10

CYBERCRIME

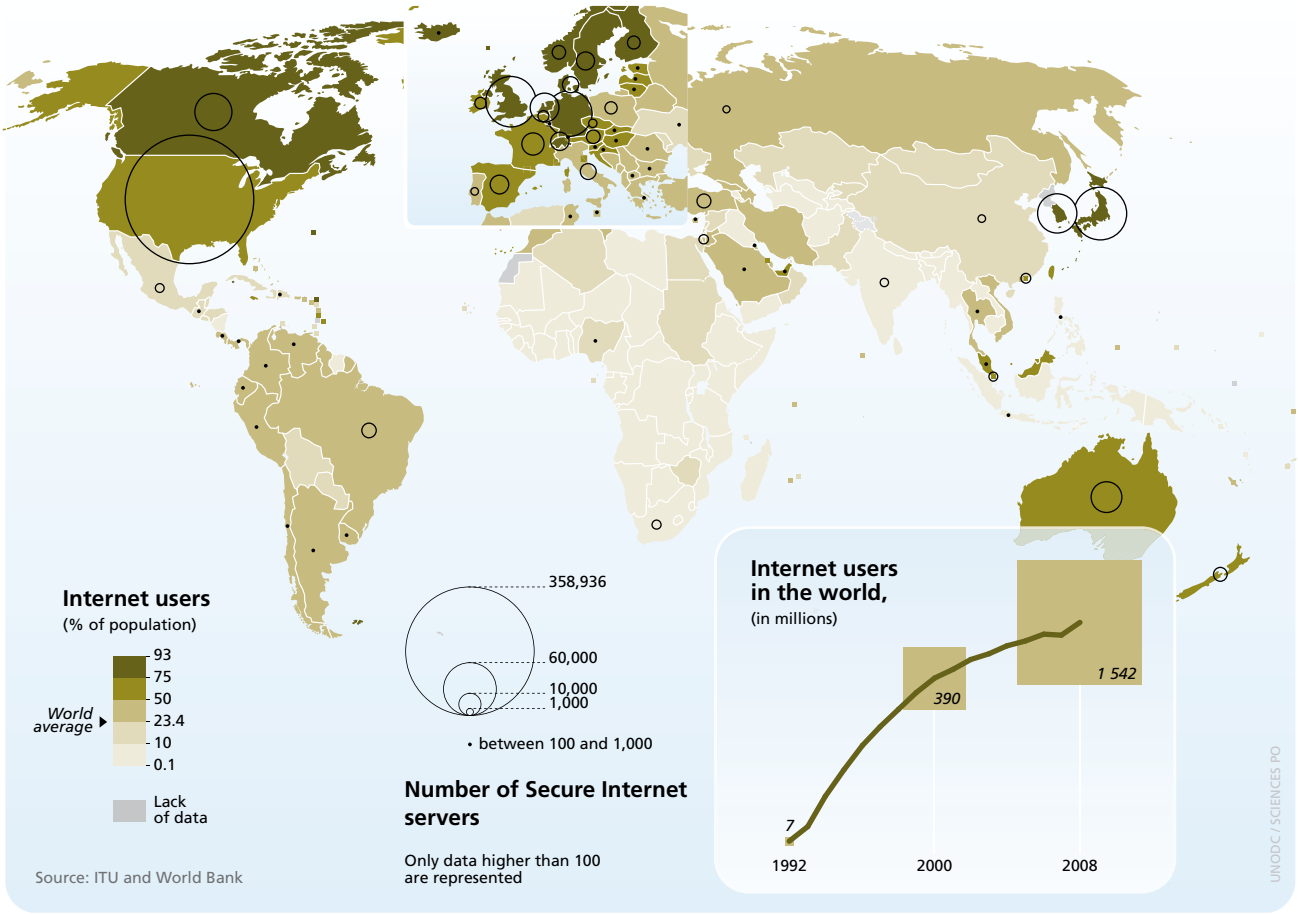
CYBERCRIME

In less than two decades, the Internet has grown from a curiosity to an essential element of modern life for millions.[1] As with other aspects of globalization, its rapid expansion has far exceeded regulatory capacity, and this absence of authority has left space for many abuses. The problem is compounded by the fact that the Internet was fashioned on a military system designed to circumvent interference and external controls.[2] But even those who most loudly champion its creative anarchy have come to realize that the Internet can only reach its full potential if some basic ground rules are established and if antisocial behaviour is vigorously discouraged. The challenge remains how, exactly, to do this.

"Cybercrime" has been used to describe a wide range of offences, including offences against computer data and systems (such as "hacking"), computer-related forgery and fraud (such as "phishing"), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content).[3] It has evolved from the mischievous one-upmanship of cyber-vandals to a range of profit-making criminal enterprises in a remarkably short time. Of course, criminals, like everyone else with access, make use of the Internet for communication and information gathering, and this has facilitated a number of traditional organized crime activities. But the growing importance of the Internet and our collective dependence on it has also created a number of new criminal opportunities. This chapter considers two of the most problematic: the well-established fraud of identity theft and the previously unprofitable trade in child pornography. The former is an acquisitive crime, an updated version of check kiting. The latter is a kind of electronic trafficking, transmitting contraband across borders through the Internet.

A key question at the outset is whether these two activities could or should be classed as organized crime. Both are offences that tend to favour lone or small groups of perpetrators. Among the great advantages cyberspace offers to criminals are anonymity and the ability to allow otherwise unassociated individuals in different parts of the world to

FIG. 160: **SHARE OF INTERNET USERS AND NUMBER OF SECURE INTERNET SERVERS,** 2008



network on a transactional basis (through the use, for example, of bulletin boards, typical in both offences). The inherent limitations in organizing identity theft and child pornography for the profit of standing criminal groups are discussed further below. Other forms of cybercrime, particularly intellectual property violations, may be more attractive to standing groups, and evidence has been increasing that organized cybercrime groups of some longevity are operating in areas like software piracy and other forms of copyright infringement.[4] And there are a number of reasons why cybercrime in general and organized cybercrime in particular might increase in the near future.

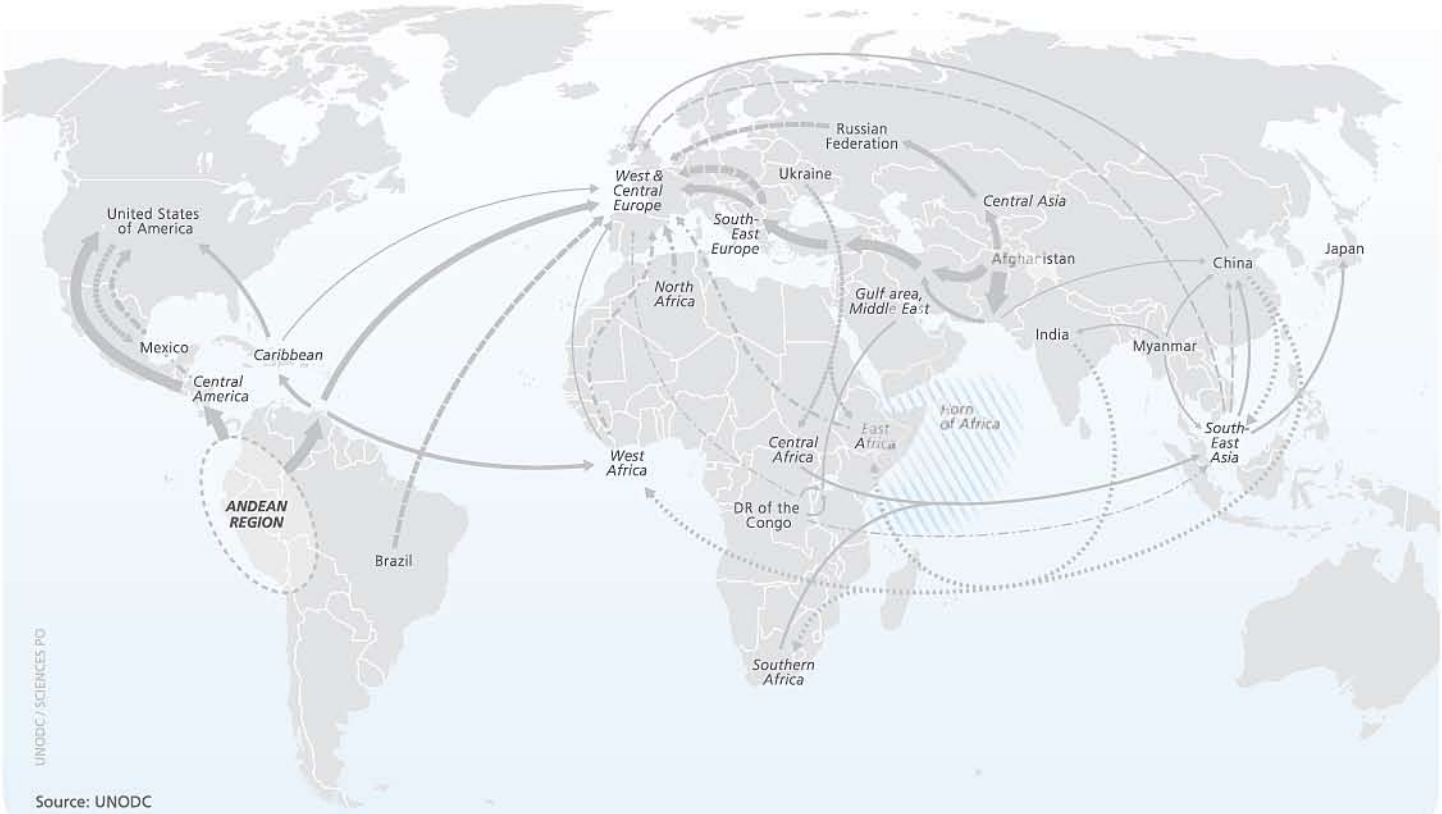
First, the technology of cybercrime has become more accessible. Software tools can be purchased online that allow the user to locate open ports or overcome password protection.[5] These tools allow a much wider range of people to become offenders, not just those with a special gift for computing. For example, the proprietors of the recently discovered "Mariposa" botnet (a network of "enslaved" computers), perhaps the largest in history, were said not to have advanced hacking skills.[6] Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices.[7] While skilled cyberthieves would likely see no advantage in working for a standing organization, these tools could allow criminal groups to employ large numbers of relatively unskilled individuals to labour on their behalf.

Second, the profile of Internet users is changing. In 2005, the number of Internet users in developing countries surpassed the number in industrial countries.[8] If these new users were no more likely than those in developed countries to be predators, the number of predators should continue to expand apace. But the number of high-value victims, largely located in richer areas, will remain more or less the same. As a result, the intensity of the attacks on this unchanging victim pool will likely grow. The Internet has made high value victims as accessible as local ones for perpetrators in the developing world.[9]

Finally, each new offender can increase the number of attacks exponentially through the growing use of automation. Many millions of unsolicited bulk spam messages can be sent out by automation within a short time frame.[10] Hacking attacks are often also now automated[11] with as many as 80 million hacking attacks every day[12] due to the use of software tools that can attack thousands of computer systems in hours.[13] Recently, a botnet was detected involving 12.7 million infected computers, include those of many of the world's biggest corporations.[14] The capacity to launch millions of attacks is relevant for two reasons:

- It makes viable criminal strategies that would otherwise be unprofitable due to the high failure rate. For example, despite widespread knowledge of the nature of advance fee fraud and phishing schemes, these remain profitable because the perpetrators need only succeed in locating one or two marks in millions of attempts.
- It allows cyberthieves to fly under the radar by taking only a small amount of money from a large number of victims, decreasing the chances of detection.[15]

Some analysts have posited losses to cybercrime to have been as much as 1 trillion US dollars in 2008,[16] although these sorts of figures are hotly contested. Given the breadth of the activity and the number of possible victims (over 1.5 billion internet users recorded in 233 countries),[17] it is difficult to come up with comprehensive estimates.



10.1. Identity theft

Route

Vector:	*Internet*
Location of perpetrators:	*Both developing and developed countries*
Location of victims:	*Primarily developed countries, especially the USA*

Dimensions

Annual market volume:	*About 1.5 million victims globally*
Annual value:	*About US$1 billion globally*

Offenders

Groups involved:	*Data acquisition is primarily an individual activity; "cashing out" may involve organized groups*

Threat

Estimated trend:	*Overall identity theft appears to be declining, but the trend in the portion that is electronic is unclear*
Potential effects:	*Increase in the costs of credit, depressive effects on the economy, loss of trust in e-commerce*
Likelihood of effects being realized:	*High*

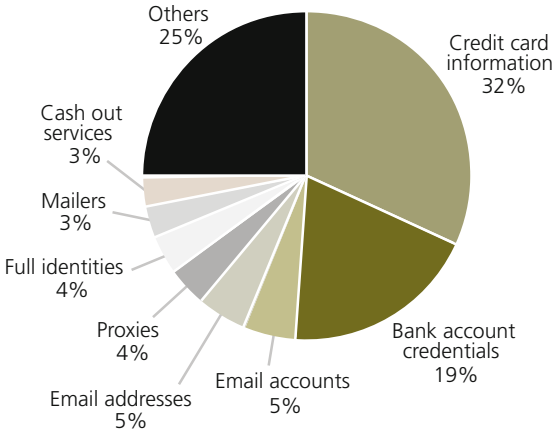
What is the nature of this offence?

The imposters who pepper history were unusual individuals with the confidence and skills to convince others that they were someone that they were not. In the days when most people died in the community in which they were born, however, the idea of widespread identity theft would have been absurd. In recent years, human mobility has reached such levels that governments and businesses have become reliant on technical devices to establish identity, such as documents, identification numbers, and, increasingly, biometric indicators. The Internet has placed even greater emphasis on associating people with bits of data, including codes, passwords and personal identification numbers. This information can be obtained by cybercriminals in a variety of ways, and used to steal money or incur uncollectable debt through the Internet or more conventional channels.

Today, identity-related offences are the most common form of consumer fraud.[18] The technique is modern, but it is not new. With the widespread use of checks and credit cards came the misuse of these same instruments, by criminals posing as the authorized user. These documents can be obtained through theft or robbery, and this remains one of the most common forms of what could broadly be described as "identity theft." More elaborate forms of impersonation were commonly based on personal data acquired by stealing mail or rummaging through refuse.[19] This information could be used to acquire identity documents, allowing the offender to open checking accounts or obtain credit cards, which would be used to acquire cash or goods. Credit card numbers could be obtained through discarded carbons and used to place telephonic orders for goods, often delivered to mail drops. These paper-based forms of fraud are still far more common than their electronic counterparts, but they are relatively slow and the potential for large profits is limited. Electronic forms of identity theft present many advantages, discussed below.

The misuse of credit card information is often identified as the most common form of identity-related crime.[20] Rather than rummaging for carbons, large databanks of credit card information with personal identification numbers can be downloaded by those able to hack their way into protected sites. This information can be sold on to those in a position to exploit it, and for many cybercriminals, this is the end of the process. Their goal is to collect huge volumes of protected information and sell it, typically via dedicated bulletin boards, to criminal groups who specialize in "cashing out".[21] These bulletin boards offer a wide range of information and services for sale, typically in bulk packages.[22]

FIG. 161: **BREAKDOWN OF GOODS AND SERVICES AVAILABLE FOR SALE ON SAMPLED UNDERGROUND ECONOMY SERVERS IN 2008 BY TYPE**



Source: Symantec Global Internet Security Threat Report 2008

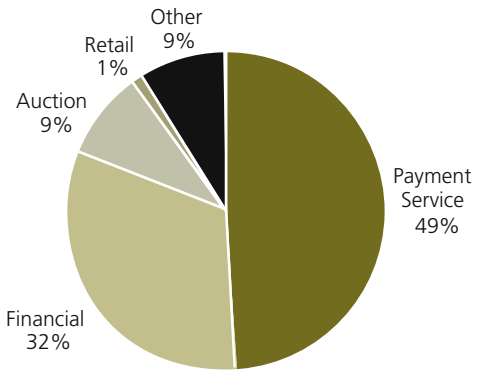
Electronic banking has offered opportunities for acquiring the cash more directly. The most recent techniques used to acquire identity information by Internet-related methods can be broken into three large headings: "phishing", or deceiving Internet users into divulging their personal information; "malware", or the use of unintentionally-installed software which collects and transmits personal information; and "hacking", or illegally accessing computer systems remotely.

Phishing

Some countries use the term "identity fraud" to describe this phenomenon, which could be classed with offences formerly described as "larceny by trick".[23] The technique involves fooling victims into disclosing passwords and related information by posing as the relevant financial institution or other organization with a legitimate interest in this information. There are at least two headings under which phishing attacks can be further divided:[24] email-based and "pharming".

E-mail-based phishing typically occurs in three phases. In the first phase, offenders identify legitimate companies that are offering online services and communicating electronically with customers.[25] The Anti-Phishing Working Group identified 259 e-mail information campaigns that had been hijacked by phishers in June 2009.[26] The most targeted sectors were payment services (49%) and the financial sector (32%).[27]

FIG. 162: INSTITUTIONS FEIGNED IN PHISHING ATTACKS



Source: Anti-Phishing Working Group, Phishing Activity Trends Report 2/2009

In the second phase, offenders design websites that look like the legitimate websites of the identified company, known as "spoofing sites." In order to direct users to the spoofing sites, offenders often send out e-mails resembling those from the legitimate company.[28] These sites request the user to provide details such as passwords and other information that can be used for identity theft. The estimated response rate to e-mail phishing is between 3% and 11% of those to whom the request is sent.[29] Of these, some sites are so convincing that up to 5% of those accessing the site have provided the requested information.[30]

In the third phase, the offenders use the information disclosed by the victim to log on to the victim's accounts and commit offences, such as transferring money or applying for new accounts. The transfer of money from the victim's account often involves financial agents to launder the funds so acquired.[31] In June 2009 Anti-Phishing Working Group detected more that 49,000 unique phishing sites.[32]

The second technique used to direct the user to the spoofed website is manipulation of the Domain Name Server (DNS) in a process known as "pharming."[33] This usually involves installing malware on the individual user's computer or a DNS, which routes traffic on the Internet. When a computer or DNS is infected, users attempting to access their electronic bank accounts or other online information are redirected to a spoof site. When they enter their personal information to log on, the identity thieves record this information.

Malware

Instead of e-mail scams, identity thieves can use malicious software to obtain the desired information directly from the user's computer.[34] Toolkits that enable offenders to design such malware are available for US$200 to US$500.[35] Once installed, there are a number of ways these software devices can operate.[36] They can directly scan hard drives to collect information formatted in ways typical of passwords, credit card numbers and social security numbers.[37] Since many people use the same passwords for multiple accounts, detecting one or two can be enough to unlock all the users' accounts. They can also be designed to intercept communications or log keyboard strokes - literally recording every entry made by a user - and this information can be sifted electronically for passwords and related information.

Hacking

The term "hacking" is used to describe the unlawful access of a computer system.[38] It is one of the oldest computer-related crimes,[39] and in recent years has become a mass phenomenon.[40] By targeting computer systems that host large databases, offenders can obtain identity-related data on a large scale,[41] and this is an increasingly popular approach.[42] In the largest case detected in the past in the USA, the thieves obtained more than 40,000,000 credit card records.[43]

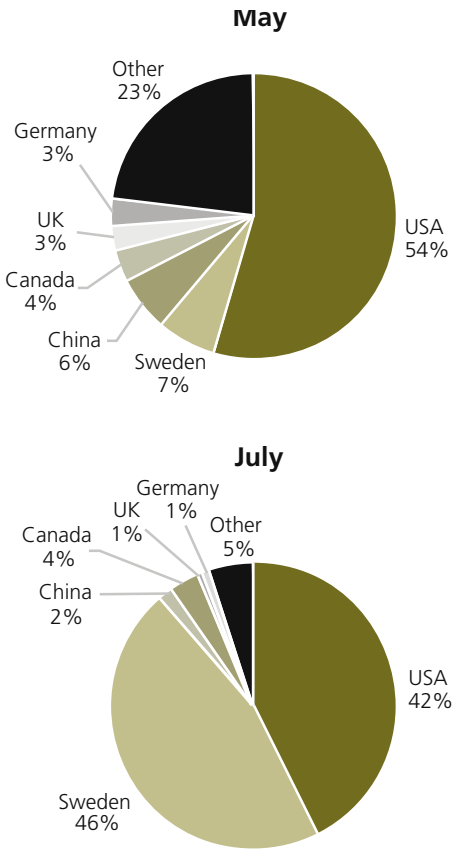
Apart from direct financial profit, offenders can use identity-related information for other purposes, including using a victim's bank account to launder money.[44] In addition, they can circumvent identification and terrorist prevention measures by using obtained identities. The Report of the Secretary-General of the United Nations on Recommendations for a global counter-terrorism strategy highlights the importance of developing tools to tackle identity theft in the fight against terrorism.[45]

Who are the offenders?

Identity theft is not necessarily a crime that needs to be committed with the help of others.[46] Single offenders with access to the technology can acquire and use this information on their own, or sell it on to others who can better exploit the data. Both the seller and the buyer of identity-related information are involved in the offence, but they do not form a "group" any more than do the buyers or sellers of any other commodity. Where groups exist, they tend to be both smaller[47] and more loosely structured[48] than those involved in other forms of organized crime. One of the great advantages of the Internet for criminals is that it allows the formation of exactly these ad-hoc associations between otherwise unrelated individuals.[49]

Since offenders may act as individuals and the crime may be committed from anywhere in the world, it is very difficult to profile identity thieves. It is estimated that many of the currently active groups are operating from Eastern Europe,[50] but this is difficult to demonstrate statistically. West Africa is also implicated: a recent survey of businesses operating online found that one quarter had stopped accepting orders from certain countries due to repeated fraud. Of these, 62% indicated Nigeria was one such country, followed by Ghana (27%) and Malaysia (21%).[51] National indicators, such as the coding language of malware, show too much volatility to be true indicators of the origin or residence of the criminals. The same is true for the location of servers used in the crime. For example, in May 2009, the country hosting the largest share of detected phishing websites was the USA, with 54% of the sites detected.[52] One reason for the dominance of the USA may be the high number of servers located in that country. But just two months later, the profile changed, with Sweden hosting the largest share: 46%, up from 7% in May.[53]

FIG. 163: **COUNTRIES HOSTING PHISHING SITES,** MAY AND JULY 2009



Source: Anti-Phishing Working Group

In terms of victims, the USA has been reported as the leading source of credit card numbers advertised on underground economy servers.[54] Figures from the USA show that most computer crime against US citizens is committed by other US citizens. Two thirds of the perpetrators of Internet crimes reported to the US national Internet Crime Complaint Center in 2008 were based in the United States, with 11% coming from the United Kingdom, 9% from Nigeria, 3% from Canada and 2% from China. South Africa, Ghana, Spain, Italy and Romania each comprised less than 1% of the perpetrators.[55]

How big is the problem?

As a new and ill-defined crime area, data on the scale of cyber identity theft are very rudimentary, with most figures emerging from national assessments. The United States appears to be the source of most of the identity information dealt on-line, comprising a large share of the value of the global market, so it is particularly relevant as a national example.

Albert Gonzalez is said to be the single most prolific identity thief in United States history. Gonzalez was indicted in multiple cases, including the Shadowcrew case (1.5 million data items stolen),[56] the TJX Companies case (46 million)[57] and the Heartland Payment Systems case (130 million – the single largest US case ever).[58] In addition to being used to withdraw cash from ATMs, the stolen information was sold to conspirators in Eastern Europe. His net profit from these exploits remains unclear, but his guilty plea included forfeiture of US$1.6 million, one condominium, a luxury car and some personal items. It remains possible that Gonzalez has additional wealth secreted in overseas accounts, but considering the extent of his activity, these assets seem rather modest. A large Nigerian identity theft ring detected in New York resulted in the indictment of 48 people. This network was alleged to have made US$12 million in 2008, or about US$250,000 apiece.[59]

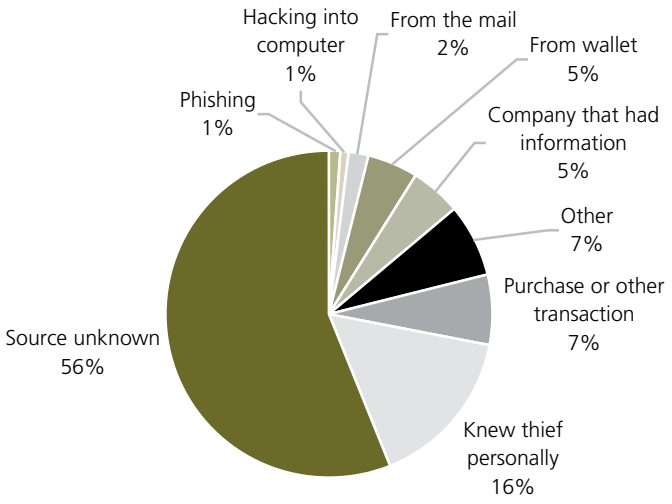
Based on a government survey in the USA in 2006, it was estimated that within a 12-month period, some 10 million people lost on the order of US$15.6 billion to identity theft. This represented a significant downward revision from a previous estimate based on a similar methodology. Victims were asked how the information was obtained. Over half of the victims did not know, and of those who did, the majority indicated sources that precluded cybercrime. Only 2% said the information was obtained

by phishing or hacking into a computer.[60] If the chances of the victim knowing the source of the leak were the same for both cyber victims and other victims, then perhaps 5% of the US$15.6 billion loss could be attributed to cybercriminals, or US$780 million. An update of this survey conducted by a private research organization in 2007 found a declining trend in the incidence of identity theft in the USA.[61]

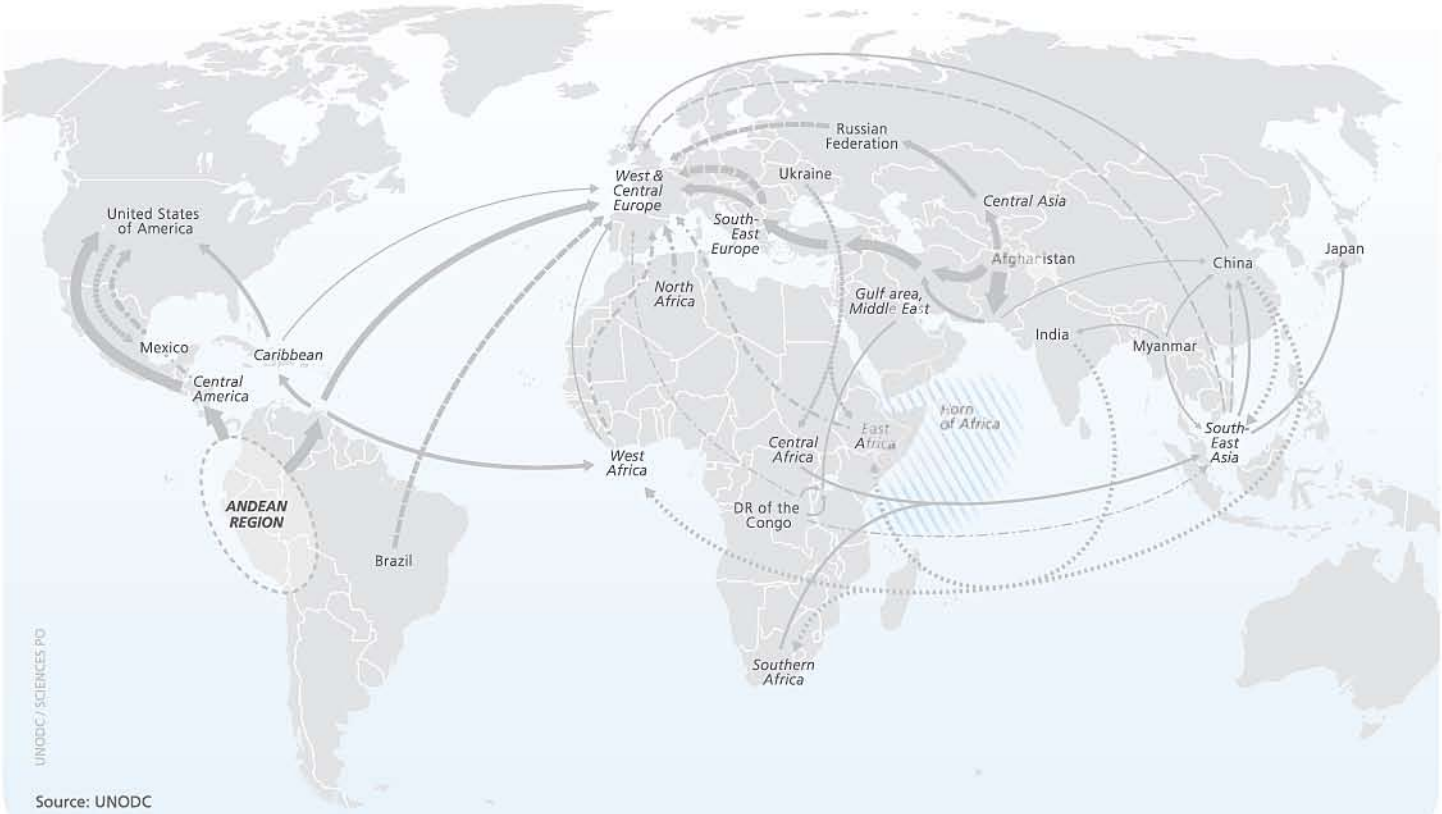
Outside the USA, other Anglophone countries have found much smaller total losses. In Australia, identity theft loss estimates vary from less than US$1 billion to more than US$3 billion per year.[62] In the United Kingdom, the cost of identity fraud was recently said to be 1.2 billion pounds (just under US$2 billion).[63] Total losses in Canada were pegged at about US$2.5 billion in 2002.[64] It is unclear what share of these losses was computer-related.

Beyond these countries, there are very few data. One annual study by a security company with global reach concluded that the USA was the source of some two thirds of the credit card information sold on known underground economy servers in 2008.[65] If the USA represents two thirds of the market and US losses are on the order of US$780 million, global losses would be on the order of US$1 billion.[66]

FIG. 164: HOW IDENTITY WAS OBTAINED IN CASES OF IDENTITY THEFT IN THE USA



Source: Federal Trade Commission



Source: UNODC

10.2. Child pornography

Route

Source:	*Developed and transitional countries*
Vector:	*Internet*
Destination:	*Developed and transitional countries*

Dimensions

Annual market volume:	*Perhaps 50,000 new images generated*
Annual value:	*About US$250 million*

Offenders

Groups involved:	*Primarily individuals organized through social networks*
Residence:	*Developed countries*

Threat

Estimated trend:	*Unclear*
Potential effects:	*Child victimization*
Likelihood of effects being realized:	*High*

What is the nature of this market?

The virtues of the Internet include its ability to transmit great volumes of information at little cost anywhere in the world, and its ability to bring together people of common interests who would otherwise never meet. Unfortunately, the Internet is equally efficacious when the subject is vice, and pornography has traditionally been a mainstay of Internet content. [67] Of this, an indeterminate amount is child pornography. It appears that almost all child pornography transmitted today is in electronic form, typically traded though bilateral or multilateral exchanges. Behind every image of child pornography lies a victim of sexual abuse and, arguably, of human trafficking.

Until recently, the production and acquisition of child pornography were highly risky activities.[68] Only a limited number of paedophiles had access to the facilities to produce hard copy materials, most materials were produced by amateurs,[69] and their dissemination was limited to social networks that were both difficult to establish and fragile.[70] Offenders, when arrested, were generally in possession of a handful of images.[71] These considerations suggested that a good deal of the demand for these materials would necessarily go unmet, and that the market would remain fundamentally unprofitable.

One of the risks associated with the growth of the Internet is that the greater accessibility of child pornography could lead to greater demand, and thus greater profitability in the production and sale of these materials. If child pornography were to approach the profitability of adult pornography, this could attract the attention of organized crime groups, transforming what had been a furtive paper exchange into a professional operation and leading to greater levels of victimization.

The greater accessibility of these materials may have a number of less direct impacts as well. Repressed paedophiles may find validation in these depictions of their fantasies and a sense of community in the groups that exchange child pornography. To gain acceptance in these groups and to achieve recognition among their peers, they may feel compelled to produce their own footage. These materials can even be used to "groom" victims, to convince them that such conduct is normal and accepted.

The possibility that children are being victimized for the sole purpose of making marketable child pornography is subject to empirical verification, but, to date, has not yet been tested. Despite the seizures of many hard drives and even servers containing hundreds of thousands of images, very little work has been done examining the content of these images to determine what can be said about the nature of production – how much is professionally produced, and how much is clearly amateur. In fact, little research has been done on the global scale or growth of the child pornography industry. Such an exercise would seemingly be straightforward to do, since image comparison can be automated, using, for example, the PhotoDNA software from Microsoft. Using a capture/recapture estimation technique, the universe of child pornography could be quickly surmised. Looking at different drives seized at different points in time, the growth rate of the market could be estimated. This could be complimented by a content analysis, looking at issues like the language spoken in video clips, indicators of the age of the images, or other indicators of when, where, and how the current stock of child pornographic images has been produced. Given the importance of the issue, it is remarkable that such research has not yet been done. Some of the best content-oriented studies are discussed below.

Based on limited case studies, it does appear that those caught in possession of these materials today possess far more images than in the past.[72] But it remains unclear whether there are significantly more images in circulation, or whether each offender simply has access to a more complete collection than before. One study of dated digital images found a strong clustering in recent years, but images taken before the advent of the digital camera were necessarily excluded.[73]

How is the crime committed?

A key initial question to ask in understanding the child pornography industry would be: is the distribution of child pornography similar to YouTube, where most of the content is produced by amateurs competing for prestige within their peer group, or does it resemble the adult commercial pornography industry, which is run like a business? It appears that child pornography is available in both commercial and non-commercial domains, but the ratio between the two remains unclear.[74] It does appear that peer-to-peer exchanges, generally not commercial, have become the most popular means of exchanging these materials, however.[75]

There have been studies of site content based on public reports to national complaint lines, but these studies generally do not capture peer-to-peer exchanges, and consequently the materials they review may not be representative of all those cur-

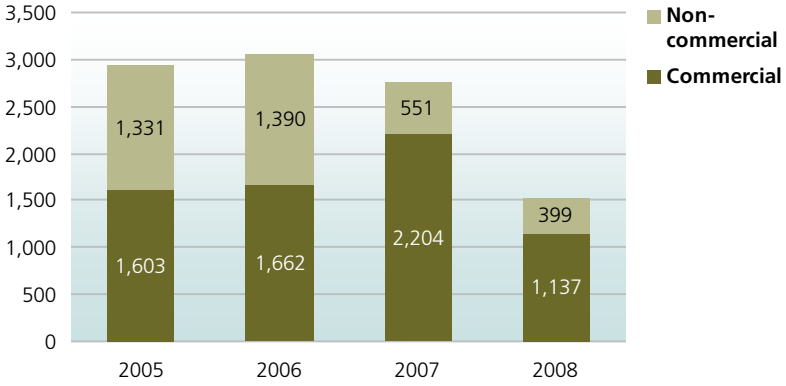
rently being exchanged. The Internet Watch Foundation is an organization in the United Kingdom that receives site-content complaints, the vast majority of which are related to child sexual content. In 2005 and 2006, the division between commercial and non-commercial domains was close to even, but more recent years show both a sharp shift to commercial sites and a diminishing number of overall detections.[76] This may not be a true trend, however, since diminishing detections may be related to trend toward the greater use of peer-to-peer exchange rather than public websites, a trend that may be particularly pronounced among non-commercial actors.

A similar organisation in Canada – Cybertip.ca – recently found that a much smaller share of the sites reviewed were commercial: only 13%. It found that the share of commercial sites varied greatly by the host location of the websites. In the Russian Federation, for example, only 2% of the known websites were commercial, while in the UK, 21% were. This ratio may be related to the likelihood of being prosecuted in the host jurisdiction.

In the Cybertip.ca study, the commercial websites reviewed were actually more likely to feature modelling-type images and less likely to show sexual assault than non-commercial ones. This may be partially due to the fact that some of the commercial sites were themed to emphasize the innocence of the children.

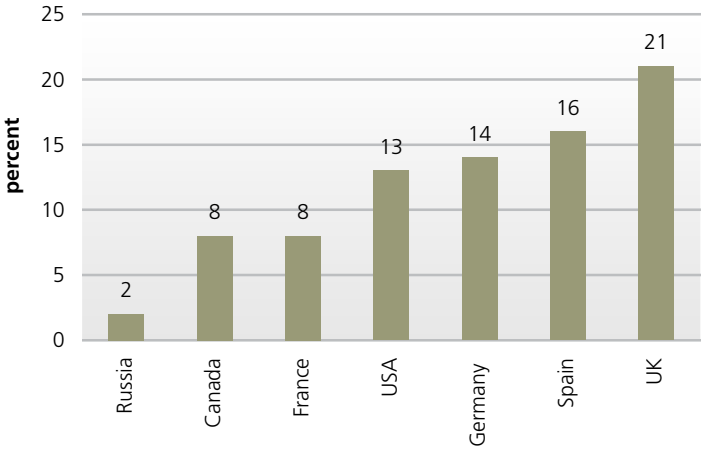
Whether commercially motivated or amateur, offenders do not seem to have difficulties in sourcing victims, because their targets are generally too young to defend themselves. Contrary to what might be expected, the victims of child pornography are not primarily teenagers just shy of adulthood. In the Cybertip.ca study, the majority appeared to be under the age of 8, with many of the most severe images featuring babies and toddlers. Commercial sites were more likely to show these very young children than non-commercial sites. The Internet Watch Foundation also provides a profile of the victims, noting that 69% of the victims appear to be under the age of 10, with 24% being less than 7.[77] In one sampling, 39% of those persons caught with images of child sexual abuse had images of children younger than 6 years old.[78] In the Cybertip.ca sample, girls comprised 90% of the victims on commercial websites, compared to 83% on all websites. While some studies have found greater gender balance, this is in keeping with the gender ratio found in other large studies.

FIG. 165: CHILD PORNOGRAPHY DOMAINS REPORTED TO THE INTERNET WATCH FOUNDATION (UK)



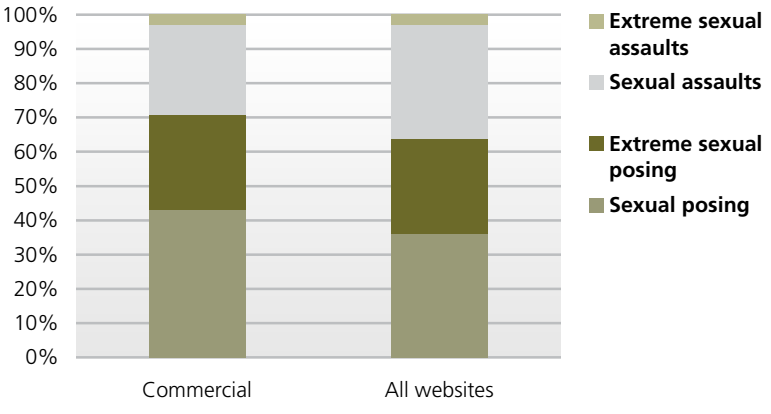
Source: IWF Annual Report 2007 and 2008

FIG. 166: SHARE OF ALL CHILD PORNOGRAPHY WEB SITES REVIEWED BY CYBERTIP.CA THAT WERE COMMERCIAL, 2009



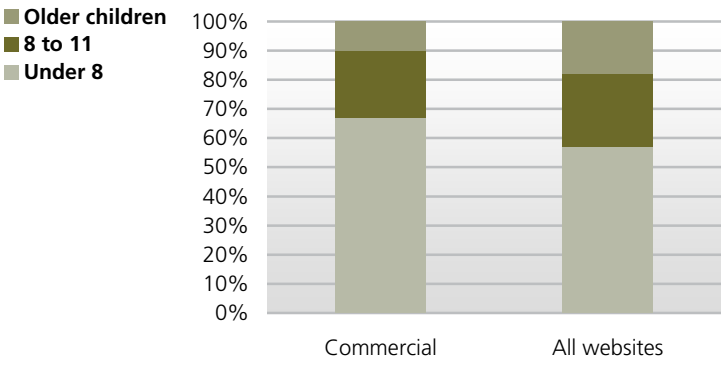
Source: Canadian Centre for Child Protection

FIG. 167: NATURE OF THE ABUSE ON COMMERCIAL WEBSITES COMPARED TO ALL CHILD PORNOGRAPHY WEBSITES



Source: Canadian Centre for Child Protection

FIG. 168: APPARENT AGES OF THE VICTIMS ON COMMERCIAL WEBSITES COMPARED TO ALL CHILD PORNOGRAPHY WEBSITES



Source: Canadian Centre for Child Protection

Cybertip.ca also found that most commercial websites sell memberships, and although online payment systems appear to be preferred, the majority also offered credit card payment options. Sites tend to be themed, and frequently open with a homepage featuring a collage of images and text. There are generally links to a thumbnail gallery containing some 20 to 60 images with further links to a large collection of members-only material. Many of these sites move frequently to new hosts in different countries, illustrating that the location of the host computer may have little to do with the origin of the material.

Aside from surveys of this sort, there are other reasons to believe that much of the production of child pornography is not primarily commercially motivated. As described below, the making of child pornography is generally opportunistic; the victimizer is very often a person entrusted with the care of the child. It appears that, in most cases, the images are generated as a result of the abuse, rather than the abuse being perpetrated for the purpose of selling images. More research is required to come to a firm conclusion on this issue, however.

Those with an interest in child pornography locate and access the sites in several ways. Much material can be gained through networking on usenet groups or through bulletin board services. To gain access to non-commercial websites with large volumes of material, candidates may be required to submit images, both to bolster supply and to demonstrate bona fides. For example, those wishing to join the "Wonderland" club of the late 1990s were required to submit 10,000 images to the database, which gained them access to some 750,000 additional images.[79]

Child pornography vendors often set up fictitious businesses in order to obtain a merchant account for credit card processing.[80] To evade detection by law enforcement, payment schemes used by commercial child pornography websites are increasingly complex.[81] The rapid growth of anonymous financial services has been reported.[82] The demand for anonymous payments led to the development of virtual payment systems and virtual currencies enabling anonymous payment.[83] Virtual currencies may not require identification and validation, thus preventing law enforcement agencies from tracing money-flows back to offenders. Recently, a number of child pornography investigations have succeeded in using traces left by payments to identify offenders.[84] The use of anonymous payment systems such as E-Gold can hinder such investigations.[85]

Who are the offenders?

Prior to the Internet's coming of age, child pornography was not a business of interest to traditional organized crime groups,[86] and there is little evidence of their participation today. Based on domain analysis, it is very likely that the number of organized groups involved in child pornography is small.[87] Those who produce, distribute and consume child pornography are all culpable, but could operate independently and in different parts of the world. In amateur operations, there is often substantial overlap: consumers of child pornography may produce their own material for trade, and set up or participate in online forums for distribution. These networks are not financially motivated, however, and so would not be regarded as organized crime groups under the UN Convention against Transnational Organized Crime. Considerations of this sort led the global NGO "End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes" (ECPAT) to conclude:

> *The majority of child pornography distributed internationally is, in fact, exchanged between paedophiles and child molesters without any commercial motive. Furthermore, while there is evidence that organised crime is involved in adult pornography, the same is not generally true for child pornography.*[88]

Research indicates that up to 97% of those who engage in sex crimes against children on the Internet act alone.[89] This may also be true for both the production and dissemination of pornographic materials: it is possible for single offenders to set up and maintain commercial child pornography websites without having to act in groups.[90] On the other hand, the exchange of these materials, whether

for financial benefit or not, is a group activity, and for some offenders may become an end in itself.

Whether professional or amateur, the damage done to the victims is the same, and those who exchange child pornography for non-commercial reason are often abusers themselves. Frequently, the child sex abusers captured in pornographic images are people who are meant to be caring for the children they victimize. According to data gathered by the US National Center for Missing and Exploited Children, in more than one quarter of the cases where the relationship was known, the victimizer was the parent of the child victim, and in an additional 10% of the cases, it was another relative. The perpetrator was a stranger in only 4% of the cases. One study found that 46% of those arrested for possession of child pornography in the US had access to children through their job or organized youth activity.[91]

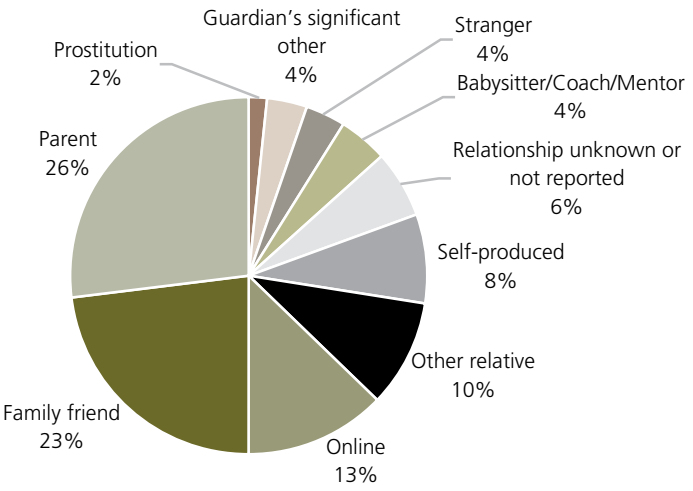
The majority of those who collect child pornography appear to be male, "white and westernized",[92] although there is a subgenre featuring underage Japanese girls aimed at the Asian market. While some studies differ,[93] quite a few show the majority of collectors to be primarily middle-aged. Aside from this, the background appears to be fairly diverse. Those who produce these materials appear to fit a similar profile. In a study of 155 child pornography offenders, 85% admitted to having victimized children themselves.[94]

Because those who produce child pornography are often the relatives of the children, the victims tend to match the ethnic profile of the victimizers: 96% of the victims in the Cybertip.ca sample were white. Research in Australia similarly concluded that most of the victims were white (86%), with some Asians and very few children of aboriginal background.[95]

In 2009, the single largest content analysis ever produced was conducted on more than 250,000 images collected by the UK Child Exploitation and Online Protection Centre. This research found that 91% of the victims were white and 81% female, with 38% being white, prepubescent females. Some 6% were Asian females. Black children were conspicuous by their absence.[96]

It has been argued that most of the victims come from developing countries,[97] but it is difficult to reconcile the facts above with this conclusion. Large-scale production in Africa is excluded due to the ethnic profile of the known victims. Amateur pornography produced in Mexico, Philippines and Brazil has been detected,[98] but clearly these sources do not predominate. It is frequently asserted that

FIG. 169: RELATIONSHIP BETWEEN THE PERPETRATOR AND THE VICTIM IN CHILD ABUSE IMAGES CIRCULATED ONLINE



Source: National Center for Missing and Exploited Children[99]

90% of the commercial child pornography comes from "Eastern Bloc" countries in Europe,[100] and that, as a location, Eastern Europe appears to be key to the organization of the trade.[101] This would be compatible with the ethnic profile described above. A number of cases have been documented in the Russian Federation, Ukraine, the Republic of Moldova and Belarus, often involving child modeling agencies.[102] But given that the producers and the consumers seem to be essentially the same people, most of these images likely originate in the main consumer countries.

The USA holds the largest national share of the domains related to child pornography that are detected by groups like the Internet Watch Foundation and Cybertip.ca, but the USA also has by far the largest number of domains of all sorts.[103] The Russian Federation generally also figures prominently in these assessments. Of course, as noted above, the location of the offenders may be different than the location of the domains they use – this is one advantage of the transnational nature of the Internet for those selling child pornography.

Despite their use of the Internet, child pornographers and their clients are not necessarily technologically sophisticated. Only 6% of the offenders in one sample used encryption technology.[104] In another sample, 17% used password protection, 3% evidence-eliminating software only 2% used remote storage systems.[105] It is possible that more sophisticated consumers have evaded detection altogether, however.

How big is the flow?

As noted above, the lack of research on the size and growth of the universe of child pornography is striking. Known databases have included up to one million images, but these figures include videos which contain many thousands of still images. The largest database that has been cleared of redundancies was collected by the project "Combating Online Paedophile Networks in Europe" (COPINE) at University College Cork in Ireland, which contained some half a million images, some of which might be 30 years older or more. In the late 1990s, an average of four new victims were appearing each month in images traded by the newsgroups they monitored.[106] If this trend were to continue, and 1,000 images were taken of each child, this would yield a growth of some 50,000 images per year, or about 10% growth annually.

Some very large estimates have been made of the value of the commercial child pornography industry, with very little evidence to back them up. In one frequently cited estimate, the on-line commercial child pornography industry is said to be worth US$20 billion. Via a number of intermediary sources, this figure is variously cited to UNICEF and the FBI, both of which have disavowed the number.[107] As will be discussed below, this amount far exceeds credible estimates of the value of the adult internet pornography industry, and is about a quarter of the value of the global cocaine trade, a far more expensive and popular commodity.

Perhaps leery of providing a more precise estimate, a number of sources have referred to child pornography as a "multi-billion dollar industry",[108] although the basis for these calculations remains equally unclear. There are at least two ways a more accurate estimate could be made.

- Industry-based: an estimate of the annual turnover of the total pornography industry could be multiplied by the share of all pornography that involves children.
- Consumer-based: an estimate of the number of offenders could be multiplied by the amount spent by each annually.

Industry-based

Little credible recent research has been done to estimate the size of the market for adult pornographic materials. One 1999 scan of web content found that just over 1% of 2,500 randomly selected servers contained pornography.[109] In 1998, the online adult pornography industry was estimated to generate between US$750 million and US$1 billion in revenues annually.[110] It is likely that the demand has expanded since that time,[111] as the number of Internet users grows, but the number of free sites has also expanded. In addition, many of the new users are located in developing countries, and many of these new users may face restrictions in their access to internet pornography. China, for example, uses a national filter to prevent access to these materials, and treats violations very seriously – over 5,000 people were arrested for internet pornography offences in 2009.[112] As of 2000, online pornography also became illegal in India.

The consensus seems to be that the market has become more competitive, with a small number of commercial providers[113] competing with the proliferation of free sites. The volume of pornography-related web searches is very large, but one industry estimate suggests that only 0.3% to 0.4% of those visiting the pay sites actually purchase content.[114] Those who do pay tend to be collectors, who subscribe to access huge volumes of material, with fees in the tens of dollars securing entry to extended consortia of websites.[115] Although pornography may play a greater role in the lives of paedophiles than for the public in general, it is highly unlikely that the value of the industry exceeds that of the adult trade, due to the much smaller user base. These considerations would favour an estimate of less than US$1 billion annually.

Consumer-based

There are no generally accepted figures for the prevalence of paedophilia, but some insight into the number of people who might buy child pornography can be gathered from criminal justice data. Data associated with law enforcement investigations have suggested some very large figures for the number of offenders and the annual turnover of particular networks.[116]

"Operation Avalanche" was probably the largest-ever investigation focusing on commercial child pornography. Landslide Inc. was a company offering credit card and subscriber services for child pornography websites. It offered subscriptions to more than 5,000 websites globally[117] which, at the time of shut down, were reported to have between 75,000[118] and 390,000[119] customers. The profit, said to be generated mostly through child pornography-related financial services, was reported to be up to US$1.4 million a month.[120] This suggests a profit of around US$3,500 per site per year.[121]

Some 7,000 British citizens were implicated in Operation Avalanche, making possible Operation Ore, a controversial crackdown in the United Kingdom in 1999. The litigation surrounding these arrests has suggested that a share of those allegedly paying for child pornography never downloaded it. In fact, some appear to have been victims of identity theft – their credit card information was bought by website owners and charges falsely generated. Both Operation Avalanche and Operation Ore appear to have resulted in relatively few convictions compared to the number of offenders initially implicated, and many of the British convictions are still under appeal more than a decade later.[122]

In fact, the number of arrests and convictions for possession of child pornography annually are rather modest, even in the best resourced countries. British Home Office figures show 116 offences were recorded for "abuse of children through prostitution and pornography" in 2008/9.[123] In Canada, 1,408 people were charged with possession of child pornography in 2008.[124] This is up considerably from the 159 people were charged with possession of child pornography in 2003.[125] The figure was 1,407 in 2007, suggesting a rather stable situation today.[126] The United States Federal law enforcement authorities, which actively pursue online sex offences, were referred 2,539 suspects for possession of child pornography in 2006, of whom more than half were prosecuted.[127] Due to the deployment of several federal task forces, including those focused on child abuse on the Internet,[128] this figure was up sharply from the 169 detected in 1994.

If US federal authorities were referred even 1% of those in possession of child pornography annually, this would indicate a pool of one quarter of a million offenders, equal to less than one tenth of one per cent of the US population. If a similar share were offenders in Europe, including the Russian Federation, this would still be less than one million consumers in total. There is evidence of consumption of these materials in Asia, but even so, a figure of more than two million Internet child pornography consumers globally would posit extremely low detection rates and can be considered an upper limit.

How much do each of these people "consume" annually? Many child pornography consumers have been found in possession of large numbers of images.[129] As mentioned above, extreme examples include databases of 250,000[130] or even 1 million images,[131] although such figures quickly reach the point of absurdity, unless a large share are video images. If viewed and acquired at a rate of one per minute, selecting 1 million still images would represent almost four years' continuous work, labouring 12 hours per day. According to one sampling, the average number of images in the possession of offenders investigated was 16,698.[132] This would represent a substantial investment if these images were selected and purchased individually, but case studies suggest that, as with the adult industry, material tends to be acquired *en masse*, through trade or subscription services. Other studies suggest far smaller numbers of images per offender: one US-based study of 429 arrestees found that more than half (52%) had fewer than 100 images, and 86% had fewer than 1,000 images.[133] The study distinguished a subset of "organized" collectors (27%), who were more likely to have large collections, video material, non-digital child pornography, images of children under 6 years old, better computer systems and encrypted files.[134]

To consume one billion dollars worth of material, each of the two million global consumers would have to spend US$500 annually apiece, or about US$40 per month. One recent study found an average commercial site membership was US$53 per month,[135] so this is within the realm of possibility, but posits that all child pornography consumers are paying subscribers. It also assumes that subscribers receive sufficient new material every month to justify the monthly fee.

All this would suggest that 1 billion US dollars would be pressing the outer limits of a credible estimate for the annual global turnover for child pornography. It is far more likely that the figure is considerably less, given that a good deal of material is shared between peers. And, if the US figures are representative, perhaps a quarter of global consumers (the share classed as "organized") are likely to be regular subscribers, for a market value on the order of US$250 million.

IMPLICATIONS FOR RESPONSE

Of course, the impact of child pornography cannot be reduced to a dollar figure. And while production of this material appears to be largely an amateur activity, international action should be taken against those aspects of the market that do constitute transnational organized crime: the networks that distribute these images. These networks do comprise groups of some longevity aimed at the commission of a serious offence. The acquisition of new images represents a form of "material benefit", so even networks engaged in bartering could be considered organized crime groups under the United Nations Convention against Transnational Organized Crime. The same is true for identity theft: the actual theft may be largely an individual activity, but those who organize this market and exploit the data constitute transnational criminal networks. There are at least two levels at which the problem can be addressed: prevention and justice.

Prevention can be conducted by individual governments, or even by non-governmental actors. Offending sites can be rapidly disabled, monitoring groups established and tip-lines promoted. These national efforts can be global in scope, since the Internet knows no boundaries. Public education will continue to play a key role in preventing online financial victimization, as well as preparing children to deal with and report attempts to exploit them.

Prevention efforts should have some ameliorative effect, but perpetrators will continue their attempts until a credible threat of incarceration can be generated. Creating this threat will require both international cooperation and national action. Unfortunately, there is, at present, no international agreement to cooperate on cybercrime, aside from the general provisions of the Convention against Transnational Organized Crime. Establishing such an agreement should be seen as a matter of international priority.

Within this framework, national law enforcement agencies can cooperatively take advantage of the anonymity of cyberspace. Undercover work that would take months of preparation in the "real world" can be conducted by anyone with a terminal and a good set of leads. This is unlikely to prevent the activity altogether, but may discourage new players from entering the market place and reduce the incentives for stealing