure of the hacker of the ‘80s is far from today’s.

These answers possibly mean that the company, feeling as a potential target, has not developed a proper IT Security Risk Analysis, while trying to figure out who may want to attack its IT infrastructure and gain access to its information.

This mistake probably happens because every time people hear “hackers profiling,” the word “profiling” automatically makes them think about something that has already happened, rather than something that may happen.

The hacking world has changed dramatically in the last thirty years, and the somehow “romantic” figure of the hacker of the ‘80s is far from today’s.

At the very beginning, “hackers” were computer researchers in places like MIT and Berkley; they wore long, white lab coats and gloves while working in big aseptic data rooms.
1. How you would define yourself with respect to the hacking activities you are conducting?
I’m a Black Hat. This means that hacking is my job and gives me salary. I run black-ops for those hiring me. I’m quite expensive.

2. How did you learn hacking techniques?
Mainly at school. At the University we also used to have a couple of cybercafés at the very beginning (around 1999-2000), which is basically where most of us started.

3. What led you to become a hacker?
I’d say it was a mix of friends and free time. I was a teenager hanging out at that cybercafé and... everything began there, ya know. I was impressed by the things those guys were doing, I just fell in love with hacking... it was that much easier to accomplish goals, hacking into servers, stealing information, pictures... a lot of fun. Then I went into other things, meaning money.

4. What were/are your aims?
Right now it’s just money. People can hire me, I do the job, get the money, and disappear.

5. Have your motivations for hacking ever changed over time?
I would say yes. At the very beginning it was all about curiosity and learning. Then I decided to step forward into the real world, where people pay you money because they don’t know how to play as I do.

6. Are you part of a group or do you act alone?
I was initially part of a group. Then some people left, others stayed, although they lacked real skills; in the meanwhile I grew up and updated myself. That’s why right now I’m working mainly alone. I may buy 0day from some friends, but I prefer to run all jobs alone.

7. What criminal offenses have you committed with a computer?
I guess they would include gaining unauthorized access to computer systems and networks; stealing accounts, personal information, and selling them out. And I guess also industrial espionage and money laundering.

8. Have you ever been arrested or convicted for computer crimes?
No.

9. Have laws and penalties against cybercrimes had a deterrent effect on you?
Sort of... but I’ve decided to take the risk.

10. Have technical difficulties encountered when penetrating a system represented a deterrent or a challenge?
They are basically a challenge. Whenever the target can’t be hacked well... ya know, there’s plenty of other targets out there :)

11. What is your main aspiration?
Stop working in 2 or 3 years, retiring, giving money to my family, buy my own house.

12. Can you describe the impact and results of the hacking activities you have conducted?
I don’t understand the question.

13. Have you ever considered the negative effects of your hacking activities on people?
Are you talking about identity theft and this kind of things? Yes I did consider the effects, but... it’s not my fault if the victim is an idiot, I’m sorry.

Interview conducted by Raoul Chiesa in coordination with the UNICRI Management and External Relations team.
Hacking used to mean “building something” while thinking outside the box, in a different manner, applying new views and problem-solving approaches.

The reason why the hacking phenomenon spread at the beginning of the ‘80s is simple: because of the business. Companies went on the market with the very first home computers, models like Commodore VIC-20 and C-64 or Sinclair ZX-Spectrum, and with the grandparents of today’s Internet routers, the “modems,” running as slow as 300 baud-bits per second!

It was the beginning of the second hacker’s generation, and the most known to the public too. It is not by chance that the general cliché image of a hacker that most people have in mind is that of a teenager, sitting at his desk in his room, typing at the keyboard of his PC, sending commands to the other side of the world... In reality, those kids who were hacking in the ‘80s are probably your IT Security Managers today, and the world of hacking has been replenished with different players. Most of these new players may attack the same targets, but their motivations and goals will probably differ from each others, and substantially so.

The Hackers Profiling Project (HPP) started in 2004 at UNICRI to answer these and many other questions.

Applying the same approach used above, when analyzing the digital evidences left from the attacker on a computer system (meaning, while running a Digital Forensics analysis) we may ask ourselves what the overall goals of the attacker were and why he/she would run that kind of attack on our machine.

The Hackers Profiling Project (HPP) started in 2004 at UNICRI to answer these and many other questions. And, even if we do not have all the answers yet (since the project is still on-going), we can nonetheless surely address the question raised above: who are the attackers?

As a matter of fact, the HPP research team has been able to identify nine different main categories of attackers. We use the word “attacker” and not “hacker” simply because the evolution of the hacking world and of cybercrime itself has merged together different actors, who do not always belong to the category of “hackers” in a strict sense, at least as we were used to know.

The 9 main attacker categories

Wannabe (Lamer)

The “wannabe,” often labelled a “lamer,” is the “I would love to be a hacker” kind. They use hacker techniques without neither knowing nor having the curiosity to learn how they actually function. They use “hacker toolkits,” which can be downloaded for free from Internet; these toolkits automate processes otherwise made manually and in a “creative” way by more experienced hackers (and that often include mistakes and backdoors). They post a huge amount of messages on forums and BBSs (Bulletin Board Systems), asking other hackers to teach them how to become a real hacker. They want to learn to be hacker without really being one, and often their actions result in huge damages to some computer system or network.

Script kiddie

The “script kid” term stands for “the boy from the scripts,” meaning those hackers relying on UNIX/Linux shell scripts written by others. They lack technical skills and sophistication, and the ones least capable are called “point-and-clickers,” since their attacks are called “point-and-click attacks.” They are interested only in the result and not in learning how computer and hacking techniques work. They simply download from Internet (or from the “crews” they belong to) software and hacker tools, and follow the related instructions. A very good example of this profile was “Mafia Boy”, a 14 years-old kid arrested on Montreal, Canada, after running DDoS (Distributed Denial-of-Service) attacks to e-Bay, Amazon, Yahoo! back in 2000.

Cracker

The term “cracker” was created around the beginning of the ‘90s, when the hacker community wanted to somehow differentiate the malicious (or lame) actions highlighted by the media, from the serious hacker research done by many underground groups such as CCC, Loph, THC and so on.

Generally speaking, crackers have good technical skills, which allow them to pursue their purposes; in the last years, nevertheless, due to the different players in the cybercrime arena (particularly when referring to skimming and phishing activities), we have also found crackers with poor or average technical background and field skills. Note also that they are different from the so called “software crackers” who crack software protection to reproduce it illegally (a.k.a. software cracking): this was something very in vogue back in the ‘90s, and it is still employed in many Asian and African countries.

Ethical Hacker

“Ethical hacker” is not just a term, but it designates an entire debate both in the underground community and in the information security market. An ethical hacker is somebody with excellent hacking skills, whose “past life” may have been with the bad or with the good guys, who decides to help the community, digging with software and discovering bugs and mistakes in widely (or poorly) used IT infrastructures (i.e. social networks), protocols or applications.

They are creative hackers, since they try not to use software created by others and they prefer creating it by themselves (scripts, exploits and/or 0-days) or improving it when there are no useful programmes for their attacks. They would prefer a manual attack rather than an automated one, and this is something to carefully note and a rule to apply to your IDS (Intrusion Detection System)! Ethical hackers are also highly sophisticated and specialised in different operating systems, networks and attack techniques: this means they can range from Sun Solaris, HP/UX or OpenVMS to Microsoft Windows.
QPS (Quiet, Paranoid, Skilled Hacker)

If this type of attacker are on a system, and if they have just a remote feeling that they may be caught, they will disappear. This kind of hackers attack IT systems not because they are looking for information, but perhaps because they just love that particular release of HP/UX that one is running, or loves a SS7 backbone.

The QPS are creative hackers, using as little as possible software made by others, since they prefer creating them by themselves. They are similar to Ethical hackers on a lot of issues.

Cyber-warrior/Mercenary

This is one of those categories that appeared in the last few years because of Internet’s globalization and of the “hacktivism” phenomenon. Cyber-warriors feel like heroes from their own environment (i.e. an extremist group with political or religious background). Their skills may vary substantially, from basic ones of a script kid to good or excellent ones, especially when specialized on focused areas (i.e. DDoS, or Web Defacing, or Wi-Fi).

Not being “exposed” in the business environment like the Industrial Spy profile, the Mercenary hacker works on commission, getting money to attack specific targets. A lot of the well-known Russian mobs (such as the RBN, the Russian Business Network) use this kind of elements to support their illegal activities.

Industrial Spy Hacker

The practice of industrial espionage had existed as long as business itself, infiltrating spies in companies throughout the years, and walking out of them with information stored on paper files, microfilms, floppy disks, cd-roms and, today, USB keys or emails.

Nevertheless, the recent scandals of industrial espionage that have emerged in the last years surely involve Industrial Spy Hackers, which modernized this practice taking advantage of the new opportunities brought in by Information technology.

Government Agent Hacker

Nowadays the existing information technology and the granularity itself of information allow external attackers from governments to run highly-sophisticated attacks, specifically focused towards nations’ know-how in different business markets.

Military Hacker

When the HPP research team introduced this kind of profile back in 2004, the reactions we received were doubtful: it appeared we had gone “too far.” Unfortunately, history seems to confirm our assumptions, given the latest waves of “information warfare” highlighted in the newspapers from all over the world.

This profile is also often associated with the term “state-sponsored attack,” which effectively represents the logic and the approach behind those attacks run by Military hackers.

Conclusions

While this list of profiles is not to be considered a complete one or a golden rule to follow blindly, it is nevertheless a very good first step. In order to apply it to your own company or institution’s environment, keep these profiles in mind when trying to figure out the W4s: Who, Where, Why, When.

In order to apply it to your own company or institution’s environment, keep these profiles in mind when trying to figure out the W4s: Who, Where, Why, When.
your computer may be "pwned." While you're reading this article a miscreant might be virtually peering over your shoulder, or worse. Then again, perhaps you follow best practices for securing your computer: you patch your operating system, you maintain a current anti-virus software subscription, and your Web surfing habits are fastidiously cautious. Unfortunately your computer may still be pwned. Depending on whom you ask, approximately 1.8 billion people are connected to the Internet. Team Cymru conservatively estimates that over 5 million unique computers are compromised at any given time. In dispensing with the FUD (Fear, Uncertainty, and Doubt) that often plagues the cyber security industry, the realistic global compromise rate is approximately 0.003%. An issue that plagues less than 1% of the world's computers may not appear to be an issue at all, but context is everything. When a new worm begins spreading, the cost of repairing millions of computers and interruptions to business can be staggering. When bank accounts are drained and e-mail accounts compromised, the victim is often left feeling helpless. When mothers are social engineered out of their life savings by a faceless criminal thousands of miles away, all of a sudden the impact of technology used for malevolent purposes becomes important. When a network responsible for processing 100 million debit/credit cards daily is breached, or the control systems for a city's electric grid are disabled the fallout is beyond unpleasant.

Over the past decade cybercrime has continuously evolved, motivated by profit, ideology, and nationalism. The Internet has enabled criminals to ply their trade in new and innovative ways. The physical elements of crime have been replaced by digital trails that are becoming increasingly difficult for law enforcement to follow. Attribution for cybercrime is rare, and prosecution is even rarer. Yet, the fight continues as investigators work harder toward criminal attribution. In this article, Team Cymru explores the nuances of today's most insidious cybercrimes.
The Underground Economy

The term “Underground Economy” has historically been used to denote business that occurs outside of regulatory channels. Around the turn of the 21st century, Team Cymru adapted the term to the cyber locations and individuals who buy, sell, and trade criminal goods and services. Today the Underground Economy can be found in IRC\(^2\) networks, HTTP forums (web boards), various Instant Messaging services, and any other communications platform that lends itself to anonymous collaboration.

Today, the publicly available Underground Economy is a shell of its former self. The undercover operations targeting and subsequently arresting criminals involved in web forums like Shadow Crew,\(^7\) Carders Market,\(^8\) and Dark Market\(^9\) have pushed the fraud trade further underground.

The Underground Economy is comprised of criminals who typically specialize in a specific criminal commodity. A few of the more common commodities include credit/debit cards, personal identities, hacked servers, hacked network equipment, malware (malicious code), Internet vulnerability scanners, e-mail spam lists, fictitious identification documents, and fraudulent money movement services.

Like any economy, this one involves various strata of criminal proficiency and experience. Participation in the Underground Economy requires only minimal technical ability, and many criminals’ strategy is to defraud other criminals. The higher levels of the Underground Economy involve technically talented actors who work with other criminals through private communication methods often involving encryption. The public criminal market place is contracting, but the criminal activity itself is increasing in both volume and sophistication.

The Underground Economy is comprised of criminals who typically specialize in a specific criminal commodity

Scareware/“Fake Anti-Virus”

One of the latest trends in cybercrime profiteering involves “scareware,” also known as fake anti-virus software. The scam is maximized during a global event, such as the recent earthquake in Haiti. Criminals understand that a large event such as Haiti creates millions of queries on popular search engines like Google. Savvy criminals research key words linked to the event in question and then use those terms to create a new website in search of information related to the global event in question. Once the public accesses the website, a message is displayed informing the user that his/her computer is infected with malicious code. The webpage encourages the user to download an application that will clean the current infection and also locate additional malicious code that may be residing on the victim’s computer. Before this theoretical activity occurs, the program solicits credit card information. Typically the price for this scareware is twice what legitimate anti-virus companies charge for their product. The victim’s credit card is then charged and the user is left with a piece of software that is deliberately spurious at worst, and marginally legitimate at best. Either way, the victim is scared into believing a threat exists and the fraudster’s software package is the only way to resolve the issue.
Phishing is the digital representation of social engineering tactics. The ploy involves tricking Internet users into providing confidential information, believing that the website requesting the information is legitimate. In fact, these Phishing sites are cleverly designed forgeries. The sophistication of these attacks continues to increase and the line between malware and phishing is blurring.

One of the largest criminal platforms for phishing and spam has been labelled by anti-virus software companies as “Avalanche.” It is believed that Avalanche is operated by a group of miscreants who run their criminal enterprise like any legitimate software company. Avalanche uses a technology that is specifically known in the security community as a “fast flux botnet.” The botnet is large and compromised of geographically diverse “zombies” (infected computers). The botnet also possesses powerful functionality (known as “fast flux”) that allows phishing websites to avoid take down efforts much longer by constantly migrating the website’s address to a different zombie in the botnet. The Avalanche owners generate revenue by leasing their expansive botnet platform to criminal customers for a wide array of wickedness. The flexibility of this particular botnet ensures owner attribution efforts are especially difficult. Phishing has given birth to Pharming and Smishing.

Phishing typically involves changing the internal settings on a victim’s computer thereby bypassing a victim’s legitimate address query functionality. For example, a victim may open a web browser and request hsbc.com. The website loads and while the page appears to be hsbc.com, it is in fact a Phishing site. The user is seamlessly delivered to a spurious website because the victim computer’s internal settings were changed to redirect specific website requests to malicious websites that appear legitimate.

Smishing is Phishing across mobile phones. Smishing involves spamming SMS (mobile phone text messages) messages to a large pool of mobile phone numbers with a social engineering message and a corresponding website link to visit. Fortunately consumers appear to be much more wary of unknown mobile phone message senders vs. unknown e-mail senders. If mobile phone identity becomes a future challenge, then Smishing will become more interesting to criminals. Banks protect their customers by campaigning to have phishing sites disconnected from the Internet as soon as the site is detected. Typically a bank will petition a website hosting provider to take down a phishing site within four hours of detection.

Pharming typically involves changing the internal settings on a victim’s computer thereby bypassing a victim’s legitimate address query functionality. For example, a victim may open a web browser and request hsbc.com. The website loads and while the page appears to be hsbc.com, it is in fact a Phishing site. The user is seamlessly delivered to a spurious website because the victim computer’s internal settings were changed to redirect specific website requests to malicious websites that appear legitimate.
Cybercrime and Fraud

Recently the author of this article was on a trip to Chicago when he was notified that his credit card was used in Philadelphia. The spurious credit card was presented in person to purchase physical goods. The thieves had managed to capture the data contained on the credit card’s magnetic stripe before replicating the data to the magnetic stripe of a blank “white plastic” card. The swiftness between card compromise and physical exploitation was amazing. Unfortunately this scene occurs daily all over the world. A credit card compromised in Britain, may be used within 24 hours in India. Criminals involved in physical world fraud are constantly leveraging technology to increase their profits.

Victim debit/credit cards can be used or sold as “cvv” or “dumps.” The criminal colloquial “cvv” represents the data embossed on the front of a card such as name, card number, expiration date, and the 3-digit security code printed on the rear of the card. “Dumps” describe the track1 and/or track 2 data encoded to the card’s magnetic stripe. A criminal is able to monetize “cvv” through online or phone purchases of legitimate goods. “Dumps” are monetized through duplication of the physical card and subsequent purchases of goods in person. Typically criminals resell the fraudulently obtained merchandise on auction type websites for competitive prices.

Stolen credit/debit card details remain especially lucrative for criminals. When PIN numbers can be tangentially obtained with a victim’s card details, criminals will monetize cash very quickly at ATM locations.

Team Cymru has observed groups of criminals operating in disparate geographic locations to maximize profit. Attacks on ATMs have been well coordinated, as have groups buying physical goods. Criminal groups can compromise and monetize their own credit cards, but typically criminals seek to purchase credit cards details from quality suppliers. The lure of easy profits creates a constant demand for quality dumps.

The source of stolen cards continues to originate through two primary methods: skimmers and network breaches.

UnAuthorized access to computers and networks containing credit card track data has proven especially disastrous for merchants and banks. The breaches of Heartland Payment Systems,11 RBS WorldPay,12 and TJX13 illustrate the determination of criminals to find and secure large databases of credit card track data. In the past, Point of Sale (POS) terminals used in retail outlets were exploited through vulnerabilities in the underlying operating system that these terminals use. Failure to patch the operating system has led to remote exploitation via freely available hacker tools. Data exfiltration has occurred for months before the merchant discovered or was alerted to the tainted POS terminal. Criminals continue to aggressively hunt for large amounts of card track data either in storage or in transit. Once a target is identified, the compromise is only a matter of time and resources. Today, financial databases and networks continue to fall victim to the most motivated and talented hackers. Previously, compromises have existed for over a year before the breach was discovered. The purveyors of this data will quickly become rich, as will the end users who purchase the data for coordinated exploitation.

The payment card industry (PCI) is in the final stages of implementing an updated version of the Data Security Standard (DSS).14 DSS is a collection of policies and procedures designed to establish a best practices document for organizations involved in transferring or storing payment card details. While DSS is absolutely necessary and obligatory for merchants, it merely acts as a stopgap for an outdated magnetic stripe card technology. Multiple European countries have fully implemented EMV (also known as “Chip + PIN”), which has significantly reduced the criminal demand for “chipped cards” in these respective countries.

In this framework, debit/credit cards store data on an encrypted chip embedded in the card. While the implementation of the technical EMV specification may be different at various banks, overall the adoption has been very successful from a fraud perspective. Unfortunately this evolution has increased demand for monetization schemes in countries that do not use EMV. A global bank movement to the EMV standard would significantly raise the bar on criminals specializing in this trade. In the realm of “Card Not Present” fraud (telephone and Internet purchases), Visa and MasterCard implemented “Verified by Visa” and “SecureCode” respectively, which require an additional password before a transaction is successfully completed. Unfortunately, a substantial number of “cvv” sold in the Underground Economy today are accompanied by the corresponding Verified by Visa or SecureCode password. This is the result of criminals slightly modifying Phishing and malware attacks.

The source of stolen cards continues to originate through two primary methods: skimmers and network breaches.
EMV also acts as a specification for secure online banking. Securing online banking access via a username and password in concert with security questions is a failed model. The financial services sector obviously defines failure on an annual rolling metric basis, but consumers and businesses feel the failure effects daily. Multi-factor authentication is a security term used to describe authentication procedures that require additional criteria be validated before access is granted. This usually means producing something you have in your possession in concert with something you know like a password or PIN. Multi-factor authentication certainly increases the difficulty of bank account compromise, but in its current form it is far from a solution for preventing fraud. Most two-factor deployments involve a hardware “token” issued by a bank to a customer. The digits displayed on the token change at regular time intervals. These digits are required in tandem with a customer’s password in order to successfully authenticate online.

The criminal response to two-factor authentication has been a continual stream of malicious code (also known as “malware”). The criminal response to two-factor authentication has been a continual stream of malicious code (also known as “malware”). Some of the more malevolent malware families are labelled by anti-virus software companies as “Sinowal,” “Zeus,” “Silent Banker Trojan,” etc. The malware itself is programmed to execute clever functions while remaining as undetectable on the victim’s computer as possible. The malware typically turns off any anti-virus software present on the computer and then silently waits. It waits for the victim to open a web browser and login into their bank or other financial account(s). The malware then typically conducts a “Man in the Middle” or “Man in the Browser” attack. Skipping the technical minutiae, the malware is capable of initiating an account transfer that looks legitimate to the victim's hard drive, key logging, advertising, and more. As Internet users’ habits evolve, malware authors take notice and develop new malicious features both for infection and monetization.

Then again, malware’s objective is not always revenue. Consider “Operation Aurora” and the intended purpose of an apparent attack on Google’s network for the purpose of collecting data about human rights activists. On the surface it certainly appears the attack was not motivated by greed. Therein lies the differentiator between malware: purpose. Custom malware is typically only written when the surfeit of available malware or hacking tools will not suffice. Often, this is the case where stealth is paramount, such as in the case of “GhostNet,” which appeared to be exfiltrating data from the Dalai Lama’s network for over a year before anyone discovered the breach.

Malware is a scourge upon the Internet, and a particularly nasty subset of that malware is botnets. A botnet is a collection of infected computers (also known as “zombies”) that are typically centrally controlled by a remote entity. Ten years ago a bot was a piece of code that automated some activity, typically in Internet Relay Chat (IRC). Today, the term bot usually implies a malicious persistent connection from an infected computer to a Command & Control (CnC) interface. This has created the problem of exporting real criminal tools to the criminal masses for a small fee. A handful of malware authors create botnet code that is then sold to the criminal public, typically for a few hundred dollars. These “crimeware” kits are delivered with meticulous instructions for use and a scale of fees for updated functionality and/or upgrades that prevent anti-virus detection. In fact the escalating game of cat and mouse between malware authors and anti-virus companies has become so extreme that over the past five years Team Cymru has observed 30 million unique malware samples and a very small percentage of those samples are actually new pieces of computer code. The difference represents the by-product of polymorphism, encryption, and other obfuscation techniques (known in the security industry as “stubs”). Since anti-virus companies largely depend on exact signatures to identify malicious code and malware authors create malware that mutates (or is “packed” differently) every time it runs, thus producing a completely different signature for detection. Other obfuscation techniques attempt to hide the malicious code in a virtual shell (a stub) and anti-virus software only scans the benign shell.

Botnets are particularly sinister because they exponentially increase a criminal’s capabilities and malicious schemes. Instead of infecting and controlling one victim’s computer, a bot herder (an individual who controls a botnet) is capable of centrally controlling thousands, sometimes even hundreds of thousands, of victim computers at once. Presently, criminals who have no technical ability can purchase a botnet and further their criminality online. Regrettably, the purveyors of these botnets are now publicly advertising and marketing in order to differentiate their product in the market place. In Underground web forums and Twitter feeds, botnet authors are actively attempting to increase revenue despite raising their risk profile with law enforcement.

Given the geographic disparities between victim’s computers, CnC nodes, and the bot herder(s), law enforcement’s attribution efforts are increasingly protracted and frustrating affairs. Until national cybercrime legislation enjoys global reciprocity, law enforcement’s efforts will continually be stymied. The picture, however, is not completely bleak. Law enforcement continues to pursue malware/botnet cases across international boundaries with occasional success. Presently, the problem is in scope. The current number of cyber-trained investigators is a pitfall in relation to the number of criminals currently writing or using malware. The other impediment to quick criminal case disposition is the nature of the Internet itself. Technologies like TOR and VPN networks allow criminals to move about the Internet anonymously. Internet privacy is certainly a noble value to support and uphold, but when law enforcement is unable to acquire required data in a timely fashion, cybercrime will continue to increase because the risk/reward equation is fundamentally skewed in their favour.
A confluence of malevolence is affecting the Web today. While “Web 2.0” represents an exciting new structure for ideas and opportunity, criminals are mirroring the optimism. Websites like Twitter and Facebook have become de facto communication tools, and criminals are leveraging the communication streams with innovative schemes. The trust models built into social media networks allow criminals to commandeer a victim’s account and subsequently communicate with all of the victim’s friends and associates. This equates to a new infection vector for bot herders. Additionally, groups specializing in criminal money movement used to create fictitious businesses online and then post reshipping and bank funds forwarding employment advertisements then post the malware in locations where criminals entice victims to download a website that hosts malicious code, on these types of prompts, the malware installation occurs effortlessly.

Speaking of infection vectors, do you ever wonder how all of this malware actually infects a victim’s computer in the first place? Malicious e-mail attachments were once the main threat that required wariness, along with self propagating worms that exploited unpatched operating systems; and while those threats still remain, by and large the favourite infection vectors include “drive by downloads,” Peer-to-Peer network file distribution, and social network social engineering. Criminals discovered that it was becoming increasing difficult to push malware to victims so they decided to post the malware in locations where victims would naturally infect themselves on the Web. By hacking popular websites or incentivizing visits to a lesser known website that hosts malicious code, criminals entice victims to download a “component” or “control” that is required for content functionality. Since many Internet users are conditioned to click through the successive dialogue boxes on these types of prompts, the malware installation occurs effortlessly. When direct e-mails are the infection vector of choice (known as “Spear Phishing”), sophisticated actors will use vulnerabilities in prolific applications such as Adobe Acrobat.28 A PDF attachment appears much more innocuous to the end user than a zip or executable file.

Peer-to-Peer networks can be especially disastrous for business computers shared on the computer with the rest of the network. The good news is that ISPs (Internet Service Providers) are implementing “walled gardens” in an effort to help protect their customers. Working with cyber security researchers, ISPs integrate daily lists of known CnC servers across the Internet. When a customer’s computer is observed communicating with a known CnC server, the computer is “quarantined” from the larger network and the customer is alerted. Once the customer’s computer has been cleaned of the malicious infection then the computer is reconnected to the Internet. This approach has proven effective to minimize a customer’s potential vulnerability after becoming infected.
The future

While it is difficult to accurately predict the future cyber threat landscape, Team Cymru believes the continued adoption of smart phones represents an increasingly lucrative target for criminals. Mobile malware that creates a “backdoor” or is able to perform “man in the application” functions will be able to compromise victims’ mobile banking activities. Additionally, maintaining secure code in mobile phone applications will remain a challenge for the companies providing the application storefronts such as Google, RIM, and Apple. Since thousands of applications are submitted for approval on different mobile phone platforms, storeowners must continue to rigorously check each application’s code for maliciousness and ensure the company in question authorizes the application being represented.

Conclusion

At one end of the spectrum, cybercrime appears to be increasing in scope and complexity, but the vexing concern is that decade old attacks still enjoy success. Well known vulnerabilities continue to exist on the Internet and information security best practices are continually ignored. Information assurance is still regarded as a niche field of study for students and professionals who labour in back rooms. Fortunately, large cybercrime events are garnering additional publicity, and government policy makers are beginning to appreciate the constant threat to governments, businesses, and individuals constantly at risk of being victimized. The issue is crime. Fundamentally we are discussing people and their behaviours. Cybercrime is not a technical problem and technology will never solve crime regardless of whether it occurs in the cyber realm or not. The incentives must be removed. The risk of attribution for cybercrime must increase through global legislative reciprocity and a substantial increase in technical law enforcement staffing and training.

The good news is that law enforcement is forging partnerships with the cyber security industry, researchers, and academics that are on the front lines in the cybercrime war. Often these individuals provide the keenest insights into particular cybercrime groups and criminal cases. The proactive partnerships are leading to noticeable arrests and that is good for the world’s 1.8 billion Internet users who hope their computer is not pwned.

* Levi Gundert is a Southern California native with a background in business, technology, and security. Mr. Gundert is a former Secret Service Agent who specialized in economic and cyber crimes. He led multiple proactive cybercrime initiatives within the Electronic Crimes Task Force which resulted in worldwide arrests in cybercrimes. Mr. Gundert currently supports Team Cymru’s business intelligence group. He is a Certified Ethical Hacker (CEH), Systems Security Certified Professional (SSCP), and Certified Information Systems Security Professional (CISSP).

1 “Pwned” is criminal parlance for the act of compromising a computer or network device and gaining unauthorized access to the resources within. The term is a derivation of “owned.
2 http://www.internetworldstats.com/stats.htm
3 Team Cymru Research NFP is a specialized Internet security research firm and 501(c)3 non-profit dedicated to making the Internet more secure. By researching the ‘who’ and ‘why’ of malicious Internet activity worldwide, Team Cymru helps organizations identify and eradicate problems in their networks. Much of Team Cymru’s time is spent identifying emerging trends within the Underground related to the monetization of compromised information. Team Cymru works with various organizations and industries affected by the Underground Economy. Many of Team Cymru’s efforts are for the benefit of Internet users, and at no cost to their partners. Team Cymru also works with Law Enforcement, where appropriate, from over 60 countries around the world.
4 On a rolling basis, over 25% of the world’s computers have probably been infected at some point.
5 http://www.paltelegram.com/latest/6288-1000-israeli-websites-hacked-since-flotilla-attack
6 Internet Relay Chat was an early Internet protocol that allows multiple clients to connect to a server or network of servers. Channels are created within an IRC server that are akin to. Since clients can maintain control of the infected computer.
7 http://www.consumeraffairs.com/news/04/05/shadowcrom.html
9 http://www.fbi.gov/page2/oct08/darkmarket_102008.html
10 http://www.msnbc.msn.com/id/37701078/ns/world_news/europe/
12 http://www.wired.com/threatlevel/2010/03/alleged-rbs-hacker-arrested/
13 http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever
16 http://www.owasp.org/index.php/Man-in-the-browser_attack
17 http://www.theregister.co.uk/2010/06/07/electronic_account_raided/
19 http://www.wired.com/threatlevel/2010/01/operation-aurora/
20 http://en.wikipedia.org/wiki/GhostNet
21 A bot may poll a CnC server at different time intervals, but the bot herder maintains control of the infected computer.
22 This number includes code embedded in HTML (webpages) which tends to contain a high level of similarity to other malicious web samples.
23 http://www.infoworld.com/t/hacking/your-favorite-malware-authors-now-twitter-851
26 http://www.torproject.org/
31 http://www.businessweek.com/magazine/content/08_16/b4080002218430.htm
32 http://www.net-security.org/secworld.php?id=9371
34 Mr. Gundert is a former Secret Service Agent who specialized in economic and cyber crimes. He led multiple proactive cybercrime initiatives within the Electronic Crimes Task Force which resulted in worldwide arrests in cybercrimes. Mr. Gundert currently supports Team Cymru’s business intelligence group. He is a Certified Ethical Hacker (CEH), Systems Security Certified Professional (SSCP), and Certified Information Systems Security Professional (CISSP).
The current era of cybercrime is no longer dominated by hackers accessing computer systems just for fun or notoriety. The development and growth of the digital economy has changed the criminal landscape dramatically. High rewards combined with low risks have made digital networks an attractive environment for various types of criminal groups. In the non-digital era, organised crime sought after the safe havens offered by countries with weak governments and unstable political regimes. Today’s organised criminal groups can benefit from national jurisdictions that do not have proper legal frameworks and technical capabilities to fight cybercrime. The easiness of communication, anonymity, and the accessibility of tools for illegal operations have transformed cybercrime into a global, fast-expanding and profit-driven industry with organised criminal groups thriving behind it.

Organised crime in cyberspace: changing structure

Organised criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in cyberspace. While some traditional criminal organisations are seeking the cooperation of e-criminals with the necessary technical skills, newer types of criminal networks operating only in the area of e-crime have already emerged. The structure of these criminal organizations is different from traditional organised crime organisations. Criminal activities are usually conducted within multi-skilled, multifaceted virtual criminal networks centred on online meetings. These networks are structured on “stand alone” basis, as members rarely meet each other in person and sometimes do not even have a virtual contact with other colleagues. This sophisticated structure, together with access to the core operations granted only to trusted associates, prevents organised cybercrime groups from being detected and infiltrated by law enforcement. The networks themselves could involve from ten to several thousand members and could include affiliated networks in their structure. Regardless of the number of members and affiliates, virtual criminal networks are usually run by a small number of experienced online criminals who do not commit crimes themselves, but act rather as entrepreneurs. The leading members of the networks divide the different segments of responsibility (spamming, controlling compromised machines, trading data) among themselves. Some “elite” criminal groups act as closed organisations and do not participate in online forums because they have enough resources to create and maintain the value chains for the whole cycle of cyber-offences, and therefore have no need to outsource or to be engaged as outsiders into other groups.

Tools and models for criminal activity

Organised crime borrows and copies business models from the legitimate economy sector. Cybercriminals employ models similar to the B2B (business-to-business) for their operations, such as the highly sophisticated C2C (criminal-
to-criminal) models, which use very effective crime tools available through digital networks. The computer systems’ vulnerabilities and software are exploited to create crimeware such as viruses, Trojans, keyloggers. These crimeware tools offer criminal groups the flexibility of controlling, stealing and trading data.

The development of botnets, networks of compromised computers running programs under external control, transformed some types of cybercrimes such as phishing into the worldwide underground ecosystem run by organised crime. The estimated financial gain of these criminal groups ranges from tens of thousands to tens of millions of dollars. The trade of botnets has also become a high-revenue activity that could be also linked to organised crime. The botnets’

The sole way to address the problem is to develop long-term responses that would include coordination and harmonisation of efforts on both national and international levels.

costs are relatively low compared to the criminals’ financial gain and to the damage to individual consumers and businesses, as well as to the financial health, reputation and trust in online transactions as a whole.

Crimeware is also used to deploy Crime-as-a-Service business models that represent the system of trading and delivering crimeware tools. Data supplying models are also used to share the tools to commit cybercrimes. For instance, by creating “customer” systems where instruments are available on demand, “users” just log into the server and choose from the range of tools suitable for fraud, phishing, and data stealing and then download them. When user data is stolen, criminals can use crimeware servers to commit organised attacks. Crimeware servers allow to control compromised computers and manage the stolen data.

Addressing the problem

Fighting cybercrime has always been a complex problem due to the number of ICT network users, the transnational nature of the Internet and its decentralised architecture. Cybercriminals, and especially organised criminal groups, have been and probably would always remain several steps ahead of legislators and law enforcement agencies. C2C networks benefit from anonymous communications, automation of attacks and the difficulties that law enforcement agencies experience in determining the location: servers with crimeware could be in one country, while members of the network could be in another one, targeting victims across the world.

In addition to strengthening the current legal frameworks, updating old legislation, harmonising laws on an international level, what is needed is also the cross-sector cooperation on national level as well as international cooperation in detecting, investigating and preventing e-crimes committed by organised criminal groups. The development of a comprehensive understanding and a forward-looking approach are required since fighting organised cybercrime seems to have a moving target.

Countries face the problem of addressing this international problem collectively. Some States just do not have the necessary tools to respond to the activities of the organised cybercriminals, they may lack the technical skills or have legal drawbacks. The development of a common understanding that no country could be safe alone in the global ICT network is very important.

Future trends and responses

With the absence of a global strategy to counter organised cybercrime, the problem is very likely to deepen in the foreseeable future. With the development of ICT networks and the opportunities they offer, criminal groups will benefit from the entire range of the tools and models available to the legitimate economy sectors. The information’s availability would make it not only more accessible to organised groups, but also more easy for them to foster and automate their fraud-committing activity. It would also probably link more opportunistic criminals to existing criminal networks.

Cybercrime is transforming itself into an illegal industry, where syndicates are highly sophisticated and are very hard to identify. Some cybercrime industries would be run solely by organised criminal groups, constantly seeking the newest technical solutions and for the creations of new markets. As a result, it would be likely for the cybercrime ecosystem to be soon dominated by criminal organisations, as cybercrime networks that have already become international would multiply opportunities and reach the global scale by exploiting the legal frameworks’ weakness and searching for safe havens in countries with less capability to detect and fight them. This will make fighting cybercrime a more difficult task for law enforcement agencies.

As markets and trading itself have always attracted organised criminal groups seeking benefits from illegal activities, the growth of digital operations and services in legitimate markets are a key enabler for organised cybercriminals, both for committing traditional crimes and for developing new types of illegal activities. Using business models that have proved their effectiveness for the legal business sector, organised cybercrime groups deploy highly sophisticated tools of online criminal activities. The risk for individuals, businesses, and governments grows with the further digitalisation of their economy. E-activity is conducted as long-term sustainable criminal operations. Due to the borderless nature of the Internet, the problem of organised cybercrime has truly global consequences when no country can ensure safety only within its borders. The sole way to address the problem is to develop long-term responses that would include coordination and harmonisation of efforts on both national and international levels.

* Dr. Tatiana Tropina is Senior Researcher at the Cybercrime Institute in Cologne, Germany.
Terrorist Use of the Internet and Legal Response

*Marco Gercke, Daniel Thelesklaf*

Without doubt terrorist organisations today are using the Internet for various purposes. Unlike the early debate when the focus was on potential terrorist-related network-based attacks against critical infrastructure and the use of information technology in armed conflicts (cyberwarfare), it is widely recognised that the range of activities is more complex. Terrorist use of the Internet includes research, training, propaganda and communication. But despite more intensive research many aspects are still uncertain as reports about concrete incidents often remain classified. The following article provides an overview of the different areas of terrorist use of the Internet and the concept of legal response.

I. Terrorist Use of the Internet

1. Propaganda

While ten years ago only 12 of the 30 foreign terrorist organisations listed by the U.S. State Department maintained websites, in 2004 the United States Institute of Peace reported that almost all terrorist organisations have websites. The Internet-related propaganda activities include the distribution of video messages and the descriptions and justifications of activities. The Internet has substituted traditional channels of distribution, particularly with regard to video messages.

2. Collection of information

The Internet has proven to be highly useful for collecting information. Millions of websites provide information that can be used for legitimate as well as illegal purposes. One example are satellite pictures. High-resolution satellite pictures, previously available only to a handful of military institutions, are today made available by various Internet services. Other examples include instructions on how to build bombs, and even virtual training camps, providing information on the use of weapons in an e-learning approach. Such instructions are available on a large-scale online.

In 2008, Western secret services discovered an Internet server that allowed for the exchange of training material and communications. Several websites were reported to be operated by terrorist organisations to coordinate activities. In addition, sensitive or confidential information that is not adequately protected from search robots can be found via search engines. Terrorist organizations have started to explore this technology. In 2003, the U.S. Department of Defense was informed about a training manual linked to al-Qaida providing information on how to use public sources to find details about potential targets. In 2005, the German press reported that investigators had found downloaded manuals on how to build explosives on the computer of two suspects, who then attempted to attack the German public transportation system with homemade bombs.

3. Communication

In the investigations following 9/11, it was reported that the terrorists used e-mail communication to coordinate their attacks. The press reported that detailed instructions about the targets and the number of attackers had been exchanged via e-mail. The threats related to a technology shift are also accentuated by the fact that the interception of Voice-over-IP calls is going along with significantly more challenge than the interception of regular phone calls.

4. Use of information technology to prepare for “real world” attacks

It has been reported that terrorists are using online videogames as part of their preparation for attacks. Various online games simulate the “real world” by allowing the user to manipulate characters (avatars) in a virtual world. Theoretically, those online games could be used to simulate attacks, though it is not yet certain to what extent they have been used to do so.
5. Attacks against critical infrastructure
Over the past decades, more and more countries have turned into information societies.24 Services such as online banking and telephone communications using Voice-over-Internet-Protocol (VoIP) are very popular.22 But it is not only the communication sector that has shifted its services online: information technology and Internet services are today used to control and manage many functions in buildings, transportation systems, waterways and energy grids.23 Critical infrastructure is widely recognised as a potential target for terrorist attacks, as it is, by definition, vital for the stability of the State.24 Infrastructure is considered to be frail, and its incapacity or destruction could have a debilitating impact on a State’s defence or economic security.25 This concerns, in particular, electrical power systems, telecommunication systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems and emergency services. The civil disturbance caused by Hurricane Katrina highlights the dependence of developed societies on those services.26 Both the new means of communication and the use of information technology to control critical infrastructure have influenced terrorist organisations’ ability to use the Internet for attacks against critical infrastructure and to make it more vulnerable to attacks.27 Interconnected systems that are linked by computer and communication networks are especially attractive targets.28 A network-based attack would do more than cause a single system to fail. Rather, it would bring down an entire network of systems and their related infrastructure. Even short interruptions of services would cause huge financial damage to e-commerce businesses, government service providers and the security sector.29

II. Legal Response
The recognition of the threat associated with terrorist use of the Internet and the related challenges has led to various legal approaches to address the issue. The ones on a national level in particular show significant differences. With regard to systematic aspects, there are three different approaches of how countries are addressing the specific challenges of terrorist use of the Internet:

1. Applying existing cybercrime legislation, developed to cover non-terrorist related acts, to terrorist use of the Internet;
2. Applying existing legislation, developed to cover non-Internet related terrorist acts, to Internet-related acts as well;
3. Enacting specific legislation on terrorist use of the Internet.

1. Application of Cybercrime legislation
Some countries are using existing cybercrime legislation that was developed to cover non-terrorist related acts to criminalize terrorist use of the Internet. One example for such provision is Art. 2 of the Council of Europe Convention on Cybercrime,30 which was developed to cover traditional cybercrime, but not specifically designed to address terrorist related acts:

**Article 2 – Illegal access**
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Based on the experiences with this approach, three aspects ought to be taken into consideration. Substantive criminal law provisions that were implemented to cover non-terrorist related acts (such as illegal access31 or system interference32) might be applicable in terrorist-related cases, but very often the range for sentencing will differ from specific terrorism legislation. Depending on the dogmatic structure of procedural law this could influence the ability to use sophisticated investigation instruments that are restricted to terrorist or organised crime related investigation.

Secondly, and with regard to procedural instruments, the situation is slightly different. The application of cybercrime specific investigation instruments in cases of terrorist use of the Internet (such as the expedited preservation of computer data33) is going along with less challenges, since most countries do not limit the application to traditional cybercrime offences but to any offence involving computer data.34

Finally, regional instruments developed to address the challenge of cybercrime, but not specifically terrorist use of the Internet, often contain exemptions for international cooperation with regard to political offences. One example is Art. 27, paragraph 4.a of the Council of Europe Convention on Cybercrime.

**Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements**

[...]
3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
b) it considers that execution of the request is likely to prejudice its sovereignty, security, order or other essential interests. [...]

FREEDOM FROM FEAR - July 2010 19
It has been reported that terrorists are using online videogames as part of their preparation for attacks

The provision authorizes parties to the Convention to refuse mutual assistance if it concerns an offence which the requested Party considers a political offence, or connected with a political offence.6 As this is often the case when it comes to terrorist use of the Internet, such approach can hinder the investigation. To improve the situation the terrorist-specific legal frameworks, such as the 2005 Council of Europe Convention on the Prevention of Terrorism7 contains an exclusion of the political exception clause in Art. 20.8

With regard to the Convention on Cybercrime, the issue is only solved with regard to those countries that have signed and ratified both Conventions.9

2. Application of existing (non-Internet specific) terrorism legislation

Another approach is to use existing terrorism legislation to criminalise and prosecute terrorist use of the Internet. On example for a traditional instrument is the aforementioned Council of Europe Convention on the Prevention of Terrorism.10

Article 5 – Public provocation to commit a terrorist offence

1 For the purposes of this Convention, public provocation to commit a terrorist offence means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.

2 Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

The Convention defines several offences, such as the above-mentioned public provocation to commit a terrorist offence: however, it does not contain provisions criminalising terrorist-related attacks against computer systems or specific data-related procedural instruments. However, especially with regard to investigating Internet-related offences, specific procedural instruments are required as the investigation process differs significantly from traditional ones, and traditional instruments would therefore often fail.

3. Development of specific legislation dealing with terrorist use of the Internet

The third approach is the development of specific legislation addressing terrorist use of the Internet. One example is Section 4.f of the Draft ITU Cybercrime Legislation Toolkit.

Section 4. Interference and Disruption

[...](f) Intent to Cause Interference or Disruption for Purposes of Terrorism. Whoever commits interference and/or disruption pursuant to paragraphs (a) and (b) of this Section with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyberterrorism, shall have committed a criminal offense punishable by a fine of [amount] and imprisonment for a period of [duration].

The International Telecommunication Union (ITU) is the UN organisation that has most responsibility for practical aspects of cybersecurity.40

The aim41 of the Draft Toolkit is to give countries the possibility of using sample language and reference material in the process of national cybercrime legislation development, that can assist, according to the Toolkit’s developers, the “establishment of harmonized cybercrime laws and procedural rules.”42

The Toolkit was developed by the American Bar Association on the basis of a comprehensive analysis of the Council of Europe (CoE) Convention on Cybercrime and the cybercrime legislation developed by countries. It aims to be a fundamental resource for legislators, policy experts, and industry representatives, providing them with the framework to develop consistent cybercrime legislation. Moreover, in addition to traditional approaches, the Toolkit also contains several specific terrorist-related offences.43

* Dr. Marco Gercke is the Director of the Cybercrime Research Institute.

Mr. Daniel Thelesklaf is the Executive Director of the Basel Institute on Governance.

5 Regarding the use of YouTube by terrorist organisations, see Heise Online News, 11 October 2006, available at http://www.heise.de/newsticker/meldung/79311; Staud in Sueddeutsche Zeitung, 05.10.2006
13 For more information regarding the search for secret information with the help of search engines, see Long, Skooids and van Eikelenborg, Google Hacking for Penetration Testers.
14 ‘Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty per cent of information about the enemy.’ For further information, see Conway, ‘Terrorist Use of the Internet and Fighting Back’, Information & Security, 2006, page 17.
20 Regarding other terrorist-related activities in online games see Chen/Thoms, ‘Cyber Extremism in Web 2.0 – An Exploratory Study of International Jihadist Groups’, Intelligence and Security Informatics, 2008, page 98 et seq.
21 For more information on the information society see Masuda, The Information Society as Post-Industrial Society; Dutta/De Meyer/Jain/Richter, The Information Society in an Enlarged Europe; Maldoom/Marsden/Sidak/Singer, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Information Society: Hoymby/Clarke, Challenge and Change in the Information Society.
31 See for example Art. 2 Convention on Cybercrime.
32 See for example Art. 5 Convention on Cybercrime.
33 Art. 16 Convention on Cybercrime.
34 See in this context for example Art. 14 Convention on Cybercrime: Article 14 –Scope of procedural provisions
1. Each Party shall adopt or maintain, or, if such measure is not adopted, shall adopt, other criminal offences committed by means of a computer system; and
2. the collection of evidence in electronic form of a criminal offence. […]
35 Convention on Cybercrime, ETS 185.
36 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b. it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.
37 Council of Europe Convention on the Prevention of Terrorism, ETS 196.
38 Article 20 – Exclusion of the political exception clause: 1 None of the offences referred to in Articles 5 to 7 and 9 of this Convention, shall be regarded, for the purposes of extradition or mutual legal assistance, as a political offence, an offence connected with a political offence, or as an offence inspired by political motives. Accordingly, a request for extradition or for mutual legal assistance based on such an offence may not be refused on the sole ground that it concerns a political offence or an offence connected with a political offence or an offence inspired by political motives. […]
39 Council of Europe Convention on the Prevention of Terrorism, ETS 196.
43 Sec. 2 d) (Unauthorized Access for Purposes of Terrorism), Sec. 3 f) (Unauthorized Access to or Acquisition of Computer Programs or Data for Purposes of Terrorism), Sec. 4 f) (Intent to Cause Interference or Disruption for Purposes of Terrorism), Sec. 6 h) (Intent to Furtherance of Terrorism).
Foreword

In the last decades the most developed countries of the world have realized a social model characterized by a high “quality of life” of their citizens. There are, in fact, many services and opportunities available to every citizen, which contribute to satisfying their needs or expressing their attitudes.

Energy provision, healthcare, transportation and financial systems represent some of the fundamental pillars of this “quality of life” model. The availability of those services is perceived as a natural fact, to the extent that if they were no longer accessible, most of us wouldn’t know what to do in many circumstances.

The current situation has changed profoundly since the beginning of 20th Century, when every family heated its house with lumber collected by the family members and possessed autonomous transportation means (horses, mules etc.), or when an entrepreneur would have to install autonomous power generation mechanisms for its manufacture.

Moreover, in the last years there has been an increasing attention to the dependence on those infrastructures allowing the provision of services, and whose unavailability would unacceptably compromise the quality of our lives. Those infrastructures have been dubbed as “critical,” and the need to protect their existence and enduring functioning became a synonym of the need of protecting our “quality of life.”

CI Protection Initiatives

Following the terrorist attacks that shocked the world in the first years of the new Millennium, both in North America and in Europe, many advanced countries started to consider the protection of their critical infrastructures (CI) in a more organic way, taking into account potential intentional attacks against them.
Among the first countries to take action, the U.S.A. established the Department of Homeland Security (DHS) right after the attacks of 11 September 2001. This entity immediately outlined the protection of critical infrastructures and key assets among its critical mission areas, drafting the National Infrastructures Protection Plan (NIPP), which provides a unified nation-wide strategy for its national protection.

The DHS is also mandated to guide, integrate and coordinate the national efforts for improving the protection of critical infrastructures, developing and implementing programmes and methodologies of risk assessment, inter-sector guidelines and metrics.

By the end of 2004 the European Union followed this rising interest and launched the European Programme for Critical Infrastructure Protection (EPCIP). Such programme also addresses prevention, preparedness and response to terrorist attacks, and it is still supporting many initiatives promoting critical infrastructures’ security.

The directive 114/2008 of the European Commission represents instead a first step for harmonizing the protection of European critical infrastructures (ECI) around a common baseline of measures. The first step of this baseline is the identification of the critical infrastructures, applying cross-cutting criteria based on the ex ante assessment of human casualties, economic consequences and public effects due to a possible outage of candidate infrastructures.

After identifying and designating the ECIs, each of these must provide a liaison officer and complete an “operator security plan” based on the most widely accepted risk management concepts. Every EU country must also designate a national contact point on the matter and periodically report to the Commission. This directive initially applies to critical infrastructures in the energy and transportation sectors, and will be extended to other sectors in the near future.

**CI Threats and Impacts**

Critical infrastructures are managed by a constellation of private and public organizations which are naturally prone to a wide variety of threats that can impact the citizens’ “quality of life,” depending on their own characteristics in terms of processes, assets etc. Some of those organizations, for example, might rely more on information systems than others and will thus be more susceptible to cyber attacks, as in the cases where SCADA (Supervisory Control And Data Acquisition) systems are involved. In this latter situation, constantly growing in number, the continuous functioning of large infrastructures (power plants, oil sewage, air traffic sensors etc.) can be consistently assigned to automated or semi-automated systems interconnected by distributed networks. Nowadays, many industrial processes (like automobile construction, food production and even goods’ distribution) are also being progressively controlled by SCADA or ICT (Information and Communication Technology) systems, which help cutting operational costs and increasing efficiency. In all of these contexts, a cyber attack could not only have the same consequences as a physical sabotage, but it could prove to be even tougher because of the possibility of reaching a large number of similar systems via remote links.

Since the ultimate goal is to protect the frequently cited “quality of life,” critical infrastructure must be protected not only against all types of intentional attacks. These may range from retaliation sabotage by a disgruntled employee up to terrorists attacks aimed at waging fear and damage in a region or country, but also from natural events and disasters to mechanical failures and the omnipresent human errors.

Every one of those threat families is composed by a vast number of possible actions performed by different actors (threat agents) which, as a part of the risk management discipline, are then connected to specific impacts. Those impacts are related to the simple question “what would happen if,” and are thus strongly coupled with threats. In any case, most of the approaches used worldwide to identify critical infrastructures are “all hazard;” this means that the criticality assessment is based on the impact of a breakdown of the infrastructure leading to the interruption of the service provision, irrespectively of the specific threat scenario that would lead to the breakdown itself.

The most widely recognized high-level impact is the loss of human lives, but the “quality of life” goes well beyond the “survival” concept, thus bringing into consideration other impacts like social and political stability, economic losses, pollution, confidence in institutions, psychological suffering and many others, which, in turn, may be generated by a large number of possible threats.

**CI Protection Solutions**

Prevention is a key factor and, in fact, all modern critical infrastructure protection programmes mandate in their very core some kind of risk assessment activity, identifying the critical assets, evaluating the threats to which they are prone and the effectiveness of the adopted protecting countermeasures. If the results of this activity show an insufficient protection, it must be remedied through the adoption of additional countermeasures.

Indeed, most operators of major critical infrastructures already implement effective risk management and business
continuity plans. In many sectors, specific rules are in place to guarantee operational continuity. Nevertheless, due to the highly interconnected nature of critical infrastructures, a fault in a “minor” infrastructure, perhaps not properly secured, could cause an unexpected cascading effect, leading to the progressive breakdown of other infrastructures. This circumstance calls for an enhancement of the overall level of security, guaranteeing a “basic” operational continuity for all the infrastructures contributing, even indirectly, to the citizens’ “quality of life.” Since the impacts to the life quality are so wide-ranging and different, conducting a realistic risk assessment is neither an easy task nor is it something that many organizations are used to doing. Luckily there are some contexts in which those topics are adequately addressed, as within “management systems.” Those organizational frameworks are sets of requirements, established by some national or international standard, aimed at correctly managing a specific topic in a documented and improvement-oriented way. Some examples of management systems relevant for critical infrastructures include:

- ISO 22399 on incident preparedness and operational continuity;
- ISO/IEC 27001 on information security;
- OHSAS 18001 on occupational health and safety;
- ISO 14000 on environment.

The correct joint application of those sound methodologies could be a huge step forward in the protection of critical infrastructures. All those management systems are based on risk assessment concepts and they are interoperable between them. Moreover, they are mature objects supported by competent communities, dedicated tools and they even offer control and certification capabilities. Most importantly, every one of them separately addresses some of the relevant impacts to the “quality of life.” Rather than inventing new solutions to already addressed problems, the correct joint application of those sound methodologies could be a huge step forward in the protection of critical infrastructures. This fact, opportune-ly coordinated in its application by local and interstate governments, even in a gradual step-by-step way, should ultimately be able to bring our society to a more stable and sustainable state of “quality of life.”

* Marco Carbonelli, Laura Gratta work in the Interministerial Coordination Secretariat for Critical Infrastructure Protection, within the Italian Presidency of the Council of the Ministers, and are in charge of the Critical Infrastructure modelling and the Directive 114/08 CE national implementation areas, respectively. Luisa Franchina is Director General of the Team on CBRN attack risk of the Italian Department of National Civil Protection, and is the Head of the Interministerial Coordination Secretariat for Critical Infrastructure Protection, within Italian Presidency of the Council of the Ministers. Fabio Guasconi is a Team Manager for @ Mediaservice.net S.r.l., a Security Advisory firm and is the chairperson of the Italian ISO/IEC JTC1/SC27 committee. Daniele Perucchini is the Leader of the Critical Infrastructure Protection Area within Fondazione Ugo Bordoni.
THEY TOOK MY HOME,
BUT THEY CAN'T TAKE MY
FUTURE
Online Crimes against Children

* John Carr

The emergence of the Internet as a mass consumer product has not necessarily created any entirely new genres of crime, but it has certainly given a new twist to some very old and familiar ones
The emergence of the Internet as a mass consumer product has not necessarily created any entirely new genres of crime, but it has certainly given a new twist to some very old and familiar ones. Above all it has changed the scale on which a number of offences are carried out. Crimes against children are a classic example. Crimes involving the production and distribution of child abuse images are a very specific case in point. Prior to the arrival of the Internet, in most parts of the world it was extremely difficult to get hold of child abuse images. Usually, a person interested in acquiring any had to know someone who already had some, otherwise they had to go to great trouble and take several risks. This led one distinguished expert on child protection to describe the exchange of child abuse images at that time as being “a cottage industry.”

Today, however, the images can be a mouse click away. It is a global industry worth millions of dollars to those who engage in it for financial gain.

Numbers

Taking 1995 as “Year 0” (the last year before the Internet boom erupted in many countries), Interpol at that time knew of around 4,000 child abuse images in total. Figures recently supplied by Interpol and other data published in the UK and Italy suggest that today the number of known images is around 1,000,000, and the number of children abused to make them runs in the tens of thousands. There is a marked growth in images of younger children being subjected to ever more violent and depraved sexual acts. It is anybody’s guess how often the images and their duplicates are downloaded or exchanged online and off, but it is likely to run into billions. Another indication of the change in the scale of offending comes from an examination of the numbers of images seized by the police when arresting suspects. Prior to the Internet, typically police officers would arrest individuals with only a handful of images in their possession, or in unusual cases maybe hundreds. In the whole of 1995 the police in Greater Manchester in the UK seized the grand total of 12. In June 2009 in a single action the police in Mexico arrested one man, Arthur Leland Sayler, who possessed 4 million images. The trend in convictions is another useful signifier. Taking 1995 once more as the baseline, in the UK 142 people were cautioned or proceeded against for child abuse image offences. In 2007 it was 1,402. Precise comparisons between 1995 and 2007 in terms of Internet usage are not very meaningful because broadband barely existed in 1995, while by 2007 it had become commonplace. In 1995 fewer than two millions UK households had Internet access (primarily dial-up), whereas by 2007 the number of households with Internet access was up to 15.23 millions, of whom 84% had broadband. The inference is pretty clear. There is a strong link between Internet crimes of this kind and the growth in the number of Internet connections within a country. No nation appears to be exempt.

The scale of activity addressed

There are well established procedures for notifying hosting companies of the presence on their web servers of illegal images. These procedures normally work very well and the
There is a marked growth in images of younger children being subjected to ever more violent and depraved sexual acts. Images are removed swiftly when the hosting company is in the same jurisdiction as the person reporting it; however, if the image is on a web site housed in a foreign jurisdiction there can be inordinate delays, while the images remain on view. This has led to the development of a practice known as “blocking,” which renders the image inaccessible in the reporting country.

Blocking has afforded an opportunity to gain a rare insight into the overall level of illegal activity taking place in this space. Five months after blocking was launched in Denmark in 2006 the Danish police estimated 238,000 users had attempted to reach known illegal child abuse sites. In Norway blocking was stopping between 10 and 12,000 attempts per day. In Sweden it was 20 – 30,000 attempts per day. In 2009, British Telecom (BT) estimated their solution was preventing 40,000 attempts per day to access known child abuse web sites over their broadband network. Extrapolated across the whole UK broadband network this suggests blocking is preventing up to 58 million attempts per year. These are substantial numbers.

The rise of Peer2Peer networks

For the foreseeable future, the worldwide web will remain a key medium for the distribution of child abuse images, but Peer2Peer networks such as Limewire and Gnutella are rapidly growing in importance. In an in-depth documentary broadcasted on Irish TV on 31 May 2010, it was disclosed that in the past six months a US technology company had traced 1.2 million people in all parts of the world who had accessed child abuse images over a number of Peer2Peer networks. Ireland itself is a small country, with a population of around 4.25 millions and about only 2.8 million Internet users. Yet in a period of 30 days the same US company detected roughly 1,000 individuals in Ireland trading or downloading child abuse images. Downloading child abuse images is a serious offence against the children depicted and it deserves police attention entirely in its own right, but there is also evidence which suggests that people who get involved in downloading such images may find themselves on a path that ultimately leads them to commit new offences against children, either in the real world or online. This is another major reason for wanting such images to be removed from public view as quickly as possible: it helps reduce the numbers of potential new online and offline child abusers.

Internet is not to blame

The Internet itself is not to blame for any of this. At the end of the day the decision to engage in criminal conduct is the result of a conscious choice made by individuals. But this data underlines the singular role that technology plays in facilitating a range of crimes against children. It reminds us also of the vital importance of law enforcement agencies across the world having the capacity to understand how the technology works, and having trained personnel at hand who can put that knowledge to work to protect children.

Prior to the Internet, typically police officers would arrest individuals with only a handful of images in their possession

* John Carr is Secretary of the UK Children’s Charities’ Coalition on Internet Safety and a Senior Expert Adviser to the ITU’s Child Online Protection initiative. He is also a member of the Executive Board of the UK’s Council for Child Internet Safety and a member of the Advisory Council of INHEOP, the global association of internet hotlines.
Estimating and Interpreting the Prevalence of E-fraud across the World

Survey-based Estimates

The International Crime Victimization Survey (ICVS) is a standardized survey on experiences of crime that has been carried out five times since 1989 in a large sample of European countries, in the USA and in Canada. The last round of the ICVS was coordinated by UNICRI (Van Dijk, Van Kesteren & Smit, 2008). In developed countries the ICVS consisted of computer-assisted telephone interviews of probability samples of 2,000 inhabitants per country. The questionnaire includes questions about victimization experiences in the course of last year covering various forms of frequently occurring types of crime (e.g. burglary, robbery and assaults). The ICVS asked about consumer fraud for the first time in the 1992 sweep in developed countries. People were asked whether someone selling them something or delivering a service had cheated them in terms of quantity or quality of the goods or services during the past year. Although the question does not exclude serious incidents of fraud, most of the incidents reported probably amount to simple forms of cheating in shops. In the fifth sweep of the ICVS, carried out among samples from 30 countries and 33 capitals or main cities, those who reported being victims of fraud were asked whether this happened while shopping online. Answers to the latter question are the source of the results presented here.

On average, 11% of respondents in the participating countries said they had experienced some type of consumer fraud in the course of last year (2005). Victims of consumer fraud were asked where the incident had taken place. At a national level, 45% of victims said the fraud had taken place in a shop; 11% was the victim of a fraud during either building or construction work or by a garage, while 9% mentioned it had happened while shopping online. This implies that 1% of the national inhabitants of developed countries had been victimized by a case of E-fraud in the course of one year. Among inhabitants of capital cities, the victimization rate by E-fraud was 1,5% in one year.

Table 1 illustrates these details.

* Jan Van Dijk
Victimization by Internet-based consumer fraud is most common in the USA, Poland, Germany, Bulgaria and the United Kingdom. Prevalence rates are lowest in Italy, Finland and Greece. Among the capitals Lima (Peru), Berlin, New York and London stand out with comparatively high rates of victimization.

In a second follow-up question, respondents reporting fraud were asked whether it had been a case of credit card fraud. It was so in 7% of all cases of fraud and in 27% of all cases of E-fraud. The latter finding shows that a major part of E-fraud consists of Identity Theft with the use of credit cards (Identity Fraud).1 Furthermore, the ICVS results showed that only 10% of all frauds are ever reported to the police. Cases of E-fraud are presumably more often reported to other agencies such as banks.

According to UNDP’s 2006 Human Development Report, between 50 and 70% of the population in industrialised countries had access to the Internet in 2005. This implies that around 2% of Internet users had been victim of Internet-based fraud annually. In many developed countries in 2005 Internet-based frauds had reached prevalence levels similar or above those of conventional property crimes such as car theft or pick pocketing. Prevalence rates were, as mentioned, especially pronounced among inhabitants of main cities. Since 2005, both Internet access and E-commerce (the use of Internet for shopping) have become more common. It is therefore likely that prevalence rates of Internet-based frauds have gone up significantly as well. In fact E-fraud might well be on its way to becoming the most common form of property crime affecting citizens of the industrialised world.

---

1 The 2003 US National Crime Victim Survey investigated victimization by credit card fraud as a subcategory of identity theft. This study showed a one-year prevalence rate of victimization by credit card fraud of 2.4%. The Australian version of the ICVS, which used a somewhat different set of questions on E-fraud, showed that 5% of the national public had been victimized by credit card fraud while doing transactions on the Internet (Johnson and Krone, 2007). The British Crime Survey has included a question on credit card fraud in its questionnaire since 2006. The national prevalence rate has gone up from 3.7% in 2005 to 6.4% in 2009 (Walker et al, 2009).
Discussion: Is E-fraud Security Driven?

Countries or cities with comparatively high rates of victimization by Internet-based frauds are a mixed group in terms of Internet use. It comprises both countries where Internet is most widely used (the USA and the UK) and countries that are technologically less advanced (Bulgaria and Peru). Locations with low victimization rates also appear to be heterogeneous in terms of Internet use. For example, the use of Internet for commercial transactions is very common in Iceland and Finland where Internet-based fraud is rare. On the face of it, there is no strong relationship between the prevalence of E-commerce in national populations and the prevalence of E-fraud. According to criminal opportunity theory E-crimes are likely to be driven by the extent of E-commerce. The lack of an obvious positive correlation is therefore somewhat surprising. One possible explanation for the lack of such relationship is an inter-country variation in the legal and technical security measures against E-fraud. Examples are differences in the authentication procedures for the use of credit cards or for online banking. In some countries the use of pin codes has been made obligatory for the use of credit cards, while in others it is not. In the USA, authentication for online banking has remained relatively simple (use of a single password), compared to, for example, the Netherlands where the Central Bank has imposed more stringent security procedures on banks (Vermeulen, 2010).

The variation in security provisions might determine prevalence of E-fraud more strongly than differences in the level of E-commerce per se. This “security hypothesis” merits further testing in comparative international studies such as the 2010 round of the ICVS.

Literature


* Prof. Dr. Jan Van Dijk was the director of the Research and Documentation Centre of the Dutch Ministry of Justice and professor of Criminology at the University of Leiden. In 1987 he launched the International Crime Victims Surveys. Between 1998 and 2005 he worked for the United Nations in Vienna and Turin (as Head of Research of UNICRI). In 2008 he received the Sellin-Glueck Award of the American society of Criminology for his lifelong contribution to international criminology. He currently holds the Pieter van Vollenhoven chair in Victimology and Human Security at the University of Tilburg (The Netherlands) and acts as consultant for Eurostat on the design of the European Union Survey on Public Safety to be conducted in 2013.
Avoid Becoming a Victim of Cybercrime

*Scot Huntsberry*

Money is typically transferred via wire transfers, leaving little recourse for the victim. The most recent trend is an increase in bank-to-bank wire transfers.

The news is full of reports detailing the stories of victims who have lost thousands, even millions, of dollars at the hands of cyber criminals. Many of us know someone who has already been the victim of one of these crimes. As widespread as cybercrime appears to be, it would be easy to conclude there is little anyone can do to avoid becoming a victim. However, the prevalence of cybercrime does not mean that victimization is inevitable or that people should avoid using the Internet. Users can make themselves aware of the vulnerabilities its use creates and can take steps to reduce their risks.

Computer users can take measures to decrease their risk of becoming the victim of cybercrime by adhering to a few simple Internet usage rules. First, users should remember to log off and shut down their computers when they are not being used. Cyber criminals often scan networks searching for “always on” computers, which they consider readily accessible and unattended targets. By minimizing the amount of time computers are powered on and connected to the Internet, people can reduce their vulnerability to hacking attacks.

Users should remember to log off and shut down their computers when they are not being used.

Next, users should install and maintain both antivirus and firewall programs. These applications serve as a first line of defence against viruses and other malicious computer programs designed to circumvent security features within computers’ operating systems. Additionally, operating system developers regularly release updates or “patches.” To increase their computer’s security, users should install these updates as soon as they become available. Cyber criminals frequently disguise malicious software as images or documents attached to email messages, so users should never open or download email attachments from unknown senders.

Many people now use wireless networks in their homes. Strong encryption within a wireless router’s settings can prevent cyber criminals from accessing and exploiting data stored on computers. Unprotected, or “open” wireless networks that do not utilize encryption to protect network traffic are very popular targets for cyber criminals. By intercepting this wireless network traffic, crooks can quickly glean personal information, passwords, and other data they can then use to perpetrate various cyber crimes.

Even worse, they sometimes abuse their access to other people’s networks to make it seem like the victims are committing cyber crime. If you have an unencrypted wireless network in your home, don’t be surprised if the police shows up.
up at your door to find out whether you have been hacking into computers, committing online fraud, or distributing contraband.

Many people maintain accounts on literally dozens of different websites, so they create easy to remember passwords. While this means you’re less likely to forget an infrequently used password, these simple passwords are quickly compromised by savvy cyber criminals. Moreover, many people use the same password on their social networking websites and their banking and brokerage accounts. When cyber crooks steal passwords for social networking websites, they often try to use them to access financial accounts. In order to avoid such problems, people should use unique and complex passwords for each of their accounts.

People should use unique and complex passwords for each of their accounts

These simple rules provide baseline security for most Internet users. However, there are additional precautions people can take to further reduce their risk of becoming the victim of a cyber crime. Understanding and recognizing some of the more common criminal schemes can help people avoid falling prey to them.

In one prevalent scheme, cyber criminals send phishing emails. These emails falsely claim to be from legitimate senders and contain documents meant to dupe the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information. Some phishing emails have links to fake websites that look just like sites the victims use regularly. After tricking victims into providing banking credentials or other sensitive information, the criminals utilize a number of different methods to access and steal the victim’s money.

Internet auction fraud is very common. Cyber criminals saturate the Internet auction sites and offer almost every product people are looking for. The postings often make it appear the seller is located in the same country as the buyer, and the criminal then advises the victim to send money to a business partner, associate, sick relative, a family member, etc.

Money is typically transferred via wire transfers, leaving little recourse for the victim. The most recent trend is an increase in bank-to-bank wire transfers. Most significantly, these wire transfers go through large banks but are then routed to banks in other countries. Similarly, sellers also occasionally direct the victims to pay using phony escrow services. Sometimes they even hijack legitimate escrow websites to make themselves appear even more bonafide. Once the funds are wire transferred to the escrow website, the seller usually discontinues contact.

Another popular scheme is the passing of counterfeit cashier’s checks. This scheme targets people who use Internet classified advertisements to sell merchandise. Typically, an interested party contacts a seller. The seller is told the buyer has an associate in the victim’s country who owes him money. As such, he will have the associate send the victim a cashier’s check for the amount owed to the buyer. The amount of the cashier’s check is frequently thousands of dollars more than the price of the merchandise and the victim is told the excess amount will be used to pay the shipping costs associated with getting the merchandise to his location. The victim is instructed to deposit the check, and as soon as the funds are credited to their account, to wire the excess funds back to the criminal or to another associate identified as a shipping agent. Because a cashier’s check is used, banks typically release the funds immediately, or after a one or two day hold. Falsely believing the check to be genuine, the seller wires the money as instructed. Ultimately, the bank discovers the cashier’s check is fraudulent and removes these funds from the victim’s account.

Some people become unwitting accomplices of cyber criminals. Criminals post work-at-home job offers on popular Internet employment sites. These jobs are advertised as “financial manager” or “payment processor” positions. People who accept these positions are told to open bank accounts and provide the account numbers to their employers. They receive transfers to these accounts and are instructed to withdraw this money and transfer it (minus their commission, of course) to designated recipients in foreign countries. When approached by law enforcement, these people are often surprised to learn they have been playing the role of “money mule” for cyber criminals. By acting as a third party receiver of funds, these people have facilitated the transfer illegal proceeds directly to cyber criminals in foreign countries.

Although the threat posed by cyber criminals is real, through the use of a few basic Internet security practices and an awareness of the more common cyber criminal schemes, individuals can reduce their risk of becoming a victim. Users should remain aware of the latest online fraud scams, many of which are described at www.lookstoogoodtobetrue.com. However, if an individual believes he has already been the victim of a cyber crime, he should notify the appropriate law enforcement agency as soon as possible, and may file a complaint online from anywhere in the world at www.ic3.gov, a partnership between the Federal Bureau of Investigation and the White Collar Crime Center. Providing timely and thorough information detailing the particulars of the scheme and identifying characteristics of the criminals helps law enforcement develop an effective investigative strategy.

* Scot Huntsberry is a Supervisory Special Agent who most recently has been working for the FBI in the Cyber Division in Washington, D.C.

The FBI’s Cyber Division is dedicated to applying the highest level of technological capability and investigative expertise toward combating cyber-based terrorism, hostile foreign intelligence operations conducted over the Internet, and cyber crime. The work of the Cyber Division allows the FBI to stay one step ahead of the adversaries technologically threatening the United States. The Cyber Division addresses all violations with a cyber nexus, which often have international facets and national economic implications, and simultaneously supports FBI priorities across program lines, assisting counterterrorism, counterintelligence and other criminal investigations when aggressive technological investigative assistance is required.
As a boy playing football in Abidjan, Didier Drogba always dreamt that one day Africa would host the World Cup. Now that dream has finally become a reality.

Didier also dreamed of a prosperous, healthy and educated Africa. One that can be achieved through the eight Millennium Development Goals (MDGs), set by 189 world leaders back in 2000. While we have made significant progress, we still have a long way to go. Half the people in sub-Saharan Africa are still living in extreme poverty. An African woman dies in childbirth every two minutes and more than 15 percent of African children will not reach their 5th birthday.

As a UNDP Goodwill Ambassador, Didier wants you to team up with him against poverty and show your support for the Millennium Development Goals. Everyone is a player. While we are at the World Cup scoring goals in Africa, we need to work together to score goals for Africa.

To learn more about the MDGs and to spread the message. Visit www.undp.org/mdg
The shift from industrial societies to information societies, and the related dependence of the society as well as the economy on the availability of Internet services have moved the attention of politics towards the cybercrime topic. While in other emerging areas of crime it is possible to use traditional crime prevention and investigation strategies, the fight against cybercrime faces unique challenges that require a special attention from both investigators and lawmakers. This article provides an overview of some of those challenges.

1. Availability of tools and instructions to commit Cybercrime

In the early days of computer crimes, committing an offence required a significant amount of technical understanding. Nowadays however, offenders can commit cybercrimes by using software devices that do not require in-depth technical knowledge, such as software tools designed to locate open ports or break password protection. Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices that can potentially turn any computer user into a cybercriminal.

Furthermore, offenders can use the Internet to find instructions on how to commit crime, both online and offline. For example, the term “Googlehacking” (or “Googledorks”) describes the use of complex search engine queries to filter many search results for information on computer security issues. Several reports emphasised the risk of the use of search engines for illegal purposes. An offender planning an attack can find detailed information on the Internet explaining how to build a bomb by using only chemicals that are available in regular supermarkets.

2. Resources

Offenders can use sophisticated methods to increase their resources. An example of this is represented by botnet attacks such as those used in 2007 against computer systems in Estonia. An analysis of the attacks suggests that they were committed by thousands of computers within a “botnet,” a group of compromised computers running programs under external control. Over recent years, botnets have become a serious risk for cybersecurity. The size of a botnet can vary, from a few computers to more than a million computers.

3. Difficulties in tracing offenders

Although users leave multiple traces while using Internet services, offenders can hinder investigations, and in particular their identification, by resorting to special services. For example, if they use public Internet terminals that do not require identification, investigations will often falter. Offenders can also make use of open wireless networks to hide their identity. While difficulties in identifying Internet users have the potential to support democratic processes, they also go along with fears of abuse perpetrated by offenders.

4. Failure of traditional investigation instruments

An effective fight against terrorist use of the Internet requires Internet-specific tools that enable competent authorities to carry out investigations. In a growing number of Internet-related cases, traditional investigation instruments are not sufficient to identify an offender. One example is the interception of Voice-over-IP (VoIP) communication. In the last
decades, States have developed investigation instruments (such as wiretapping) that enable them to intercept landline as well as mobile phone communication. The interception of traditional phone calls is usually carried out through telecom providers. Applying the same principle to VoIP, law enforcement agencies would operate through ISPs and service providers supplying VoIP services. However, if the service is based on peer-to-peer technology, service providers may generally be unable to intercept communications, as the relevant data are transferred directly between the communicating partners. Therefore, new techniques, as well as the related legal instruments, might be needed.

5. Missing control instruments

The Internet was originally designed as a military network based on a decentralised network architecture that sought to preserve the main functionality intact and in power, even when individual components of the network were attacked. Carrying out investigations in this environment goes along with challenges, as the designer of the network did not include control instruments.

Recent trends to implement technology blocking access to websites are an approach to compensate the absence of control instruments. Norway, Sweden, Switzerland, the United Kingdom, Italy, China, Iran and Thailand are among those countries that require or encourage blocking access to illegal contents stored outside the country. While this in general seems like an example of the possibility of introducing control instruments, the ability of users to circumvent filter technology using encrypted anonymous communication services shows the limitation of such approach.

6. Transnational nature of the offence

The Internet is a good example of globalisation, with services generally available to all Internet users. As a consequence, many data transfer processes affect more than one country. If offenders and targets are located in different countries, cybercrime investigations require the cooperation of law enforcement agencies in all the countries affected, as national sovereignty does not permit investigations within different States territories without the permission of local authorities. The related formal requirements and time needed to collaborate with foreign law enforcement agencies often hinder investigations, which often occur in very short timeframes. Offenders may deliberately include third countries in their attacks to make investigation more difficult.

7. Independence of location and presence at the crime site

One constituting fact common to all types of cybercrimes is the fact that offenders do not need to be present at the same location as the victim. Offenders can therefore act from locations where there is either no effective legislation in place or it is not enforced. Preventing such “safe havens” has therefore become a key intention of international approaches in the fight against cybercrime.

8. Encryption technology

Another challenge is the use of encryption technology by offenders. Encryption is a classic example of a neutral technology, since as it is not only used to hinder investigations but also to prevent unauthorised access to information. It is therefore considered a key technical solution for ensuring cybersecurity. The latest operating systems offer the possibility to encrypt computer data with the click of a mouse, making it difficult for law enforcement agencies to break the encryption and access the data. It is uncertain to what extent offenders already use encryption technology to mask their activities, but it has been reported, for instance, that terrorists are already using encryption technology.

1 For more information on the information society see Masuda, The Information Society as Post-Industrial Society; Dutta/De Meyer/Jain/Richter, The Information Society in an Enlarged Europe; Maldoom/Mandsen/Sidak/Singer, Broadband in Europe; How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; Hornby/Clarke, Challenge and Change in the Information Society.
4 In order to limit the availability of such tools, some countries criminalise the production and offer of such tools. An example of such a provision can be found in Art. 6 of the European Convention on Cybercrime.
7 One example is the “Terrorist Handbook” – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.
13 This was as well highlighted by the drafters of the Council of Europe Convention on Cybercrime that contains a set of essential investigation instruments. The drafters of the report point out: “Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques” see: Explanatory Report to the Council of Europe Convention on Cybercrime No. 132. Regarding the substantive criminal law provisions related to Cybercrime see above: Article 6.1.
14 The term “Voice over Internet Protocol” (VoIP) is used to describe the transmission technology for delivering voice communication by using


18 For a brief history of the Internet, including its military origins, see: Leiner, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff, “A Brief History of the Internet”, available at: http://www.isoc.org/internet/history/brief.shtml


28 Sieber/Nolde, Sperrverfahren im Internet, 2008, page 55


36 This issue was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out: “States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies”. The full text of the Resolution, available at http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: “There should be no safe havens for those who abuse information technologies.”

37 Regarding the impact on computer forensic and criminal investigations, see: Huebner/Bern/Bern, “Computer Forensics – Past, Present And Future”, No.6.

38 With regard to the importance of encryption technology see: OECD Report on Background and Issues of Cryptography Policy, 2007; The importance of encryption is further highlighted by the fact that 74 per cent of respondents of the 2008 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: “2008 E-Crime Watch Survey”, page 1.

39 Regarding the consequences for the law enforcement, Denning observed: “The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception and respondents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating”. Excerpt from a presentation given by Denning, “The Future of Cryptography”, to the joint Australian/OECD conference on Security, February, 1996. Regarding practical approaches to recover encrypted evidence see: Casey “Practical Approaches to Recovering Encrypted Digital Evidence”, International Journal of Digital Evidence, Vol. 1, Issue 3.

ITU (International Telecommunication Union) recognizes that information and technology security are critical priorities for the international community. Cybersecurity is in everyone’s best interest and this can only be achieved through collaborative efforts. Cyber threat issues are global and therefore their solutions must be global too. It is vital that all countries arrive at a common understanding regarding cybersecurity, namely by providing protection against unauthorized access, manipulation and destruction of critical resources. ITU believes that in developing a solution one must identify all existing national and regional initiatives, in order to foster collaboration with its multiple stakeholders and avoid duplication of efforts. With its 191 Member States and more than 700 Sector Members, ITU is uniquely placed to propose a framework for international cooperation in cybersecurity and assist in tackling cybercrime.

The World Summit on the Information Society (WSIS), which met in Geneva in 2003 and in Tunis in 2005, called upon ITU to act as the sole Facilitator of Action Line C5, “Building confidence and security in the use of ICTs”. On 17 May 2007, ITU Secretary-General, Dr. Hamadoun I. Touré, launched the Global Cybersecurity Agenda (GCA) which is a framework for international cooperation aimed at enhancing confidence and security in the information society. A multi-stakeholder High Level Experts Group (HLEG) comprising of more than one hundred experts from Governments, Industry, International organizations, NGOs and academic institutions was established to further develop main goals, analyse current developments in all areas of cybersecurity and formulate proposals on possible long-term strategies and emerging trends in cybersecurity. In 2008, the HLEG put together the Global Strategic Report which provided recommendations on key steps forward for all five pillars of the GCA.

The GCA is built upon five strategic pillars, also known as work areas, and made up of seven main strategic goals. The Five Pillars/Work Areas:

1. Legal Measures
2. Technical and Procedural Measures
3. Organizational Structures
4. Capacity Building
5. International Cooperation

Legal Measures

To better understand the legal aspects of cybersecurity ITU has devised cybercrime legislation resources. With these resources, ITU is working to assist countries in moving towards harmonizing legal frameworks. This activity also addresses the ITU-D Study Group Q22/1 approach for organizing national cybersecurity efforts, highlighting that establishing the appropriate legal infrastructures is an integral component of a national cybersecurity strategy.

The ITU cybercrime legislation resources currently consist of two main deliverables, the ITU publication titled ITU Toolkit for Cybercrime Legislation and Understanding Cybercrime: A Guide for Developing Countries.
Global Cybersecurity Agenda (GCA)
A framework for international cooperation

Cyberthreats are real and global.
Join forces with ITU & IMPACT

Child Online Protection (COP)
Our children are our future

www.itu.int/cop
ITU- IMPACT Collaboration

As the world’s first non-profit comprehensive global public-private partnership against cyber threats, the International Multilateral Partnership Against Cyber Threats (IMPACT) is well positioned to assist partner countries, especially developing nations who are broadening their Internet capabilities.

On 3 September 2008, IMPACT and the ITU formally entered into a Memorandum of Understanding (MoU) in which IMPACT’s state-of-the-art Global HQ in Cyberjaya, Malaysia, effectively became the physical and operational home of the GCA. Under this landmark collaboration, IMPACT provides the ITU’s 191 Member States with the expertise, facilities and resources to effectively address the world’s most serious cyber threats.

The partnership provides:

• Real-time analysis, aggregation and dissemination of global cyber-threat information;
• Network Early Warning System (NEWS) and emergency response to global cyber-threats; and
• Training and skills development on the technical, legal and policy aspects of cybersecurity.

Current Deployment Status
Below is an alphabetical list of countries which have already joined ITU-IMPACT collaboration:

<table>
<thead>
<tr>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albania</td>
</tr>
<tr>
<td>Albania</td>
</tr>
<tr>
<td>Algeria</td>
</tr>
<tr>
<td>Armenia</td>
</tr>
<tr>
<td>Australia</td>
</tr>
<tr>
<td>Austria</td>
</tr>
<tr>
<td>Azerbaijan</td>
</tr>
<tr>
<td>Bangladesh</td>
</tr>
<tr>
<td>Benin</td>
</tr>
<tr>
<td>Brazil</td>
</tr>
<tr>
<td>Bulgaria</td>
</tr>
<tr>
<td>Burundi</td>
</tr>
<tr>
<td>Cameroon</td>
</tr>
<tr>
<td>Cape Verde</td>
</tr>
<tr>
<td>Costa Rica</td>
</tr>
<tr>
<td>Côte d’Ivoire</td>
</tr>
<tr>
<td>Djibouti</td>
</tr>
<tr>
<td>Egypt</td>
</tr>
<tr>
<td>Gabon</td>
</tr>
<tr>
<td>Ghana</td>
</tr>
<tr>
<td>Guinea</td>
</tr>
<tr>
<td>Malaysia</td>
</tr>
<tr>
<td>Montenegro</td>
</tr>
<tr>
<td>Morocco</td>
</tr>
<tr>
<td>Nepal</td>
</tr>
<tr>
<td>Niger</td>
</tr>
<tr>
<td>Nigeria</td>
</tr>
<tr>
<td>Nigeria</td>
</tr>
<tr>
<td>Palau</td>
</tr>
<tr>
<td>Panama</td>
</tr>
<tr>
<td>Peru</td>
</tr>
<tr>
<td>Portugal</td>
</tr>
<tr>
<td>Romania</td>
</tr>
<tr>
<td>Russian Fed.</td>
</tr>
<tr>
<td>Senegal</td>
</tr>
<tr>
<td>Seychelles</td>
</tr>
<tr>
<td>Sierra Leone</td>
</tr>
<tr>
<td>Singapore</td>
</tr>
<tr>
<td>Slovakia</td>
</tr>
<tr>
<td>Slovenia</td>
</tr>
<tr>
<td>Spain</td>
</tr>
<tr>
<td>Sri Lanka</td>
</tr>
<tr>
<td>Sudan</td>
</tr>
<tr>
<td>Surinam</td>
</tr>
<tr>
<td>Sweden</td>
</tr>
<tr>
<td>Syrian Arab</td>
</tr>
<tr>
<td>Rep.</td>
</tr>
<tr>
<td>Tanzania</td>
</tr>
<tr>
<td>Thailand</td>
</tr>
<tr>
<td>Togo</td>
</tr>
<tr>
<td>Tunisia</td>
</tr>
<tr>
<td>Uganda</td>
</tr>
<tr>
<td>United Arab</td>
</tr>
<tr>
<td>Emirates</td>
</tr>
<tr>
<td>Vatican</td>
</tr>
</tbody>
</table>

NOTE: BOLD - Countries that have verbally confirmed. The administrative process is in progress.

### Child Online Protection (COP)

Under the GCA umbrella, the ITU launched the Child Online Protection (COP) initiative in November 2008. The COP initiative has been established as an international collaborative network for action to promote the online protection of children and young people worldwide by providing guidance on safe online behaviour in conjunction with other UN agencies and partners. It addresses the legal, technical, organizational and procedural issues as well as capacity building and international cooperation.

Since its launch, COP has attracted the support and recognition of leaders and experts from around the world. More recently, the President of Costa Rica Mme. Laura Chinchilla accepted the invitation to be the Patron of this initiative.

The key objectives of the initiative are to:

1. Identify the key risks and vulnerabilities to children and young people in cyberspace;
2. Create awareness of the risks and issues through multiple channels;
3. Develop practical tools to help governments, organizations and educators minimize risk;
4. Share knowledge and experience while facilitating international strategic partnerships to define and implement concrete initiatives.

### Cybersecurity Gateway

The purpose of the ITU Cybersecurity Gateway is to provide an easy-to-use information resource on national, regional and international cybersecurity-related initiatives worldwide.

In today’s interconnected world of networks, threats can originate anywhere, and thus our collective cybersecurity depends on the security practices of every connected country, entity, business, and citizen. National and international cooperation is needed among those who seek to promote, develop and implement initiatives for a global culture of cybersecurity. Through the Cybersecurity Gateway, ITU aims to enable information access, dissemination and online collaboration among stakeholders working in cybersecurity and related areas. The Gateway provides a platform to share information between partners in civil society, the private sector, governments and international organisations working on enhancing cybersecurity. The ITU invites all interested parties to explore the vast resources and links available through the Cybersecurity Gateway and join in partnership with the ITU and others to build confidence and security in the use of ICTs. The Cybersecurity Gateway has been recently updated with a newer version.

### Conclusion

It is undeniable that ICTs form an integral part of society today and that they will continue to do so in the future, with the Internet connecting ever more parts of the world. ICTs are constantly evolving, progressing and improving many aspects of our lives. This also rings true for cyber threats as they are intrinsically linked to ICT evolution. The ITU is very serious towards its responsibility for WSIS Action Line C5, “Building confidence and security in the use of ICTs”, and is working hard to address the emerging challenges of the Information Society. The Global Cybersecurity Agenda as an international framework has helped ITU take a leadership role in both cybersecurity issues and in WSIS implementation. It has helped build awareness of ITU’s activities among experts within the field and won their commitment and ownership of the strategies developed by the HLEG.

The GCA continues onwards, forming partnerships and enabling ITU Sectors to implement these strategies through concrete activities. Much has been achieved but cybersecurity is a constantly evolving challenge, which needs to be continually addressed due to the ever changing nature of ICTs. ITU will persistently work to build confidence and trust to ensure a safe and secure cyber environment for all.

For more information log on to: www.itu.int/cybersecurity Contact: cybersecurity@itu.int
FORUM ON
"ILLEGAL ECONOMY, ORGANISED CRIME AND FINANCIAL GLOBALISATION"

Debates, seminars and concerts with
Pedro Paez, Moni Ovadia, Pierre Moukala, Jurgen Roth, Colette Kitoga,
Hans Nilson, Shane Enright, Jens Weinreich, Luigi Ciotti, Monica Frassoni,
Francesco Forgione, Michele Emiliano,
Nando Dalla Chiesa
and MEPs Rita Borsellino, Saro Crocetta,
Luigi De Magistris, Eva Joly

www.ole2010.org
Universal identification is portrayed by some as the holy grail of Internet security. Anonymity is bad, the argument goes; and if we abolish it, we can ensure only the proper people have access to their own information. We will know who is sending us spam and who is trying to hack into corporate networks. And when there are massive denial-of-service attacks, such as those against Estonia or Georgia or South Korea, we will know who was responsible and take action accordingly.

Any design of the Internet must allow for anonymity. Universal identification is impossible.

The problem is that it will not work. Any design of the Internet must allow for anonymity. Universal identification is impossible. Even attribution - knowing who is responsible for particular Internet packets - is impossible. Attempting to build such a system is futile, and will only give criminals and hackers new ways to hide.

Imagine a magic world in which every Internet packet could be traced to its origin. Even in this world, our Internet security problems would not be solved. There is a huge gap between proving that a packet came from a particular computer and that a packet was directed by a particular person. This is the exact problem we have with botnets, or pedophiles storing child porn on innocents’ computers.
Imagine a magic world in which every Internet packet could be traced to its origin. Even in this world, our Internet security problems would not be solved.

In these cases, we know the origins of the DDoS packets and the spam; they are from legitimate machines that have been hacked. Attribution is not as valuable as you might think.

Implementing an Internet without anonymity is very difficult, and causes its own problems. In order to have perfect attribution, we would need agencies - real-world organizations - to provide Internet identity credentials based on other identification systems: passports, national identity cards, driver’s licenses, whatever. Sloppier identification systems, based on things such as credit cards, are simply too easy to subvert. We have nothing that comes close to this global identification infrastructure. Moreover, centralizing information like this actually hurts security because it makes identity theft that much more profitable a crime.

And realistically, any theoretical ideal Internet would need to allow people access even without their magic credentials. People would still use the Internet at public kiosks and at friends’ houses. People would lose their magic Internet tokens just like they lose their driver’s licenses and passports today. The legitimate bypass mechanisms would allow even more ways for criminals and hackers to subvert the system.

On top of all this, the magic attribution technology does not exist. Bits are bits; they do not come with identity information attached to them. Every software system we have ever invented has been successfully hacked, repeatedly. We simply do not have anywhere near the expertise to build an airtight attribution system.

Implementing an Internet without anonymity is very difficult, and causes its own problems.

Not that it really matters. Even if everyone could trace all packets perfectly, to the person or origin and not just the computer, anonymity would still be possible. It would just take one person to set up an anonymity server. If I wanted to send a packet anonymously to someone else, I would just route it through that server. For even greater anonymity, I could route it through multiple servers. This is called onion routing and, with appropriate cryptography and enough users, it adds anonymity back to any communications system that prohibits it.

Attempts to banish anonymity from the Internet will not affect those savvy enough to bypass it, would cost billions, and would have only a negligible effect on security. What such attempts would do is affect the average user’s access to free speech, including those who use the Internet’s anonymity to survive: such as dissidents in countries violating human rights.

Mandating universal identity and attribution is the wrong goal. Accept that there will always be anonymous speech on the Internet. Accept that you will never truly know where a packet came from. Work on the problems you can solve: software that’s secure in the face of whatever packet it receives, identification systems that are secure enough in the face of the risks. We can do far better at these things than we are doing, and they will do more to improve security than trying to fix insoluble problems.

The whole attribution problem is very similar to the copy-protection/digital-rights-management problem. Just as it is impossible to make specific bits not copyable, it is impossible to know where specific bits came from. Bits are bits. They do not naturally come with restrictions on their use attached to them, and they do not naturally come with author information attached to them. Any attempts to circumvent this limitation will fail, and will increasingly need to be backed up by the sort of real-world police-state measures that the entertainment industry is demanding in order to make copy-protection work.

Just as the music industry needs to learn that the world of bits requires a different business model, law enforcement and others need to understand that the old ideas of identification do not work on the Internet. For good or for bad, whether you like it or not, there is always going to be anonymity on the Internet.

http://www.schneier.com/essay-308.html

This essay previously appeared in Information Security and in Forbes as the first half of a point-counterpoint with Marcus Ranum (counterpoint which can be found at http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1380347,00.html)

This article was republished with the author’s permission.
Improve Maternal Health

Millennium Development Goals

1. Eradicate extreme poverty and hunger
2. Achieve universal primary education
3. Promote gender equality and empower women
4. Reduce child mortality
5. Improve maternal health
6. Combat HIV/AIDS, malaria and other diseases
7. Ensure environmental sustainability
8. Develop a global partnership for development

You and I Can Make It Happen

Tel: 254 - 20 - 4453440 Fax: 254 - 20 - 4453444, Cell: +254 729 - 467197 Email: milleniumcampaign@undp.org Website: www.endpoverty2015.org
Over the coming years a crucial issue in dealing with cybercrime will be the delicate balance that must necessarily be struck between personal data protection, public order, and security. If the stellar growth in e-commerce in the last decade, was accompanied by increasing alarm about the attendant potential for fraud (from e-bay scams to credit-card cloning), the next ten years seem bound to be beset by the headaches of cloud computing: who knows what dormant dangers may be inadvertently aroused merely by surfing the web, even without posting personal data online, or using social networks (all of which are exposed to data mining)? In this specific context, given the enormous wealth and value of the information that can be gleaned from the hard drives of individual PCs, from mere web searches, not to mention electronic intercepts, digital forensics and cloud computing which will certainly play an ever more decisive role in criminal investigations. This trend, already underway, was recently most singularly highlighted in the capture of a fugitive member of the “N’drangheta” (a Mafia-type organization operating in Calabria), one of Italy’s 100 most-wanted criminals, arrested because he frequently logged on to his personal Facebook account using the nickname “scarface.”

Privacy vs. Security?
A Dilemma of the Digital Era

* Giuseppe Vaciago
A Dilemma of the Digital Era

Privacy ties, even if the information is revealed on the assumption that it does not prohibit “the obtaining of information revealed through the account, so as to analyze their content for information useful to law enforcement agencies.

The user profiles on Facebook or any other social network can be mined not only to reveal the account holder’s identity, but also to “intercept” all the chats, posts and data passing through the account, so as to analyze their content for information useful to law enforcement agencies.

It is, therefore, obvious that data must also be classified on the basis of whether or not they are accessible to the public. The need for such a distinction is all the more pressing given that, so far, it has received scant consideration at European level. The U.S. Supreme Court has held that “the Fourth Amendment does not prohibit “the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose.” If these principles are to be applied unmitigated in their present form to the emergent reality of Web 2.0, they would enable intelligence and law-enforcement agencies to indiscriminately mine all information posted on social networks.

According to the results of a survey of over 2,000 Canadian undergraduates by Toronto-based Ryerson University’s Privacy and Cybercrime Institute, young people overwhelmingly tend to believe that information shared over personal networks was automatically protected by a sort of “network privacy” that did not however extend to content posted on websites. In sharp contrast with this view, the same study found, businesses and academic institutions recognize no such notion and consider all information posted online, fully in the public domain and undeserving of protection.

As the online information that could prove useful for solving, fighting and thwarting crime continues to grow in both quality and quantity at a breathtaking pace, law-enforcement agencies are bound to increase their reliance on data-mining techniques. It is therefore urgent that at least the courts focus greater attention on the type and manner of acquisition of online data deemed admissible as evidence in criminal trails.

Lastly, as European data protection agencies have repeatedly pointed out, it is also important for users, both young and not-so-young, to take greater responsibility for the type of content they post on these “virtual private premises.”

Social networks and digital data in the public domain

Digital data useful for law-enforcement purposes, may be broadly divided into information identifying a suspect (IP Address), data retranscording the latter’s web-browsing history (server logs) and the content of the suspect’s online correspondence (electronic intercepts). This type of data is indispensable for identifying a person in the course of digital investigations. Although this kind of information is accessible, as a general rule, only on the basis of warrants, subpoenas or other discovery orders issued by the relevant authorities against Internet service providers, a great deal of the data in question may, in fact, be obtained indirectly through simple web searches.

Data must also be classified on the basis of whether or not they are accessible to the public

Corporations such as Intelius Inc., offer an impressive array of highly effective services, supplying, for a fee ranging from $1 to $10, information on each and every US citizen, including residential address, fixed-line and cell phone numbers, e-mail address, criminal records, creditworthiness, employment history and level of education.

Date Check, one of Intelius’ cell-phone supported services, for instance, provides users with a full profile of potential dates, with nothing more to start with than their telephone number. The information offered includes not only personal data, but also the target’s criminal record, if any, as well as his or her earnings and assets, academic qualifications, and most crucially, current marital status, all delivered in a matter of seconds and a few clicks on users’ mobile handsets, so as to help them decide whether to start or continue a romantic relationship.

Intelius Inc. states on its website that all the information it provides is gleaned from public records: if true, this means that public data placed online on a daily basis, holds the keys to a vast variety of significant information which, until very recently, was considered beyond the reach of prying eyes. The user profiles on Facebook or any other social network can be mined not only to reveal the account holder’s identity, but also to “intercept” all the chats, posts and data passing through the account, so as to analyze their content for information useful to law enforcement agencies.

It is, therefore, obvious that data must also be classified on the basis of whether or not they are accessible to the public. The need for such a distinction is all the more pressing given that, so far, it has received scant consideration at European level. The U.S. Supreme Court has held that “the Fourth Amendment does not prohibit “the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose.” If these principles are to be applied unmitigated in their present form to the emergent reality of Web 2.0, they would enable intelligence and law-enforcement agencies to indiscriminately mine all information posted on social networks.

According to the results of a survey of over 2,000 Canadian undergraduates by Toronto-based Ryerson University’s Privacy and Cybercrime Institute, young people overwhelmingly tend to believe that information shared over personal networks was automatically protected by a sort of “network privacy” that did not however extend to content posted on websites. In sharp contrast with this view, the same study found, businesses and academic institutions recognize no such notion and consider all information posted online, fully in the public domain and undeserving of protection.

As the online information that could prove useful for solving, fighting and thwarting crime continues to grow in both quality and quantity at a breathtaking pace, law-enforcement agencies are bound to increase their reliance on data-mining techniques. It is therefore urgent that at least the courts focus greater attention on the type and manner of acquisition of online data deemed admissible as evidence in criminal trails.

Lastly, as European data protection agencies have repeatedly pointed out, it is also important for users, both young and not-so-young, to take greater responsibility for the type of content they post on these “virtual private premises.”

Data retention and Digital wiretapping: US and Europe have adopted two different approaches

Besides playing a crucial role in digital investigation, IP addresses can also be used to profile users for commercial purposes, especially in combination with cookies, as underscored in the recent European e-privacy Directive (2009/136/EC). In 2008, the German data protection commissioner, Peter Schaar, who headed the Article 29 Data Protection Working Party (comprising all European privacy authorities), expressed the view that IP addresses constitute personal data, and as such, are protected under the European e-privacy Directive.

The online information that could prove useful for solving, fighting and thwarting crime continues to grow in both quality and quantity

His remarks sparked a lively debate with certain US corporations which argued, on the contrary, that since an IP address did not, in itself, identify the user, so it could not be deemed personal information meritorious of protection under privacy regulations.

Torn between demands from European data protection authorities and US privacy rights groups to curtail data retention on the grounds that corporations like Microsoft, Google and Yahoo currently store far too much identification data for
Far too long, on the one hand, and calls by law-enforcement agencies for even more data be stored for ever longer periods of time, on the other, ISPs are at a loss to decide which direction to take.

Although Europe has opted for highly detailed data retention regulations (Directive 2006/24/EC, Article 5 states that IP addresses and server logs may not be stored for less than six months or more than two years), the issue is by no means settled. Calls for similar regulations in the U.S. were met with vigorous opposition and loud protests by both the EPIC (Electronic Privacy Information Center) and the EFF (Electronic Frontier Foundation).

There was no dearth of criticism in Europe either: Article 29 of the Working Party’s document entitled “The Future of Privacy” noted that the Directive not only lacked some adequate and specific safeguards as to the treatment of communication data, including provisions requiring an indication of the purposes for which the data are stored, or of the persons and parties authorized to access the retained information, but also failed to clarify the types of data that may in no event be lawfully stored or retained by ISPs and connectivity providers.

Recently, the German Constitutional Court outlawing the national legislation on mass storage of telephone and web traffic data, passed in implementation of the Directive. The practical repercussions of this scenario are clear: when dealing with an ISP in a jurisdiction bereft of data retention regulations, such as the U.S., or Germany, law-enforcement officers could never be sure if the information they seek has long been cancelled or is still in storage and admissible as evidence.

Electronic interceptions of online communications are even greater cause for concern in terms of privacy protection, than merely identifying a user and perusing his/her web-browsing history. Unlike phone calls, e-mails can be immediately indexed using specific tags, and often contain exceedingly useful attachments as well as other information shedding light on the context of the exchange.

The fact that electronic intercepts make it possible to glean information which is undeniably more useful than that obtained from telephone wiretaps does not seem to foster forms of transnational cooperation that are more effective than the bilateral instruments on mutual legal assistance currently in force. This issue is particularly delicate since the world’s largest “holders” of digital information are US-based corporations.

In a comment made at the 2001 Cybercrime Convention (which was also ratified by the United States), the Council of Europe laconically presented the issue of a Party permitted to unilaterally access computer data stored in another Party without seeking mutual assistance, stating that such a case is particularly complex and could not be resolved “in part (...) due to a lack of concrete experience with such situations to date.”

Conclusions

While this article is intended to highlight the differences between the European and US approaches to privacy rights and public order and security, and to spark further research and debate on the issues involved, it does however lead to three preliminary conclusions.

First and foremost, there are no winners or losers in the efforts to strike a balance between personal rights and public order and security, as these two following examples illustrate. On the one side, Europe adopted a data retention policy necessitating clearer definitions of the types of offences in connection to which stored personal data may be subjected to disclosure. On the other side, during the Bush administration the National Security Agency struck a deal with the main national telecommunications carriers to set up a database of the records of all the phone calls and online activities of American citizens.

Secondly, the EU-US joint statement released in Washington on 28 October 2009, as well as the Stockholm Program of 2 December 2009, are and must be treated as urgent calls for the active implementation of the Cybercrime Convention. Without wishing to belittle the importance of this Convention, however, it is clear that in an area such as Internet which connects the entire world, Intergovernmental Organisations also need to intervene, endeavouring to include as many countries as possible.

The huge potential of the Internet cannot be exploited merely to keep in touch with old classmates or make free video calls to family and friends

The third and last conclusion is more of a hope: the huge potential of the Internet cannot be exploited merely to keep in touch with old classmates or make free video calls to family and friends. It is precisely as a result of the global interconnectivity it offers, allowing people from different countries and backgrounds to share information and exchange ideas, that the Internet must serve as the starting point for setting up a framework of rules that reconciles privacy protection with the public interest in detecting, investigating and preventing crime both online and offline, in a manner satisfactory to all. We managed to draw up the Universal Declaration of Human Rights without the benefit of the Internet as a universal instrument of peace. Imagine what we can now do, with it.

* Giuseppe Vaciago is a lecturer in IT Law at University of Milan, focusing his research on cybercrime and computer forensics.
The biggest problems in discussing cyberwar are the definitions.

There are many things described as cyberwar that are really cyberterrorism, and the things described as cyberterrorism are more like cybercrime, cybervandalism or cyberhooliganism - or maybe cyberespionage. At first glance, there is nothing new about these terms except the “cyber” prefix. War, terrorism, crime, and vandalism are old concepts. What is new is the domain; it is the same old stuff occurring in a new arena. But because cyberspace is different, there are differences worth considering.

Of course, the terms overlap. Although the goals are different, many tactics used by armies, terrorists, and criminals are the same. Just as they use guns and bombs, they can use cyberattacks. And just as every shooting is not necessarily an act of war, every successful Internet attack, no matter how deadly, is not necessarily an act of cyberwar. A cyberattack that shuts down the power grid might be part of a cyberwar campaign, but it also might be an act of cyberterrorism, cybercrime, or even - if done by some 14-year-old who does not really understand what he is doing - cyberhooliganism. Which it is depends on the attacker’s motivations and the surrounding circumstances, just as in the real world.

For it to be cyberwar, it must first be war. In the 21st Century, war will inevitably include cyberwar. Just as war moved into the air with the development of kites, balloons, and aircraft, and into space with satellites and ballistic missiles, war will move into cyberspace with the development of specialized weapons, tactics, and defenses.

I have no doubt that smarter and better-funded militaries are planning for cyberwar. They have Internet attack tools: denial-of-service tools; exploits that would allow military intelligence to penetrate military systems; viruses and worms similar to what we see now, but perhaps country-specific; and Trojans that eavesdrop on networks, disrupt operations, or allow an attacker to penetrate other networks. I believe militaries know of vulnerabilities in operating systems, generic or custom military applications, and code to exploit those vulnerabilities. It would be irresponsible for them not to.

The most obvious attack is the disabling of large parts of...
SPEAK OUT
AGAINST DISCRIMINATION

ALL DIFFERENT
ALL EQUAL

Council of Europe campaign

www.coe.int/antidiscrimination
the Internet, although in the absence of global war, I doubt a military would do so; the Internet is too useful an asset and too large a part of the world economy. More interesting is whether militaries would disable national pieces of it. For a surgical approach, we can imagine a cyberattack against a military headquarters, or networks handling logistical information. Destruction is the last thing a military wants to accomplish with a communications network. A military only wants to shut down an enemy’s network if it isn’t acquiring useful information. The best thing is to infiltrate enemy computers and networks, spy on them, and surreptitiously disrupt select pieces of their communications when appropriate. The next best thing is to passively eavesdrop. After that, perform traffic analysis: analyze the characteristics of communications. Only if a military can not do any of this would it consider shutting the thing down. Or if, as sometimes but rarely happens, the benefits of completely denying the enemy the communications channel outweigh the advantages of eavesdropping on it.

Cyberwar is certainly not a myth. But you have not seen it yet, despite the attacks on Estonia. Cyberwar is warfare in cyberspace. And warfare involves massive death and destruction. When you see it, you will know it.

http://www.schneier.com/essay-201.html

This essay first appeared on Information Security as the second half of a point/counterpoint with Marcus Ranum (which can be found at http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1280052_id1,00.html)

This article was republished with the author’s permission.

* Bruce Schneier is an internationally renowned security technologist and author. Described by The Economist as a “security guru”, he is the author of Applied Cryptography, Secrets and Lies, Beyond Fear and Schneier on Security. Regularly quoted in the media - and subject of an Internet meme - he has testified on security before the United States Congress on several occasions and has written articles and op eds for many major publications, including The New York Times, The Guardian, Forbes, Wired, Nature, The Bulletin of the Atomic Scientists, The Sydney Morning Herald, The Boston Globe, The San Francisco Chronicle, and The Washington Post. Schneier also publishes a free monthly newsletter, Crypto-Gram, with over 150,000 readers. In its ten years of regular publication, Crypto-Gram has become one of the most widely read forums for free-wheeling discussions, pointed critiques, and serious debate about security. Schneier is the Chief Security Technology Officer of BT. More from the author can be found at www.schneier.com
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.

* Marc Goodman

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.
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. 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 MMOG’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.

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. 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.

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.

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.

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-
The project was launched thanks to the presence in Turin of important organisations of the UN System and of the European Union devoted to training, research and technical assistance.

The Turin international Summer School is organised by the European Training Foundation (ETF), the United Nations Interregional Crime and Justice Research Institute (UNICRI), the International Training Centre of the ILO (ITC-ILO), the Faculty of Law of the University of Torino and the University Institute of European Studies (IUSE).

The Turin International Summer School aims to provide to participants specific knowledge on economic, legal and social aspects related to immigration flows within the EU system.

Turin International Summer School Course Secretariat
University Institute of European Studies
Via Maria Vittoria, 26 10123 – Torino (Italy)
Ph: +39.011.8394660

summerschool@iuse.it http://summerschool.iuse.it/
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 currencies 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. 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-
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.

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
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. 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 griefer 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.

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 exchange 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 griefing 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. 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 offenses 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


4. http://motherjones.com/politics/2007/05/even-better-real-thing


Most governments and founding charters originated at least 200 years ago: the United States Constitution (which then also served as a basis in most Latin American countries), and democratic governments such as those of the United Kingdom and France. Moreover, the concept of democracy is even older than that, dating back to the ideas of Socrates, Plato and Aristotle.

Cybernetics, however, which is literally the science of government as it studies the structure of regulatory systems, is only about 63 years old. Many years ago I asked myself: What are current governments doing right or missing? What does Cybernetics have to do with the world of Law, given that laws are about controlling people’s behaviour?

Rather than telling you the long-winded story, I want to “infect” you with a quick and valuable insight and an example of my findings.

If you think that “systems” have been around for a long time and that they have had their chance to make their impact on the world, please reconsider. Reductionist thinking has become so engrained in our culture that it has become invisible. We think that just because we are able to take things apart, we know how they work. Complex systems though are inherently tricky.

Systems thinking, the process of analyzing and understanding how things work and how they influence each other, is something absolutely necessary when designing a government, otherwise it just won’t work. I learned about management cybernetics (the science of managing organizations) under Stafford Beer’s guidance, who first introduced this concept of analyzing management and organizations in the late 1950s. I discovered with great joy for instance, that the American Constitution can be mapped in detail by his Viable System Model (VSM). Stafford built this model after standing on the shoulders of the giants of cybernetics such as Norbert Wiener, W. Ross Ashby and others.

* Javier Livas
The modern state is a highly complex system. Stafford Beer discovered that nature and living things seem quite multifarious, but not as much as they would appear to be. Nature’s secret for creating complexity is a little magic trick called recursiveness, of which the human body is the best and closest example: cells, tissues, organs, each of these are a living entity working together as one. Living things have evolved thanks to genetic evolution. Ideas and concepts evolve too. Lately, we speak about memes (copiable packages of information), and about memetic evolution, which results from meme mutation. Brains or minds copy memes and change them; the amount of copying done by autonomous agents depends on the meme’s usefulness. Democracy, for instance, was a meme originally created by the Greeks, but it has come to mean many other things now. Legal solutions and institutions are memetic super packages. They are meme complexes that have evolved slowly: from Greece to the Middle Ages, through the Industrial Revolution, and the Atomic Era.

If you research what a legal system is, you will find it defined as a system of rules, or norms or some other kind of order, but you are never referred to its ultimate essence: information. The legal realm is a world of guidelines with which to govern. Laws and constitutions are like instruction manuals telling people what to do in many different situations. As such, they resort to previous agreements, such as the meanings contained in a dictionary, in order to be understood and obeyed.

The Viable System Model (VMS) explains in great detail how several systems connect to one another to create a greater one, a whole which emerges from simpler parts and can do things that the individual components cannot do themselves. Building these connections and communication lines is what the law has been doing for many centuries now. Furthermore, emergence is what makes a system behave consistently. Businesses use the holistic synergy (2+2=5) to signify that the whole is greater than the sum of its parts. Cybernetics was born as a strictly mathematical science, using sophisticated statistical methodologies discovered by Norbert Wiener when he was studying Brownian motion in gases (the seemingly random movement of gas particles imagine and yet, somehow, control and an ordered society manage to make its way through. This is thanks to the facts that laws have evolved following certain cybernetic control principles intuitively. This is not a small merit of the legal system. Therefore, if we opt for redesigning governance, we can do so with a very clear knowledge of how not to produce unwanted side effects. We can map the interactions and identify the positive and negative control loops. Positive feedback is like the acceleration made possible by a car’s engine, while negative feedback is used for control, such as the brakes and the steering wheel. Legal systems use circular causality, even if lawyers do not identify it as such. For instance, the legislative process is an example of a circular causality system. It is assumed that laws are not approved to work forever: lawmaking presupposes the need to go back and adapt legislations to the changing circumstances. These are clearly cybernetic mechanisms at work.

When I say that Law has discovered the VSM without any knowledge of cybernetics it is because trial and error leads to solving governance problems and, eventually, a system of checks and balances has proved to be a wise solution. Well, checks and balances is another word for homeostats, which nature uses to get results while maintaining an internal stability. What many people have not noticed is that legal systems use contradictory values to balance the performance of the system. Some jurists are aware of the contradictions within the process, which can imply assumptions such as: justice is the enemy of certainty; liberty is the enemy of order and so on. Lawyers are proud users of Aristotelian logic, the syllogistic logic of “All men are mortal; Socrates is a man; therefore Socrates is mortal.” This is the supreme
tool of the legal process, also used in defining the burden of proof.

However, what may seem as a chain of syllogistic reasoning could create an aberration. Consider the rules of “probable cause,” which have degenerated into a bureaucratic mess that hinders the expedition of search warrants. Why not use a more systemic approach to the problem? What if several neighbours were given the power to request a police search? Individuals do not have “requisite variety,” but the neighbourhood “system” does! Peer monitoring by neighbours would, for instance, dissuade the existence of crack houses. Has the Law realized that making finer and finer distinctions creates exactly the opposite effect?

Law has not used the power of dispersed information. Our ideas of individuality do not allow the current system of justice to know what is going on. A family knows its members better than any police ever will. Why not tap into this wealth of information? We disapprove the public lashing of graffiti violators in certain countries, but the truth is that the very existence of the rule produces a behaviour that seldom requires the punishment to take place at all! If you compare this to the high occurrence of rapes in some countries’ prisons, we can deduce that it is not the severity of the crime per se that determines the frequency of said crime, but it is instead the entire system variables that affect the behaviour of the potential perpetrators.

Another “systemic solution” is the way the Iroquois, an indigenous tribe in North America, fought the unwanted behavior of their members. They sat the culprit in the middle of the tribe assembly and said: “We are going to do nothing and stay here until you convince us that you have repented because your behavior is something we cannot live with.” This social pressure and the resulting bonding produced a society with virtually no crime! The Iroquois did not have jails, and those that repeated extreme cases of disobedience were declared “invisible,” which meant that nobody could ever speak to them again or help them in any way. Without the tribe’s support they would usually die or be killed by enemy tribes. Therefore we must look “at the whole” system before making choices.

Living systems are awash with paradoxical situations. Cybernetics embraces paradoxes such as homeostatic checks and balances. The final analysis should answer the question: is the system doing what we want it to? Is filling jails with two million people the purpose of the system? This is what the complex system does. We can change that through the use of the systems’ knowledge.

It is sad that defenders of minorities do not have their cybernetics in place. As they demand more and more safeguards of individual rights, they are giving proof of the counterintuitive nature of complex systems.

Corruption is, for instance, a very important component in the system’s performance and it can generate errors which negatively impact the communities in their functioning and in their daily lives.

Take note that I have said nothing here about those attorneys and judges’ self-interested role in perpetuating the mess. My analysis does not take into account the role played by those taking advantage of the perpetuation of this mess for self interest or political gain. Corruption is, for instance, a very important component in the system’s performance and it can generate errors which negatively impact the communities in their functioning and in their daily lives.

For more information on the topic, see Law & Cybernetics on YouTube.

* Javier Alfredo Livas Cantú is an attorney with an MBA from ITESM (Monterrey Tech). Has spent most of his time as a political activist for democracy and freedom in Mexico, and as an attorney with legislative initiatives to change laws regarding civil procedures, transparency and elections. Livas is an expert in cybernetics, a discipline first applied to management by the British cybernetician Stafford Beer. He is the author of many books, among which Cibernética, Estado y Derecho, The Cybernetic State, Más allá de la Psicocibernética, el Libro del Poder Personal, Batallas por la Democracia. He has also been writing a weekly political column in El Norte newspaper for more than 25 years and has published more than 50 videos on YouTube.
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’

We are all citizens of the same World
Please stand up for justice and equality
For decades, the international community’s approach to issues of nuclear proliferation on the one hand, and of the use of criminal law mechanisms on the other, has hardly been an integrated one. In the post-Cold War environment, the events of 9/11 have acted as a powerful catalyst for change. The conceptual borders within which these two areas (nuclear proliferation and criminal law) were “locked” have been challenged. However, only recently has this change begun to be reflected in specific international legal instruments.

Two major changes, closely linked to each other, have contributed to explain the convergence:

a) **First major change:** non-State actors are increasingly perceived as having the potential to become fully fledged “nuclear proliferators,” in the same way as State entities. It is true that some legal instruments adopted during the Cold War, such as the 1979 Convention on the Physical Protection of Nuclear Material, require the criminalization of certain conducts involving the unlawful handling and theft of nuclear material. It was certainly recognised that such material may fall into the hands of individuals for malevolent purposes, including terrorist ones. However, the overall consensus at that time was that only States would be capable and/or willing to manufacture and use nuclear weapons.

This is evident in the language of the only multilateral legal instrument which continues to represent the cornerstone of global nuclear non-proliferation efforts: the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT). One of the core requirements of the NPT is the prohibition for non-nuclear-weapon States (NNWS) to receive nuclear weapons, and a corresponding prohibition for nuclear-weapon States to carry out such transfers to NNWS. (In a nutshell, “nuclear proliferation” can be defined as the spread of nuclear weapons to States that did not previously possess them, i.e. “horizontal proliferation”, and the increase in the number of weapons by States already possessing them, i.e. “vertical proliferation”).

In a nutshell, “nuclear proliferation” can be defined as the spread of nuclear weapons to States that did not previously possess them, i.e. “horizontal proliferation”, and the increase in the number of weapons by States already possessing them, i.e. “vertical proliferation”.

* Stefano Betti
When the NPT was adopted, it was simply unthinkable that individuals acting outside State direction could ever gather the high level of skills and technological awareness necessary to pose a serious and direct global threat. Crucially, the NPT lacks a provision equivalent to the ones contained in more recent non-proliferation instruments, such as the Chemical Weapons Convention, which requires that activities prohibited for States Parties also be the object of a prohibition for natural or legal persons acting on their territory. The events of 9/11 suddenly brought to the attention of the world community a new possibility: criminal organisations could develop an autonomous capacity to acquire, manufacture, use and threaten to use nuclear weapons. Intelligence reports started to document attempts by the Al-Qaeda network to come into possession of nuclear materials and the know-how. Osama Bin Laden has even been reported stating that the acquisition of weapons of mass destruction constitutes a religious duty. In 2002, the UN General Assembly adopted the first of a series of resolutions on “Measures to Prevent Terrorists from Acquiring Weapons of Mass Destruction.” In this process, Resolution 1540 can be considered a landmark instrument since, for the first time, the Security Council used its prerogatives under Chapter VII of the UN Charter to entrench a requirement for all States to “prohibit any non-State actor to manufacture, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as accomplice, assist or finance them” (para.2).

**b) Second major change:** International criminal law is increasingly being used to control nuclear proliferation. Resolution 1540 has provided the political impetus and legal framework for the adoption of the 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005 SUA Protocol). Whereas the original 1988 SUA Convention deals exclusively with direct threats to a ship and its passengers (taking the Achille Lauro case as the paradigmatic situation), the new Protocol goes well beyond the goal of strengthening maritime security. By defining new offences of transporting nuclear weapons and related materials in violation of the NPT’s legal framework, it promotes criminal law as a central element in the global non-proliferation effort and recognizes the dangers posed by non-State actors beside “traditional” State-driven proliferators. The technical complexity of the new legal regime, merging criminal law, nuclear law and the law of the sea, reflects an attempt to face an increasingly intricate and volatile security environment.

What are the implications of the new approach, and what developments can be expected in the next few years? Although it is impossible to make predictions, some trends can already be anticipated. First of all, the 2005 SUA Protocol is set to enter into force at the end of July 2010 (having now been ratified by twelve States). Although many more instruments of ratification will have to be deposited before the Protocol can achieve the sort of “universal character,” a pre-requisite for its usefulness as a truly global cooperation platform, the focus of the international community will gradually move to issues of implementation. The multidisciplinary nature of the new legal regime will require that domestic agencies acquire a particularly high level of specialization for the purpose of incorporating international standards into domestic legal systems and enabling the law enforcement community to act effectively. The innovative approach taken in the 2005 SUA Protocol is not going to remain an isolated case. In August this year, a Diplomatic Conference under the aegis of the International Civil Aviation Organization is set to amend the existing international legal regime governing illicit acts affecting civil aviation. As things stand now, it is likely that new instrument(s) will envisage a central role for criminal law in the area of transport of nuclear weapons and materials (as well as other weapons of mass destruction) by air. Consequently, lessons learned during the implementation phase of the 2005 SUA Protocol may facilitate the understanding of similar provisions in the field of civil aviation.

Several international agencies will have to play a leading role in promoting acceptance and understanding of the new approach, and they will have to do so as a joint endeavor. Natural candidates are the International Maritime Organization, the International Atomic Energy Agency and the United Nations Office on Drugs and Crime. The need to achieve better coordination among international bodies in delivering technical assistance, particularly to developing countries, will become more and more pressing. Handling the complex security environment of the 21st Century will make it inevitably necessary for deeds to follow words.

* Stefano Betti, Terrorism Prevention Expert, United Nations Office on Drugs and Crime (UNODC). The views contained in this paper do not necessarily reflect those of the United Nations.*
Once upon a time there was journalism. Many have recited the *de profundis* for the reporting profession over the last few years. Because of the economic crisis, which has been stifling newspapers for the last two years. And before that, in an even more substantial way, because of how conflicts in the post 9/11 world have changed the way of telling History and the stories of those who are called upon to cover them.

In the future, journalism handbooks will still exist, along with the profession itself. They will still be written, perhaps not on paper, but, in my opinion, they will nevertheless be published digitally and read on Kindle. These manuals of the future will dedicate an important chapter to that sunny morning in Manhattan: 9/11 changed the world as we knew it, but it also changed journalism.

Until that day, the men and women with notebooks had lived in a sort of limbo: the pen and the recorder had almost always granted them a sort of immunity and a form of respect, albeit vague, from the factions in conflict. This, however, did not always work: during the fifteen years of bloody civil war in Lebanon, saying *sahafie* (journalist) at checkpoints wasn’t enough to avoid being stopped and taken hostage, sometimes even for years. Nevertheless, these cases were always conceived as marginal ones that did not tarnish the overall concept of immunity.

* Francesca Caferrì
However, everything changed with the wars in Afghanistan and Iraq: journalists slowly understood that the press label wasn’t enough, that the guarantee of impartiality was no longer the same, and that even those who took sides with the “victims” (the civilian population in those countries) were no longer safe. That was because they were recognized as westerners first and journalists later: they were therefore, by definition, either targets for revenge or sources of economic revenue. Many colleagues from notorious newspapers have lost their lives in this context, Corriere della Sera and El Mundo lost Maria Grazia Cutuli and Julio Fuentes; but papers typically associated with leftist and anti-war ideologies were also affected, such as Manifesto’s Giuliana Sgrena and Libération’s Florence Aubenas, who were kidnapped and held hostage for several weeks.

It was therefore almost natural for colleagues to resort to a type of journalism that has been forcefully establishing itself: embedded journalism. This American expression has been applied to reporters travelling with military units, following them everywhere and reporting their work, taking advantage of the security bubble that they (sometimes) offer. In 2006, embedded journalism was basically the only type that had survived in Iraq, telling us of the battle of Fallujah and of the bloodsheds that brought the country on the verge of a civil war.

In those months, many criticized the media accusing it of a lack of objectivity, and many took up the cudgels in its defence. I believe that the ultimate answer was given by Kevin Sites, an embedded correspondent for NBC who had filmed a group of marines shooting the final rounds against a wounded insurgent in a mosque in Fallujah. The footage was aired, provoking outrage and making a few heads roll. The journalist was overwhelmed by criticism: many accused him of having betrayed the pact that had bound him for weeks to the troops he was embedded with, who had fought to save his life too, just to be then paid back with that video. Sites defended himself, explaining that the real pact was the one he had with his job: telling reality without filters or constrictions. And in that case, reality was represented by those deadly shots against a wounded man lying on the ground.

In my opinion, that reporter saved the soul of today’s journalism, demonstrating that the press can benefit from the troops’ protection to reach areas otherwise inaccessible, but that this does not necessarily imply embracing the military’s point of view on everything. This lesson is far too frequently forgotten (particularly in the Italian context, which is the one I know best) in favour of a more servile and slovenly way of reporting: one that is not very useful to the writers, to the sources or to the readers, and one that runs the serious risk of proving right the doomsday prophets of the demise of journalism.

* Francesca Caferri is Vice-Editor (World affairs section) of La Repubblica, one of the main Italian newspapers. She has provided extensive coverage on the Middle East, USA, Africa, Europe and Latin America, specializing in development issues and major international events, with an emphasis on the Middle East. Previously, she has also worked for CNN covering humanitarian issues, international organizations and European Union issues. Francesca Caferri is a Professor of International Organizations and Foreign Affairs. In 2005 she was awarded the highest prize for Italian journalists (Saint Vincent Journalism Prize) for reporting from Cuba during the first meeting of the Cuban opposition.

Translated by Olivia Jung, UNICRI
I decided to write a book in the summer of 2009 when the Italian government started intercepting and turning back migrants at sea. I thought it would have helped me analyze what has been going on these years and what is not happening nowadays.

Despite the apparent calm that was looming over the waters of the Mediterranean in the absence of disembarkments, apprehension still arose from the many stories of the men and women who had reached, one after the other and throughout the years, the Favarolo dock of Lampedusa and the southern coasts of Italy.

Those stories echo in my ears, hindering me from finding even just a single positive aspect of the “pushbacks” in high waters. All back, the same solution was applied to all of them: indiscriminately pushed back regardless of the individual causes behind their escape. A single offhanded sentence without appeal. Notwithstanding if you are in the middle of the sea because your country is torn apart by war, or if you are in a rubber dinghy because staying at home would have meant being tortured.

On this side of the Mediterranean, the distinctions are no longer taken into account. And the reaction of a substantial portion of the public opinion applauding this initiative without considering the price paid by those migrant also makes me feel uneasy. Those pushed back, including the children, end up in detention centres in Libya, where they remain for months or perhaps years, without having committed any crime whatsoever. They are only human beings who do not have the privilege of living at home and who have to look for peace and security elsewhere. Moreover, those returned also run the risk of being sent back further south, in the middle of the desert. How can we agree with all this?

Very few of the stories of the many men and women I have met throughout the years working as a spokesperson for the United Nations High Commissioner for Refugees (UNHCR) are devoid of suffering. The condition of person on the run is almost never resolved without traumas. Most of these people endure a genuine ordeal of pain and solitude. But it is not necessarily the cruelest stories that have left...
more of a mark in my mind. There are situations where someone else’s anguish is so overwhelming that it is hard even for the listener to contain it. This transposed sense of malaise can be comforted only with a concrete action to help those people, to instill in them a glimmer of hope in the future. Humankind’s suffering is not something that one can get used to. Going back through the years, my memory takes me to Afghanistan, one of the most spectacular places on the planet. A place where you can perceive the intolerable dissonance between nature’s beauty and the horrific stories told by women annihilated by violence; the immaculate white peaks of the Hindu Kush and the nefarious crimes perpetrated against entire generations of women and girls, silent and invisible. From the Balkans, the images impressed in my mind are those of the elderly kicked out of the hospitals in Kosovo and transported in hand-carts by their relatives through impervious mountain paths under the pouring rain. In pain and quiet are the aghast looks of those seniors who would have died rather than endure that tribulation, or the looks of those skeletal prisoners released at a frontier post after having been used as human shields to protect the enemy’s military posts. It is also difficult to forget the long lines of Eritrean women and children, enveloped in the sandy winds overshadowing the sky. After walking for hours under the implacable sun and blistering temperatures reaching 50°C (122°F), they arrive exhausted and parched at the first refugee camp of Kassala, just beyond the Sudanese border. A few years later, other stories of refugees, this time told in Italy, opened my eyes on the ultimate frontier of desperation. They revealed an actual Russian roulette managed by smugglers of human beings, the real warlords of the war fought in the Mediterranean. Being forced on a ramshackle rubber dinghy or on a fiberglass skiff to cross the 160 miles separating Libya from Lampedusa basically means being willing to pay the ultimate price. But, when you are without papers, or without an entry visa for a safe country, you have no choice. But what do we know of these people and of their arduous existence? In my opinion, not enough. In the media, and consequently in the public opinion, those arriving from the sea are commonly and hastily called “illegal aliens” (or, in Italian, clandestini). It is a term loaded with prejudice, a word evoking something dangerous that has to hide from justice, even though most of the people arriving on the Italian shores are seeking asylum. This is why I consider each of these stories a legacy handed over to me, an extremely valuable patrimony in which to invest constantly through my work. Refugees do not have the privilege of living at home, and many of them wish to return there as soon as possible. When migrants are repatriated, either because they entered or are staying in the country irregularly, they do not run the risk of being imprisoned, tortured or killed; at most, they can incur in some sanction, but nothing that would put their lives on the line. But if it is a refugee who is being pushed back to his or her country of origin after having fled from it because of persecutions, being repatriated basically means being forced back into the lion’s den. There are about 35 million people in the world who live this condition of forced rootlessness, and the United Nations High Commissioner for Refugees is there to look after them. The media doesn’t give much space to the ‘other side’ of these disembarkments, so the public opinion often neglects the tragedy behind their escapes: it is too easy to take advantage of this situation and to play on people’s fear. In doing so, a victim needing help becomes a menace, a person who is frightening just because he or she arrived in this country irregularly, perhaps by sea.

Common sense can do little in front of fear, especially when it is fuelled in such a misleading way, spreading it and turning it into something collective. This perception, so arbitrary and deceptive, does not do justice to the women, men and children who have reached the Italian coasts in these years. Nor does it do justice to an Italy that is invisible, yet real: that of those who, in their everyday lives and through their jobs, promote a mutual understanding and a civil coexistence. I think of the teachers who, with the little resources given, support young foreigners in their difficult academic path and who prepare the young Italians to live in the global village. I think of the many fishermen who have risked their own lives to save hundreds of people in the Mediterranean in the past few years. I think of the Italian families who get to know and learn from this new resource, who respect their dignity and their rights. It is in these contexts that the society of the future is developing, and it is thanks to these ordinary heroes that integration becomes a concrete thing, in a spontaneous and almost unconscious way, while too often it still remains a vague and abstract objective for the institutions.

* Laura Boldrini is the Italian spokesperson for the United Nations High Commissioner for Refugees (UNHCR) and author of the book Tutti indietro (ed. Rizzoli, 2010).

Translated by Olivia Jung, UNICRI
On the International Agenda

01-04 September 2010
The Hague, The Netherlands

**Summer Programme on Disarmament and Non-Proliferation of Weapons of Mass Destruction**

The T.M.C. Asser Institute organizes a summer programme in close cooperation with the OPCW (the Organisation for the Prohibition of Chemical Weapons), the CTBTO Preparatory Commission, the BWC-ISU (Biological Weapons Convention Implementation Support Unit of the United Nations Office for Disarmament Affairs) and the IAEA (International Atomic Energy Agency). The objective of this one-week summer programme is to raise interest among the younger generation in pursuing careers in disarmament and non-proliferation as part of the larger process of enhancing stability and security in the world.


01-04 September 2010
Oslo, Norway

**International Conference on the Treatment of Sex Offenders**

The biennal International Conferences on the Treatment of Sexual Offenders aim to the dissemination of new research, treatment methods and to provide continuing education and networking opportunities. The Conferences also promote advocacy of humane, dignified, comprehensive, ethical and effective treatment of sexual offenders throughout the world.

More Information: www.iatso.org/Oslo

08-11 September 2010
Liege, Belgium

**10th Annual Conference of the European Society of Criminology**

The Conference aims to foster a Criminology that works on the double level of analysis (crime committed by a single person or by individuals linked by various kinds of relationships) and to stimulate bridges between them. The Conference will embrace most of the issues about crime, crime prevention and deviance. It will also try to enhance exchanges and cooperation between scholars, academics and other institutions (both public and private).


23-24 September 2010
Budapest, Hungary

**International Conference on “Freedom, Security and Justice”**

50th Anniversary of the Foundation of the National Institute of Criminology (NIC)

“Freedom, Security and Justice” is the title of the closing conference of the NIC Anniversary Year, with invited speakers from Hungary and abroad. The conference aims both to report on the events and achievements of the Anniversary Year, and to provide a frame for programmes on the topics of freedom, security and justice.

More information: http://en.okri.hu/content/view/123/9/
13-15 October 2010  
**Hull, England, UK**

**The 13th World Conference of the International Institute for Restorative Practices**

The interdisciplinary conference will spotlight the city of Hull, which is bringing restorative practices training to its 23,000 professionals and volunteers who work with children and young people. Beginning with educators, police, social workers and others in the Riverside section of Hull, and expanding to a wide variety of agencies throughout the city, the Hull Centre for Restorative Practices is using training programs developed by the International Institute for Restorative Practices. The conference will also include educationalists, social care and criminal justice professionals from many countries who, in small breakout sessions, will share their experiences in effectively using restorative practices.


18-22 October 2010  
**Vienna, Austria**


Pursuant to article 32 of the United Nations Convention against Transnational Organized Crime, a Conference of the Parties to the Convention was established to improve the capacity of States Parties to combat transnational organized crime and to promote and review the implementation of this Convention.


08-12 November 2010  
**Geneva, Switzerland**

**6th United Nations Conference to review the UN set on competition Policy**

The Sixth UN Review Conference will mark the 30th anniversary of the adoption of the United Nations Set of Multilaterally Agreed Equitable Principles and Rules for the Control of Restrictive Business Practices (United Nations Set). The UN Set is a multilateral agreement on competition policy that: provides a set of equitable rules for the control of anti-competitive practices; recognizes the development dimension of competition law and policy; provides a framework for international operation and exchange of best practices.

Challenging Ideas

Cybercrime: Criminal Threats from Cyberspace
David G. Raffaelli, Christopher L. J. Frid (Editors) - Cambridge University Press (2010)

Cybercrime sets out to explain two things: what cybercrime is, and why the average citizen should care about it. To accomplish that task, the book offers an overview of cybercrime and a discussion of the legal issues surrounding it. Enhancing her narrative with real life stories, author Susan Brenner traces the rise of cybercrime from mainframe computer hacking of the early days, to the organized, professional, often transnational cybercrime that has become the norm in the 21st century. She explains the many different types of computer-facilitated crime, including identity theft, stalking, extortion, and the use of viruses and worms to damage computers, and outlines and analyses the challenges cybercrime poses to law enforcement at national and international levels.

- Amazon editorial review

Handbook of Internet Crime
Yvonne Jewkes, Majid Yar - Willan Publishing (November 2009)

An essential reference for scholars and others whose work brings them into contact with managing, policing and regulating online behaviour, the “Handbook on Internet Crime” emerges at a time of rapid social and technological change. Amidst much debate about the dangers presented by the Internet and intensive negotiation over its legitimate uses and regulation, this is the most comprehensive and ambitious book on cybercrime to date. “The Handbook on Internet Crime” gathers together the leading scholars in the field to explore issues and debates surrounding internet-related crime, deviance, policing, law and regulation in the 21st century. The Handbook reflects the range and depth of cybercrime research and scholarship, combining contributions from many of those who have established and developed cyber research over the past 25 years and who continue to shape it in its current phase, with more recent entrants to the field who are building on this tradition and breaking new ground. Contributions reflect both the global nature of cybercrime problems, and the international span of scholarship addressing its challenges.

- Amazon editorial review

Cyber War: The Next Threat to National Security and What to Do About It

Cyber War goes behind the “geek talk” of hackers and computer scientists to explain clearly and convincingly what cyber war is, how cyber weapons work, and how vulnerable we are as a nation and as individuals to the vast and looming web of cyber criminals. From the first cyber crisis meeting in the White House a decade ago to the boardrooms of Silicon Valley and the electrical tunnels under Manhattan, Clarke and coauthor Robert K. Knake trace the rise of the cyber age and profile the unlikely characters and places at the epicenter of the battlefield. They recount the foreign cyber spies who hacked into the office of the Secretary of Defense, the control systems for U.S. electric power grids, and the plans to protect America’s latest fighter aircraft.

- Amazon editorial review
**Computer Forensics and Cyber Crime: An Introduction**  
Marjie T. Britz - Prentice Hall, 2nd edition (October 2008)  
This book fully defines computer-related crime and the legal issues involved in its investigation. Re-organized with different chapter headings for better understanding of the subject, it provides a framework for the development of a computer crime unit. Updated with new information on technology, this book is the only comprehensive examination of computer-related crime and its investigation on the market. It includes an exhaustive discussion of legal and social issues, fully defines computer crime, and provides specific examples of criminal activities involving computers, while discussing the phenomenon in the context of the criminal justice system. Computer Forensics and Cyber Crime 2e provides a comprehensive analysis of current case law, constitutional challenges, and government legislation. New to this edition is a chapter on Organized Crime & Terrorism and how it relates to computer related crime as well as more comprehensive information on Processing Evidence and Report Preparation.  
- *Amazon editorial review*

**The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives**  
This book is about the global cybercrime industry, which according to some estimates, is a US$1 trillion industry and is growing rapidly. It examines economic and institutional processes in the cybercrime industry, provides insights into the entrepreneurial aspect of firms engaged in cyber-criminal activities, takes a close look at cybercrime business models, explains the global variation in the pattern of cyber-crimes and seeks to understand threats and countermeasures taken by key actors in this industry. This book’s distinguishing features include the newness, importance, controversy and complexity of the topic; cross-disciplinary focus, orientation and scope; theory-based but practical and accessible to the wider audience; and illustration of various qualitative and quantitative aspects of the global cybercrime industry.  
- *Amazon editorial review*

**Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security)**  
John R. Vacca - Morgan Kaufmann (July 2009)  
This book presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. It also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book also covers security and network design with respect to particular vulnerabilities and threats. It also covers risk assessment and mitigation and auditing and testing of security systems.  
- *Amazon editorial review*
A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications
Marianne Wade, Almir Maljevic - Springer (November 2009)

In this book an international panel of experts analyzes current trends and new developments in law enforcement and legal systems throughout the continent, including material from non-English-speaking countries that is seldom available to the broader academic community. Offering a succinct overview with special focus on criminal law, police procedure, immigration law, and human rights, the book provides unique insight into what the war on terror means to EU member and non-member countries; state supporters and critics of American anti-terrorist policy; nations with recent histories of outside terrorist attacks and those facing threats from homegrown entities. This comparative approach gives readers three levels of understanding: by country, as affecting the European Union as a whole, and in the context of the UN.

- Amazon editorial review

Handbook of Crime
Fiona Brookman, Mike Maguire, Harriet Pierpoint, Trevor Bennett - Willan Publishing (February 2010)

“The Handbook of Crime” is a comprehensive edited volume that contains analysis and explanation of the nature, extent, patterns and causes of over 40 different forms of crime, in each case drawing attention to key contemporary debates and social and criminal justice responses to them. It also challenges many popular and official conceptions of crime. This book is one of the few criminological texts that takes as its starting point a range of specific types of criminal activity. It addresses not only ‘conventional’ offences such as shoplifting, burglary, robbery, and vehicle crime, but many other forms of criminal behaviour - often an amalgamation of different legal offences - which attract contemporary media, public and policy concern. These include crimes committed not only by individuals, but by organised criminal groups, corporations and governments.

- Amazon editorial review

Toto Truffa
Antonio Scuglia and Silvio Scuglia - Felici Editore (April 2009)

Written by a journalist and a lawyer (the brothers Antonio and Silvio Scuglia, respectively), Toto Truffa (the lottery of frauds) presents various tricks and techniques used to fraudulently deceive people. The offenders present themselves with thousands of different scams and costumes: fake Municipality employees, fake gas technicians or electricians, even fake priests... The swindlers are everywhere, they strike at home and in the streets, they empty out their victims’ bank accounts with a simple click of a mouse. But for every trap there’s a way out. The book Toto Truffa is a collection of 150 different types of tricks and, above all, a practical manual to avoid being deceived.

- Felici Editore review
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