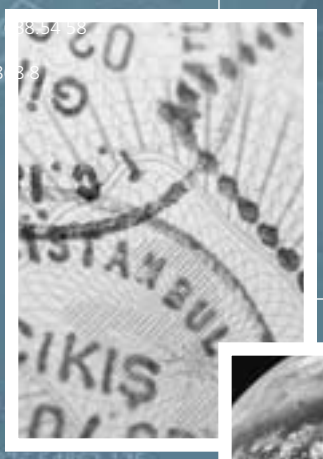
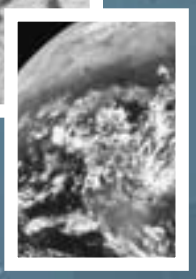
McAfee

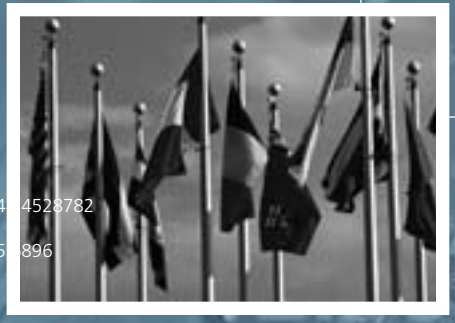
McAfee **Virtual Criminology Report**

Cybercrime Versus Cyberlaw

The annual McAfee global study on organized crime and the Internet in collaboration with leading international security experts.







Contributors

Dr. Ian Brown
Lilian Edwards
Matthew Bevan
Sharon Lemon
Bob Burls MSc
Peter Sommer
Richard Clayton
Philip Virgo
Matthew Pemble
James Blessing
Peter Milford
Dr Marco Gercke
Marc Vilanova
Haim Vismonski
Ferenc Suba
Erka Koivunen
Eugene H Spafford
Andrea Matwyshyn
Mary Kirwan
Leo Adler
Dr. Paulo Marco Ferreira Lima
Adriana Scordamaglia Fernandes Marins
Renato Opice Blum
Alana Maurushat
Peter Guttman
Andrew Adams

CONTENTS

Foreword

Cybercrime is a growing problem that negatively impacts everybody. While a lot has been done to combat cybercrime over the past decade, criminals still have the upper hand. Some experts have argued that a cyberattack could be more economically devastating than the physical attacks on September 11, 2001, so clearly something has to change. This year's *McAfee® Virtual Criminology Report* discusses what factors can drive that change.

Global cybercrime has a significant financial impact on businesses and consumers across the globe, while wider use of technology in developing countries is further opening the window of opportunity for evildoers.

As part of McAfee's effort in the fight against global cybercrime, we recently launched the McAfee Initiative to Fight Cybercrime, a wide ranging initiative aimed at closing critical gaps in the battle against cybercrime. Although we have new cybercrime laws, and recent indictments, we believe there's still more progress to be made.

You're about to read our fourth annual *Virtual Criminology Report.* This year the report discusses the extent to which cyberwar is winning the battle over cyberlaw. It highlights exactly why the McAfee Initiative to Fight Cybercrime is needed.

For this report, we consulted with more than a dozen security specialists from top institutions across the globe. These individuals, who are also on the front lines in the daily fight against cybercrime, were invited to comment on the extent to which cyberlaw is keeping up with the crimes being committed, and provide insight into how we can actually fight – and win – the battle against the perpetrators of cybercrime.

The conclusions? Read on for the details, but at the highest level the experts agree that international action on cybercrime law, enforcement, prosecution and judging is needed.

Fighting cybercrime is a 24/7 battle, a global battle, and it's only just begun.

Dave DeWalt

President & CEO

McAfee Inc.

Introduction

The annual *McAfee Virtual Criminology Report* has traditionally tracked the emerging and looming trends in cybercriminal behaviour and exposed how it has become increasingly organized, sophisticated, and global in its approach and impact.

This year, in collaboration with cybercrime experts from across the world, the fourth annual *McAfee Virtual Criminology Report* reveals the extent to which cybercrime is winning the battle over cyberlaw and that a massive and coordinated global effort is required to redress the imbalance.

Commissioned by McAfee, Dr. Ian Brown from the Oxford Internet Institute and Lilian Edwards, Professor of Internet Law at the University of Sheffield in the UK, undertook extensive research with legal authorities, law enforcement agencies and security experts across the globe to assess the current state of the fight against cybecrime and to evaluate the threats and challenges to gaining a global approach for the future.

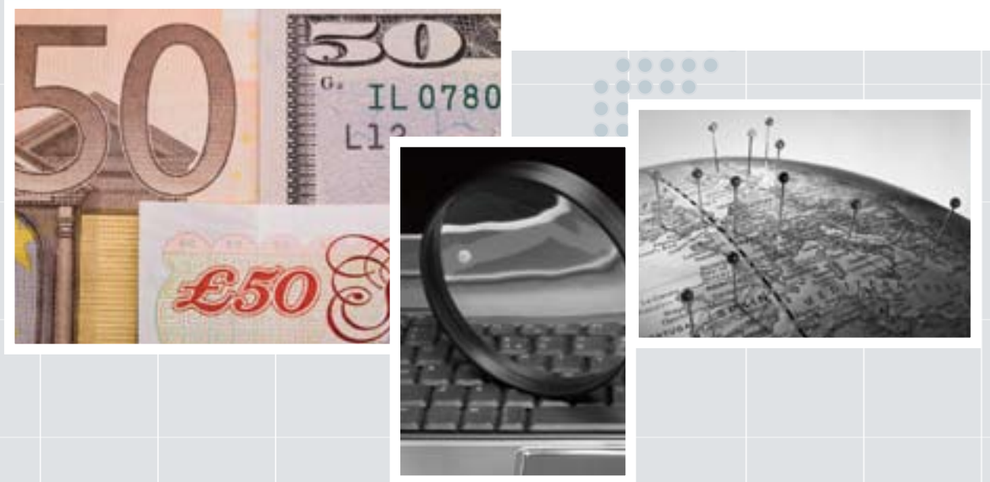
Three Key Findings Emerged

First, cybercrime isn't yet enough of a priority for governments around the world to allow the fight against it to make real headway worldwide. Added to that, the physical threat of terrorism and economic collapse is diverting political attention elsewhere. In contrast, cybercriminals are sharpening their focus. Recession is fertile ground for criminal activity as fraudsters clamour to capitalize on rising use of the Internet and the climate of fear and anxiety. Are we in danger of irrevocably damaging consumer trust and, in effect, limiting the chances of economic recovery?

Second, cross border law enforcement remains a long-standing hurdle to fighting cybercrime. Local issues mean laws are difficult to enforce transnationally. Cybercriminals will therefore always retain the edge unless serious resources are allocated to international efforts.

Third, law enforcement at every level remains ad hoc and ill-equipped to cope. While there has been progress, there is still a significant lack of training and understanding in digital forensics and evidence collection as well as in the law courts around the world. The cyberkingpins remain at large while the minor mules are caught and brought to justice. Some governments are guilty of protecting their in-country offenders. The findings suggest there is an ever greater need to harmonize priorities and coordinate police forces across physical boundaries.

The report concludes with a look at suggested steps at both the local and international level to make the fight against cybercrime more effective.

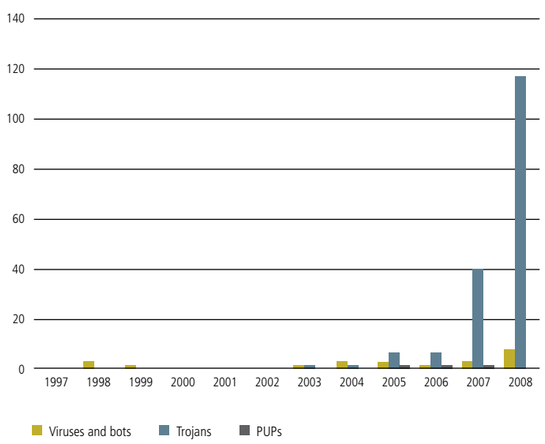


CHAPTER ONE
Global Meltdown – The Scale of the Problem

The scale of the Internet's security problems increases rapidly. Criminals have exploited vulnerabilities in both software and human psyche to spawn a broad range of threats including spyware, phishing, adware, rootkits, spam, and botnets.

The last 12 months have seen the volume of malware rising dramatically, yet cybercriminals are increasingly using tried and tested techniques to wreak havoc and solicit money.

Malware and PUP growth[1] (main variants)
In thousands



1 A PUP (potentially unwanted program) is a program that is unwanted despite the possibility that users consented to download: PUPs include spyware, adware, and dialers.

How the Economic Downturn is Set to Exacerbate Security Issues

Online fraudsters are using a variety of untraceable means by which to launder the proceeds of crime

The Gold Rush

E-gold is a digital gold currency that allows for the instant transfer of gold ownership. Unlike in the case of credit cards, all payments are final and irreversible. There are currently more than five million e-gold accounts worldwide. Due to the anonymity provided to account holders it became a popular method for cybercriminals to turn ill-gotten proceeds into clean cash.

In July 2008, the brother of Joseph Yobo (the vice captain of the Nigerian national soccer team and one of the English Premier League Club Everton's top soccer players), was kidnapped and a ransom of $10,000 was demanded in e-gold. This was clearly a new digital twist on an old crime.

Also in July 2008, e-gold Ltd. and its three directors pleaded guilty to money laundering charges and the "operation of an unlicensed money transmitting business." While e-gold's executives are still to be sentenced, the company is confident that the business can reinvigorate itself.

In October 2008, e-gold made moves towards becoming fully legal by registering with the Financial Crimes Enforcement Network (FinCEN), one of the US Department of Treasury's lead agencies in the fight against money laundering.

Cybercriminals Are Becoming Increasingly Mobilized and Untraceable

A vast number of insecure Internet-connected machines now provide a safe haven for cybercriminals. Recent figures suggest that the number of compromised zombie PCs in botnets has quadrupled in the last quarter alone and that these are capable of flooding the Internet with more than 100 billion spam messages per day. Botnets are increasingly switching to phishing, distributed denial of service (DDoS) and website attacks which are capable of causing a huge amount of damage and are a growing threat to the security of nations, the national information infrastructure, and the economy.

New ways of laundering illicitly gained money are also emerging. Online fraudsters are using a variety of untraceable means by which to launder the proceeds of crime. While previously fraudulent payments could be tracked and recovered within the banking system, experts now agree that the law has not kept up with innovations in payment systems.

Online fraudsters are increasingly using non-bank payment services, for example e-gold. This is making the old style mantra of "follow the money" harder and harder to negotiate in the cybercrime era.

Cybercriminals are also turning to the currencies in virtual worlds as a way to legitimize money. For example, they are able to set up an account, fund the account with the proceeds of fraud, malware and other illegal activities, and have an associate on the other side of the world who withdraws funds as profits, or even as working capital for another criminal enterprise. Alternatively, with the sending of messages being free in online worlds, money can also be reinvested into spam campaigns and laundered as revenue from those ventures.

Additionally, the spread of m-payments (payment via mobile phone) in less developed countries – which often lack regulatory frameworks and where corruption is rife – will likely increase the ease of money laundering in cybercrime as well as terrorist financing.

Cybercriminals to Benefit from Global Recession

The situation is set to worsen as the more headturning concerns of the global economic crisis and the continued war on terror divert attention. Ironically though, there has never been more need for focus on Internet security as the opportunities for cybercriminals to cash in have never been greater and the cost to consumers, industry and national security continue to escalate.

As Matthew Bevan, a reformed hacker, explains: "I don't think that cybercriminals are using new techniques, they are just using slightly different approaches to fool people. The latest and most effective threats tend to be automated attacks as they are much easier for cybercriminals to carry out and will provide better bang for their buck, so to speak. The less they have to invest, be it time or money, to provide better pickings, then this is where it will go."

Today, while monies spent on the investigation and prosecution of cybercrime is increasing, it still has some way to go

Cybercriminals are Capitalizing on Consumer Fear

Cybercriminals are cashing in on the fact that the economic downturn is causing people worldwide to increasingly turn to the web to seek the best deals, jobs and to manage their finances. They are preying on fear and uncertainty and taking advantage of the fact that consumers are often more easily duped and distracted during times of difficulties. In fact, opportunities to attack are on the rise.

As Philip Virgo, Secretary General of European Information Group Society (EURIM), The Information Security Alliance in the UK, warns: "We are seeing rounds of phishing emails which purport to be from banks responding to the crisis. We are also seeing a round of phony Curriculum Vitae (CV) sites, whose main aim is to collect personal details."

There is also the risk that as job security becomes more volatile and unemployment rates rise, consumers may be tempted by the fast buck of Internet money-making schemes and in fact end up as "mules" for cybercrime gangs. Recruited as "international sales representatives," "shipping managers" or other fake jobs, mules are asked by fraudsters to receive "payments" which they then transfer internationally after deducting a small "commission."

Similarly, there are sites that offer people money simply to add a few lines of code to their web pages. In this sense, they are becoming the most basic type of mule – they are the attack point.

Matthew Bevan agrees that consumers are increasingly at risk from cybercrime: "In the current economic climate where people are much more concerned with money, people are more likely to fall for the old-style, 'get rich quick' scams as their guard will be down. I am sure we'll see attacks like this increase and they will keep increasing into next year. The credit crunch is also hitting the cybercriminals – they'll be working even harder to make money."

He continues: "I also think there will be more victims of cybercrime as security is something that isn't visibly beneficial, and some people may start cutting corners – for example, choosing not to update to latest patches or versions of security software which puts them even more at risk."

Yet, e-commerce and e-government are dependent upon consumer trust and confidence online and are therefore critical to economic recovery and ongoing development.

As Alana Maurushat, Acting Director of the Cyberspace Law and Policy Centre of the University of New South Wales in Australia, summarises, consumers will eventually drive demand for cybersecurity at every level: "Consumers are, in true form of the tortoise, slowly crawling their way to becoming educated on security matters. This will have a trickle-down effect similar to green consumer movements. Where consumers have demanded environmentally friendly products, they will eventually demand safe products and services, inclusive of secure Internet transactions."

"A few years ago, the seesaw had equilibrium: there was an insufficient level of security investment from both the private and corporate side as well as the cybercrime law enforcement side … Today, while monies spent on the investigation and prosecution of cybercrime are increasing, it still has some way to go.

We have gone from an inactive to a reactive approach. Active prevention is the missing key component."

Industry Faces Balancing Act Between Short-Term Spend and Long-Term Losses

A key problem in the wake of the credit crunch may be whether laws ensuring greater security can be regarded as feasible or acceptable to industry, given the weak financial state of many industry sectors, especially banks.

An opposing argument would be that laws are essential in poor financial times, as compliance requirements will take precedence for spending over other desirables.

Peter Sommer, Visiting Professor at the London School of Economics' Information Systems Integrity Group and Visiting Reader at the Open University in the UK, remains optimistic that the need for spend to reduce potential losses will be recognized, though is conscious of the cost of industry consolidation. The hasty amalgamation of piecemeal and varied IT infrastructures will likely expose compliance issues while also putting valuable data at risk.

"Although one might think that the credit crunch will hit security spend, many recent conversations persuade me that most businesses do now realize that security budgets should be a function of efforts to reduce loss, not some arbitrary proportion of information and communications technology (ICT) infrastructure costs. A number of security managers in financial institutions think they will have actually to increase their budgets to meet the needs of the new compliance and regulatory frameworks. A further problem will be handling the transitional costs of forced, speedy mergers between institutions where two ICT infrastructures and two differing corporate cultures must now become one."

Businesses must be cautious to fully evaluate their risks and assets, and to allocate security spend accordingly. Security in a downturn is essential to preserving good business practice, reputation, and public confidence.

Mary Kirwan, an international lawyer and former cybercrime prosecutor in Canada believes that the downturn is taking business back to basics. This can have a positive effect if done appropriately but will have disastrous consequences if vital gaps in security are allowed to develop:

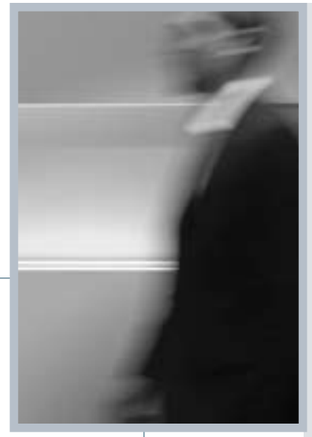
"There's a flight to quality, to safety, to studying the fundamentals. Complexity is out and simplicity is in. Business is going back to basics. Risk management is back in vogue. Security needs to move to where it belongs – up the value chain, as a critical component of a rational risk management strategy. If positioned in this way, its future is rosy."

"However, rebuilding trust is clearly essential to re-establish order from chaos in global markets. It will not be repaired if companies add insult to injury by disrespecting sensitive consumer data, and selling customers down the hacker highway."

Constant Threat of National Attack

Last year's report focused on how the Internet was increasingly becoming a weapon for political, military and economic espionage. It is a trend that has not dissipated over the last twelve months, with reported attacks still continuing to rise.

The threat of cyberterrorism has been commonly cited as over-hyped, yet there is a growing swell of opinion that hackers will eventually be bold enough and powerful enough to launch attacks that will damage and destroy critical national infrastructure.



Case Study **The Growing Evidence of Cyberespionage and National Attacks**

In May 2008, Belgium and India joined the growing force of countries claiming to be victims of attacks, believed to be originating from China. Thought to be a target because it houses the headquarters of both the EU and NATO in Brussels, Belgium has had emails containing spyware sent to State departments. Similarly, India claims its government and private sector networks are under constant cyberattack.

In August 2008, a coordinated cyberattack was launched against Georgia's infrastructure, compromising Georgian government websites including the Ministry of Foreign Affairs. The Georgian government said the disruption was caused by attacks carried out by Russia in connection with the conflict between the two States over the province of South Ossetia.

Case Study **Steps to Heighten Security Deemed Unnecessary by Government**

In August 2007, the UK House of Lords science and technology committee warned the government that the Internet was increasingly becoming a "Wild West" outside the law and stated that immediate action was needed to stop the web from becoming a "playground of criminals." They highlighted that fear of e-crime was surpassing that of mugging and that without essential measures and incentives being put in place to take control of security, public confidence in the Internet would be lost.

In November 2007, the UK government elected to reject almost every one of the report's suggestions as unnecessary.

Peer Lord Broers, who chaired the Committee's Internet security sessions, said: "In our initial report we raised concerns that public confidence in the Internet could be undermined if more was not done to prevent and prosecute e-crime. We felt that the Government, the police and the software developers were failing to meet their responsibilities and were quite unreasonably leaving individual users to fend for themselves."

However, subsequent to the massive data breaches which have plagued the UK government agencies such as the Her Majesty's Revenue and Customs (HMRC) in the last year, the House of Lords has reiterated its basic recommendations and they may be given more attention this time.

In October 2008, at the International Conference on Terrorism and Electronic Media, it was highlighted how the Internet is now the leading source for the creation of terrorist threats, and that there are now over 7500 sites linked with terrorist threats on the web.

The potential is significant, and governments must continue to ramp up resources in the fight against cybercriminal activity even in the face of global economic recession.

Governments Failing to Prioritize Security

Despite the evident increasing risk to national security, governments are still floundering at the first hurdle when it comes to cybercrime. They are failing to view cybersecurity as a priority due to technical ignorance and lack of foresight of the widespread and longer term risks and are neglecting to prioritize legislative time and resources to it.

Peter Sommer, Visiting Professor at the London School of Economics' Information Systems Integrity Group and Visiting Reader at the Open University, declares: "Cybercrime was a bigger government concern in the late nineties when the Blair administration was convinced Britain must become high-skills economy and the best place in world to do e-commerce – even then it was a struggle to get the National High-Tech Crime Unit (NHTCU) funded. NHTCU ceased to exist in 2006 when the National Crime Squad disappeared and SOCA (Serious Organised Crime Agency) is not part of the structure of UK policing – and its original 'stealth' mode of operation lost public confidence through invisibility.

"From Spring 2009 we will have a Police Central e-crime Unit (PceU), but it has taken a long time and it is still very under-funded. The public is still likely to be very confused about where to report a cybercrime. There will also be three quangos devoted to fraud reporting and intelligence and with the City of London Police as the fraud lead. Elsewhere there will also be the Serious Fraud Office. All this is a recipe for inter-agency disputes. Overall, cybercrime has not been fashionable in Labour government circles, having lost out to terrorism and antisocial behavior."

So what will happen if cybercrime continues to be overlooked or de-prioritized?

Mary Kirwan, international lawyer and former cybercrime prosecutor in Canada sums it up: "The bad guys will inherit the earth, and we will be left swinging in the wind.

"The Achilles heel of the technology sector is the same vulnerability that has the financial services sector currently on its knees: a wealth of arrogance. Complexity is worshipped as an end in itself, and simplicity is scorned. There's no understanding of critical interdependencies, through lack of communication. We've a poor grasp of what glues the Frankenstein monster we've created together, and what can just as equally tear it all apart.

"But the bad guys are in the know, and they are ready to exploit the demonstrable lack of big picture thinking in the sector."

CHAPTER TWO
The Front-Line Fight Against Cybercrime

Across the globe there is evidence of cybersecurity initiatives, but given the billions lost to cybercrime every year, is it a case of too little, too late?

EUROPE The European Network and Information Security Agency (ENISA) is a centre of expertise for the EU member states and EU institutions in network and information security. It contributes to modernizing Europe and securing the smooth functioning of the digital economy and the information society. In 2008, it had a budget of 8 million.

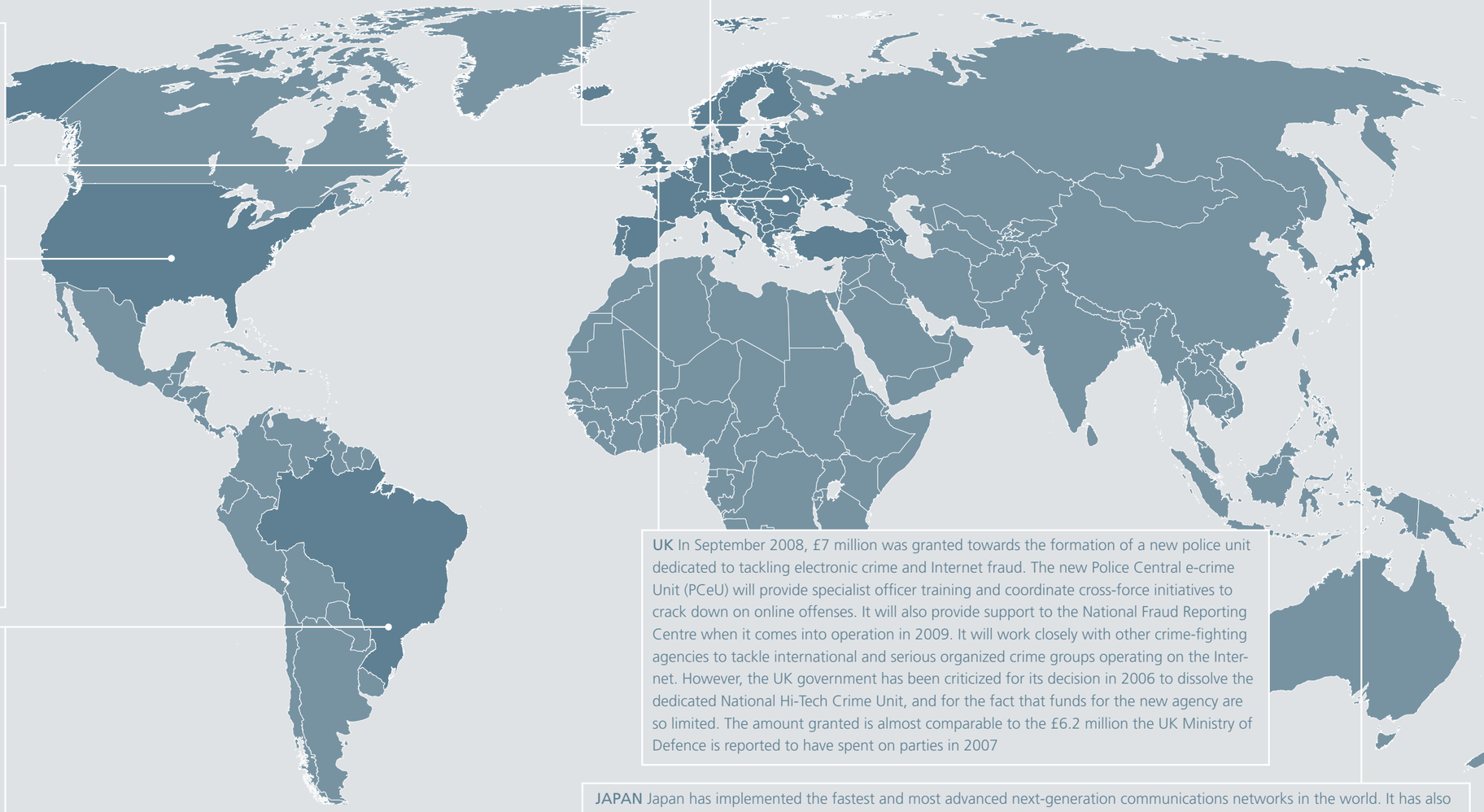
US The US spends the most amount of money on cybersecurity and has the most sophisticated technical staff and researchers working on these problems – at universities, in the commercial world and in government – of any country in the world. In 2008, the Department of Homeland Security has budgeted $155 million for cybersecurity and is gunning for $200 million in fiscal 2009. President Bush also looked for $17 billion from Congress for a cybersecurity initiative. However, the National Cybersecurity Initiative has been criticized for spending billions on "unproven, embryonic technology, and possibly illegal or ill-advised projects," and it has been said that it focuses too much on internal surveillance rather than actively defending against attacks.

Obama has pledged to appoint a national cyberadvisor to synchronise activity, reporting directly to him (rather than three steps away as per the Bush administration). He views cybersecurity as a "top priority" in the twenty-first century. Yet the details of his plans remain vague.

BRAZIL Classed as one of the top three most infected countries in the world for zombie machines and botnet activity, Brazil was also victim to 166,987 attempted cyberattacks in 2008, the third highest in the world. But Brazil is fighting back, and is revisiting the ratification of the Council of Europe's Convention on Cybercrime by means of bills consistent with this Convention. However, there is significant disagreement between the bills being processed in the Brazilian legislative houses. There is even a bill that, in practice, represents a step back in the investigatory advancements achieved so far.

ESTONIA Although small, Estonia is regarded as one of the most technologically capable countries in Europe in the cybersecurity and anti-cyberterrorism stakes. This proactivity has been prompted by the high-profile and repeated DDoS attacks on its government, news and bank servers in April 2007. In May 2008, Estonia established a top secret cybersecurity hub, operational as of August 2008 and backed by NATO and seven EU countries (Estonia, Germany, Italy, Latvia, Lithuania, Slovakia and Spain). Estonia has also pledged 50,000 to back the Council of Europe Convention on Cybercrime

ROMANIA Romania has been taking major steps to crack down on cybercrime by adding new hacking laws and strengthening its ability to fight cybercrime. This was prompted by timely phishing attacks by Romanian crime gangs that were hurting US banks to the point where some companies were blocking all Internet traffic from Romania. This coincided with official efforts to strengthen ties with the West and attain NATO membership, so clamping down on cybercrime became a focus. In 2008, Romania again cooperated with the FBI to arrest dozens more Romanians in an online fraud gang



UK In September 2008, £7 million was granted towards the formation of a new police unit dedicated to tackling electronic crime and Internet fraud. The new Police Central e-crime Unit (PCeU) will provide specialist officer training and coordinate cross-force initiatives to crack down on online offenses. It will also provide support to the National Fraud Reporting Centre when it comes into operation in 2009. It will work closely with other crime-fighting agencies to tackle international and serious organized crime groups operating on the Internet. However, the UK government has been criticized for its decision in 2006 to dissolve the dedicated National Hi-Tech Crime Unit, and for the fact that funds for the new agency are so limited. The amount granted is almost comparable to the £6.2 million the UK Ministry of Defence is reported to have spent on parties in 2007

JAPAN Japan has implemented the fastest and most advanced next-generation communications networks in the world. It has also been exposed to a series of damaging malware attacks and data breaches in recent years, particularly via Winny Peer-to-Peer (P2P) worms. Japan has fought back in an unusual way by prosecuting the inventor of the Winny P2P system for assisting in copyright infringement. This unconventional approach was used because Japan lacks adequate laws criminalizing the writing of viruses. Japan's ISPs are also playing an active role in stopping malware – four of the country's major ISPs have launched a collective plan to forcibly terminate Internet access of users caught using Winny-style P2P technology. However, the government's slow implementation of the provisions of the 2003 Act on the Protection of Personal Information does not encourage the public or private sectors to treat security issues as seriously as they should.

Research shows that while many attacks are routed through faraway countries, they are just as likely to originate close to victims

The High–Tech Crime Scapegoats

Cybercrime activity has often been cited as being primarily organized from legal havens such as Moldova and developing states such as Brazil and China. However, research shows that while many attacks are routed through faraway countries, they are just as likely to originate close to victims – where it is much easier to transfer money out of bank accounts.

"It's a myth that hackers are 15-year olds in darkened rooms, and similarly that all cybercriminals are overseas," said Bob Burls, Detective Constable at the Metropolitan Police Computer Crime Unit in the UK. "As with drugs, you have major traffickers but also street dealers. Wherever there is criminality there are criminal hierarchies, and there will also be local pockets of criminality."

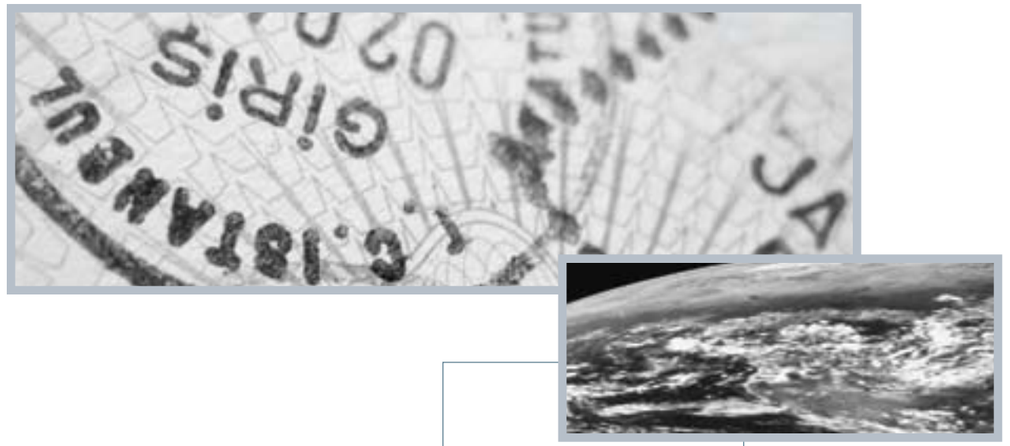
Eugene Spafford, Professor of Computer Sciences at Purdue University and Executive Director of the Centre for Education and Research in Information Assurance and Security (CERIAS) in the US, also highlights that criminals are increasingly clever in their attempts to disguise their "location" and are often much closer to home than at first assumed:

"I've been working with some law enforcement agencies trying to track down fraud that appears to be coming from other countries. Some of it may be originating in those other countries, but some of it may be originating down the street where somebody is accessing and using a computer in another country as a way of hiding their participation."

Alana Maurushat, Acting Director of the Cyberspace Law and Policy Centre of the University of New South Wales in Australia, believes that it is a rising trend and that some countries have been commonly used as scapegoats for criminal activity:

"At the moment, Brazil is the scapegoat, with the Chinese and Vietnamese rerouting traffic from these points. But the really interesting element is that the actual attacks are being carried out locally without being picked up."

"In fact, obfuscation seems to be the name of the game. It is easy to make it appear as if malware or espionage activities are originating from a country other than their original source. There is considerable misdirection as to origin of attacks. Much traffic is misdirected as a decoy. The actual attack may originate in the same city as the target. This is often done with cases of country espionage and corporate espionage."



Are We Catching the Cyberkingpins? Experts Don't Believe We Are

Cybercrime efforts and arrests may be widely touted but experts agree that those caught and brought to justice are traditionally the 'money mules' rather than the cyberbarons of crime.

"Phishing is most commonly dealt with by catching the money launderers rather than the phishermen who design the deceptive emails. In one of the biggest cases to date in the UK, the main perpetrator disappeared to Russia while minor mules were caught. It was a very expensive investigation that got little publicity," said Peter Sommer, Senior Research Fellow at the London School of Economics' Information Systems Integrity Group.

He continues, "In general, international transactions are very easily traced. Harvesters of account details sell blocks of information with some level of guarantee via covert websites and are difficult to track down. Their buyers therefore have to take risks to convert the information into cash, for example, through cash withdrawals, credit card spend, loan fraud; to do so they in turn employ expendable mules who in fact bear the greatest risk of being caught. Money has been laundered through fake auctions and casinos."

"DDoS attacks almost always lead to blackmail and should be dealt with in the same way, by catching the perpetrators at the point at which the ransom is paid. It is just too hard to identify the authors of attacks, and we will continue to see an arms race between attackers and defenders."

Paulo Lima, criminal lawyer in Sao Paulo, agrees that the cyber mafia men remain at large due to law enforcement's slowness to adapt and keep up with this growing and increasingly effective cyberthreat:

"There have been a few cases where cybercriminals have been promptly arrested, but they're usually responsible for the small attacks. Those responsible for the large operations have never been arrested. The public sector has usually acted in a mitigating manner, attacking the symptom and not the illness – there is an antiquated legal system and a completely unprepared law enforcement body."

Cybercriminals Are Protected from Prosecution

Catching the mafia men of the cyberworld is even harder when they are shielded from prosecution by political sympathies.

As Eugene Spafford, Professor of Computer Sciences at Purdue University and Executive Director of the Centre for Education and Research in Information Assurance and Security (CERIAS) in the US, explains:

"Criminal behaviour is still receiving political cover. For example, in the case of the Myanmar denial of service attacks, they took place with local Eastern European and Russian support. Russia and China are especially reluctant to cooperate with foreign law enforcement bodies for reputation and intelligence reasons."

The implication is that elements of Russian intelligence agencies are protecting the country's cybercriminals.

Alana Maurushat, Acting Director of the Cyberspace Law and Policy Centre of the University of New South Wales in Australia, believes that it is a case of mutual support: "Criminal behaviour has always received political cover from governments. It is a double edged sword. Quite often, those with the expertise and technical skill set that governments require to successfully handle tasks, are often hackers themselves. It has been my experience that hackers wear multiple hats: some black, some white, and many grey."

The Cybercop Shortage: Lack of Understanding and Training of Police and Law Courts is Stifling Progress

Experts agree that cybercriminals are also effectively immune to arrest due to the inability of policing to keep up with the digital age.

The Internet often holds the evidence that could bring cybercriminals to justice. Yet, digital tracing and forensics are often overlooked or ignored because those involved, from investigations through to trial, are untrained in how to comprehensively unearth and exploit it.

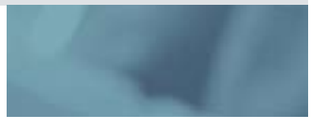
"There are mountains of digital evidence out there; the problem is that there aren't enough well-trained investigators, prosecutors and judges to use it effectively. With PC and broadband penetration increasingly high, direct and indirect evidence is easy to find from machines.

Few criminals have the technical ability to avoid leaving or wiping digital traces," said Peter Sommer, Visiting Professor at the London School of Economics' Information Systems Integrity Group and Visiting Reader at the Open University.

Case Study **Myanmar Attacks – Political Protection**

In July 2008, the websites of the Oslo-based Democratic Voice of Burma (DVB) and New Delhi-based Mizzima News were hit by DDoS attacks that shut down their websites for several days. In August two community forums, Mystery Zillion and Planet Myanmar, were disabled and shut down and on September 17, The Irrawaddy, DVB and the Bangkok-based New Era Journal also experienced similar attacks.

It is thought that these concerted attacks were coordinated by the Burmese government in anticipation of the first anniversary of The Saffron Uprising – a peaceful protest by Buddhist monks, nuns, and students against an oppressive military regime. The websites were all known to support the monks. The attacks all appeared to mainly originate from China and Russia, the main diplomatic backers of the junta (military-led government) and where it has been suggested the junta have been receiving technical training.



"In the UK, complex cases are generally well-investigated, as there is a small core of police that are highly proficient in cyberinvestigations. The problem is that most of their colleagues are yet to understand where digital evidence exists, how to access and use it, and how to interact with forensic investigators."

Paulo Lima also backs the thinking that cyberlaw enforcement needs to have more of a background in the specific technicalities of cybercrime. In Brazil, while ad hoc attempts have been made to try to address the problem, for the most part investigations are undertaken by officers ill-equipped to understand the intricacies of Internet-based crimes:

"In some states there are specialized prosecutor (district attorney's) offices (Rio de Janeiro and Minas Gerais). As for the rest, the investigation is done by the entire law enforcement body indistinctly, generally police not properly trained to effectively fight this type of crime."

Matthew Bevan, a reformed hacker, agrees that the challenge for cybercrime is in recruiting people with the right skill set: "I don't think law enforcement is equipped to deal with cybercrime, and this has always been the case as people that love IT and have the right skills go into IT jobs, not a law enforcement role. It is extremely rare that an IT specialist would join the police. Therefore, law enforcers lack the right skills to interpret cybercrime and know what to look for. A simple example could be a new USB stick that looks like a torn cable but actually holds 4GB worth of data – the police wouldn't recognize this."

It's not only the police forces on the front line that are struggling to effectively track down offenders but, where cases are brought to caution, the lack of understanding in law courts is also impeding the path to rightful penalties and convictions.

Equally, sentencing has been traditionally based on physical damage levels, where you can actually see the impact of the crime. However, with cybercrime it can be much harder to ascertain the extent of the damage done. One of the challenges for law enforcement is in getting victims involved, either because they don't realize or because they, especially in the case of businesses, don't want to admit to having been vulnerable to attack.

Vijay Mukhi, President of the Foundation of Internet Security and Technology (FIST) in India said:

"Cybercrime has become a big problem in India this year. However, politicians and judges do not understand how to deal with it, and in fact few of them ever use the Internet. Police are reluctant to register cases because they are too difficult to prosecute. The Indian IT Act 2000 has some relevant provisions but has resulted in only one successful prosecution, of credit card fraudsters. Generally, fraud and trade secrecy provisions are civil offenses and hence will not be investigated by police. Kingfisher Airlines recently lost four or five million dollars due to stolen credit cards. After Kingfisher complained to the police, no other airlines complained of similar frauds because nothing happened."

4205 5622350479
658. 7895200.02.
33695 454868.45 5 48
4528782

45 4582 688.54 58 89
8 488.5545 6896

44 822.656

4568 45 4582 688.54
58

486 86484 8 8

6541215.23. 5656

565.369 21 4477787
4651

546 78952

5

65271

Mary Kirwan, an international lawyer and former cybercrime prosecutor in Canada, also comments: "Judges and juries both get overwhelmed with technological gobbledygook. There are training programs in Canada and Ireland, but again the problem is the gap between the tech savvies and those not. Judges should also be trained to have a great deal of skepticism about technology and its security."

Peter Sommer, Visiting Professor at the London School of Economics' Information Systems Integrity Group and Visiting Reader at the Open University, added: "In the UK, experts have recently been better used by the courts, for example, Criminal Procedure Rules allow prosecution and defence experts to agree on consensual matters, such as how technology works and sometimes on a chronology of events. However, the Council for Registered Forensics Practitioners scheme to accredit experts is still not yet working. Assessment criteria must be fluid in such a fast-moving field, but this increases the expenses of accreditation, especially if it is to be meaningful. This may need to be made compulsory."

In addition, victims need to do more to protect themselves, in the same way that they do in the physical world, especially when it comes to preserving evidence. Companies need forensic readiness programs. Individuals need basic training and advice.

How Cyberspooks Are Being Poached for Private Enterprise

In the rare cases where police are being effectively trained to tackle the unique technical challenges of the cybercrime industry, rewards and incentives are often misplaced and damaging morale.

"Police career rewards go to managers rather than front-line specialists, for example, some of the best digital investigators are still detective constables or sergeants," commented Peter Sommer.

Commonly, this has led to cybercops being successfully poached by private enterprise with the promise of higher wages, resulting in wasted investment and leaving behind a dearth of essential experience.

7894152 02 30

Case Study **E-Experts Ignored**

In January 2007, Julie Amero, a substitute teacher in Connecticut, was convicted on four counts of risk of injury to a minor, following exposure of her pupils to pornography that popped up during a lesson on a school computer back in 2004.

Internet experts agreed that she was a victim of circumstance – that it was malicious malware that popped up unprompted, allowed to get through because the school's Internet filters weren't working properly that day.

According to the defense's expert witness, the defense at the first trial was not permitted to present prepared evidence in support of this theory.

Sentencing was delayed four times due to agreed lack of evidence and failure to assess the case properly. Eventually in June 2007, the conviction was thrown out, and she was granted a new trial.

Case Study **The Fine Line Between Cybercop and Criminal**

In 2003, hacker Brian Soledo was sentenced to nine years in prison for trying to steal credit card details from Lowe's hardware chain in the US. He had in fact tried to back out of the scheme but was forced to go through with the online raid when he was threatened by the buyer of the credit cards who had already been lined up.

In August 2008, it emerged that the buyer, who operated under the name SoupNazi, was 27-year-old Alberto Gonzalez and that at the time he was working for the federal police. He was arrested in Miami in possession of more than $20,000 in cash.

Authorities admitted that Gonzalez was working as an informant in a separate US Secret Service hacking investigation. He was using information from their probe to help fellow hackers avoid arrest.

Alana Maurushat, Acting Director of the Cyberspace Law and Policy Centre of the University of New South Wales in Australia, said: "Canadian, Australian and American local and state police find it extremely hard to recruit cybercops, often due to small hurdles like requirements to do seven years on foot patrol or fitness requirements. Once staff are trained, they are then often poached by industry at much higher salaries."

There has also been the occasional case of trained cybercops being lured into and recruited by the criminal underground. Police forces, therefore, need to ensure that there are clear career paths for specialist cybercrime-fighting agents.

However, while specialist training for cyberspooks is no doubt essential, there is also a need to balance their unique expertise with the core policing skills to ensure that they retain rounded proficiencies and instincts rather than wholly focusing on technologies.

As Mary Kirwan, international lawyer and former cybercrime prosecutor, warns: "We shouldn't ghettoize cyberenforcement and be carried away by the mystique of technology, to the detriment of traditional police skills. This is just crime in another medium and it's still all about the money. So traditional skills – using informants, gathering evidence, a lateral turn of mind to understand how criminals are thinking – are still the core needs and they still need the savvy to understand and exercise social engineering."

The De Factco Cybercops? The Crucial Role of ISPs in Cybercriminal Investigations

The Internet has historically not been regulated in the same way as, on the one hand, broadcasting and traditional media, and on the other hand, banks, financial, munitions, and other sectors – all industries which can potentially cause serious harm to basic societal interests. Yet the Internet is as crucial as the first as a communications medium and as likely to cause harm as the latter.

Experts agree that currently the main cybercops are in fact the ISPs. It is via unencrypted emails that many scammers are caught discussing their plans and that, when there is the legal authority to do so, has proved invaluable in police inquiries.

Both ISPs and other intermediaries, such as money transfer agencies, who can have an enormous impact on the success of global investigations, must therefore be engaged in the fight against cybercrime.

CHAPTER THREE
International Cooperation – Myth or Possibility?

Currently the Council of Europe Convention on Cybercrime is the only international agreement that covers all relevant areas of cybercrime legislation (Substantive Criminal Law, Procedural Law and International Cooperation). Adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001, it was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004.

The Cybercrime Convention – A Current Snapshot

Regional approaches also play an important role. This is especially relevant with regard to the criminalisation of illegal content where you find more similarities on a regional than on a global level. Examples for current regional approaches are: the European Union (EU), the Common Market for Eastern and Southern Africa (COMESA) states, Asia-Pacific Economic Cooperation (APEC), Organisation of American States (OAS) and the Gulf Cooperation Council (GCC).

1. **EC, the Council Framework Decision 2005/222/JHA on attacks against information systems,** was adopted by the Council of the European Union on 17 January 2005. The Framework Decision will ensure a common minimum level of approximation of criminal law for the most significant forms of criminal activity against information systems, such as illegal access, illegal system, and data interference. This includes the so-called "hacking" and "denial-of-service attacks" as well as the spreading of malicious code, spyware and malware and viruses. This approximation is desirable in order to avoid any gaps in Member States' laws that could hamper the response of law enforcement and judicial authorities at national level to these growing threats.

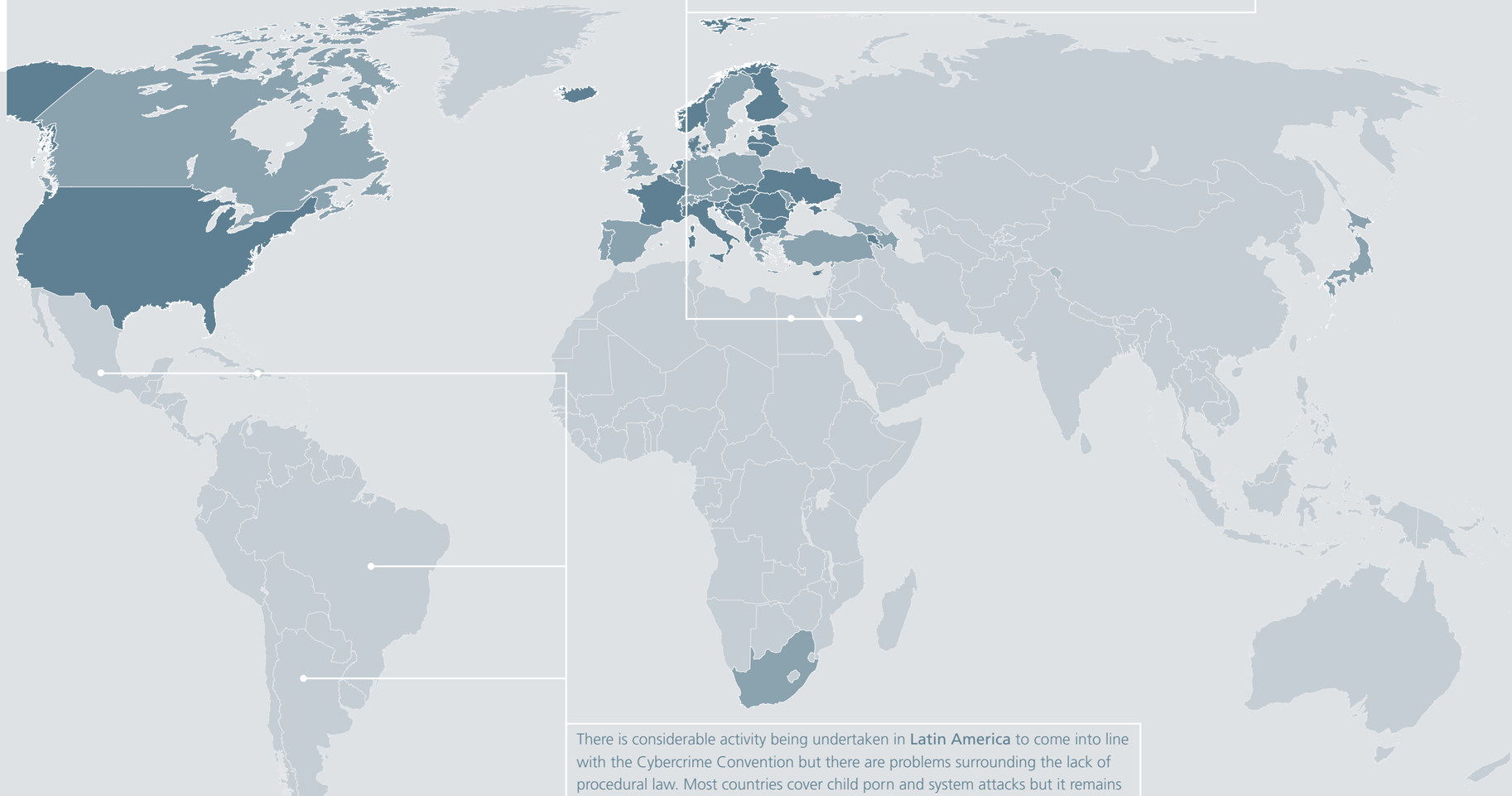
   European Program for Critical Infrastructure Protection (DG JLS) – The Directive has been drafted, while the criteria and guidelines are under development until year-end 2008.

2. **Other European group initiatives**
   G8 High-Tech Crime Sub Group
   EuroSCADA Group
   European Governmental CERT Group
   Forum of Incident Response and Security Teams

3. **http://www.virtualglobaltaskforce.com/. The Virtual Global Taskforce (VGT)** is made up of police forces from around the world working together to fight online child abuse.

Some regions, especially the **Arab regions**, feel they had no part in development of the Cybercrime Convention and prefer to put together their own regional instruments rather than accede – in most cases, however, such instruments remain in keeping with the Convention.

The **Gulf States** meanwhile have chosen to go the route of preparing their own law, with the Cybercrime Convention as a model. The UAE was the first country that enacted a comprehensive cyberlaw among the Gulf States. It has been working well against cybercrime in the country, but plans are underway to extend the law into other Gulf Cooperation Council (GCC) States.

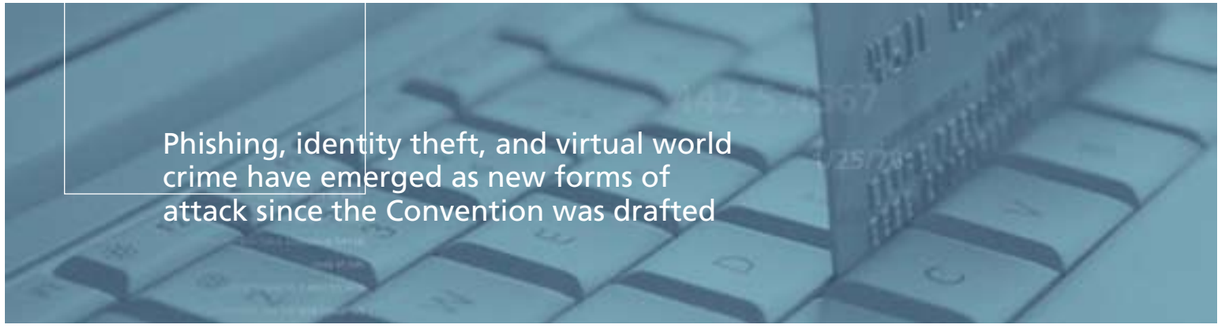


There is considerable activity being undertaken in **Latin America** to come into line with the Cybercrime Convention but there are problems surrounding the lack of procedural law. Most countries cover child porn and system attacks but it remains unclear as to whether botnets are illegal. Costa Rica and Mexico have been asked to accede to the Cybercrime Convention while Argentina and Dominican Republic already have working legislation. Brazil is drafting cybercrime legislation which is under debate but alleged to be "very tough."

Countries that are **ratified** with the Cybercrime Convention

Countries that are **signed** with the Cybercrime Convention

Countries who have yet to participate with the Cybercrime Convention



Phishing, identity theft, and virtual world crime have emerged as new forms of attack since the Convention was drafted

International Standards Stumble as Countries Fail to Synchronize

In total, 45 countries have signed up to the Cybercrime Convention to date, but after seven years since its inception, only half of them have successfully ratified it.

The Convention is viewed as having been mainly developed by the West, and of all the non-member States to have acceded, the US is the only country to have fully ratified. There are some notable exceptions.

However, Marco Gercke, Professor at the University of Cologne and UN and Council of Europe expert on the Cybercrime Convention, clarifies that it is proving a good harmonization model:

"You have to drill down into each country and region to see the success of the Cybercrime Convention. For example, Germany has not yet ratified only because it has one provision left to get right in its own country legislation."

Overall, it appears that the principle of the model is working, but some countries are still too focused on national concerns and priorities to think about the international greater good.

Peter Sommer, an expert in information systems and innovation at the London School of Economics in the UK, said: "The Council of Europe cybercrime treaty is working reasonably well, although some countries are still ignoring it. It provides standard definitions, mutual legal assistance and evidence exchange procedures, and makes extradition easier. Eastern European nations are less cooperative, especially Russia. They attend meetings – for example the G8 meeting 10 years ago – make promises, but do not follow through. They have been more cooperative on child abuse images. They make plain that they cannot prioritize fraud against non-Russians. Nigeria has been bad in the past but is now improving, especially in boosting their forensics capabilities."

One of the biggest problems in drafting cybercrime laws is in harmonizing definitions. It is a huge challenge to be able to get agreement on crime X being the same in State A and State B. Yet this agreement is essential for extradition as well as for evidence and jurisdiction.

The Cybercrime Convention has helped but has numerous get-out clauses meaning that synchronization has not really been achieved.

This lack of harmonization also affects comparative reporting and statistics and so the full scale and impact of cybercrime cannot be counted.

Law is Failing to Keep up with Cybercrime

Now seven years old, the Cybercrime Convention is also showing signs of being too dated to effectively address the modern-day attacks on the cyberworld.

Phishing, identity theft and virtual world crime have emerged as new forms of attack since the Convention was drafted which fails to offer explicit guidance on how to deal with them. This makes it difficult for local prosecutors and again adds to the problem of extradition if countries do not agree on a definition of, or response to, a crime.

Though these crimes can be covered under more general provisions, it makes it easier for prosecutors if there are nominate offenses. So do we need a new Cybercrime Convention?

Case Study **Heist at the Habbo Hotel**

Cybercriminality in virtual worlds is becoming an increasingly big problem. Virtual world gaming is starting to suffer from real-world problems – theft of identity and virtual assets, extortion, and even terrorist attacks. This is particularly evident in countries such as South Korea where 30 million of its 46 million people are active in social networks like CyWorld and police are seeing many attacks coming from China.

In November 2007, a Dutch teenager was arrested for allegedly stealing 4,000 worth of virtual furniture from rooms in Habbo Hotel, a 3D social networking and gaming website.

Five other teenagers were also questioned in connection with the case. The group apparently created fake Habbo websites and lured players into visiting them. Usernames and passwords were then harvested and used to break into the real accounts to steal the virtual furniture. The credits to buy furniture in the first place were purchased using real money.

Police are certain they will need better capacity to deal with such virtual crimes in future.

Marco Gercke, Professor at the University of Cologne and UN and Council of Europe expert on the Cybercrime Convention, disagrees with the need for a whole new structure but acknowledges that there is a definite lag in law. Regular reviews and updates are needed to take place to ensure that both laws and investigations stay in line with cybercriminal advancements:

"While we don't need a new model law, we could have added protocols to deal with new issues. I think that new scams should be addressed if the current legislation is not able to cover them. In a 2007 identity theft study for the Council of Europe, I pointed out that the Convention does not cover the transfer of obtained identities (identity theft). This could be an issue that needs to be covered in the future.

"The Convention was developed before the end of 2001. A lot of things have changed since that time. This is not only relevant with regard to substantive criminal law but the necessary procedural instruments as well. New investigation instruments like key-loggers ("Magic Lantern") and identification instruments (Computer and Internet Protocol Address Verifier) are already in use in countries like the US but not mentioned in the Convention."

International Cooperation Yields Success for Cybercriminals. Why is Law Enforcement Failing to Communicate?

As Ferenc Suba of CERT in Hungary comments: "The Council of Europe's Cybercrime Convention is a good guide for legislation. Operational needs now trump the need for new law."

Indeed, traditional law enforcement is strongly bound to physical national boundaries. Such distinctions generally do not exist on the Internet, so law enforcement by local agencies is very difficult."

Mary Kirwan, a former cybercrime prosecutor in Canada, highlights that while cybercriminals are organized and work fast together to ensure success, international law enforcement falls short at even simple communication:

"The law is irrelevant to most cyberhackers – they can operate out of anywhere. The reality for law enforcement is that if you want them to act as speedily and effectively as the international cybercrime community, you need to give them the tools. If the hackers share all their information, and businesses and governments share none of their information, you can imagine

205 5622350479 658. 7895200.02. 33695 454868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656 546 78952 565.369 21 4477787 4651

which does better. When a crime gang needs a document decrypted, say, they ping the community and an answer comes back like that."

In a handful of cases, international cooperation has successfully brought down cybercriminals, but experts are skeptical of the impact that it is having on cybercrime gangs who are quick to mobilize and move on.

"My previous experience, not only with credit card and similar exchanges, but also underground websites dealing in cracked software, hacking tools and indecent images of children leads me to anticipate that there are always several rival websites for each 'theme,' and although at any particular time one may dominate, the others will assert themselves if the dominant one disappears or is compromised for any reason," said Peter Sommer, Visiting Professor at the London School of Economics' Information Systems Integrity Group and Visiting Reader at the Open University in the UK.

The recent sting on a criminal forum called Dark Market by the FBI, in conjunction with other law enforcement agencies, is thought to be a drop in the ocean: while it is encouraging to see that efforts can be coordinated, it is not happening nearly enough.

Alana Maurushat, Acting Director of the Cyberspace Law and Policy Centre of the University of New South Wales in Australia, said: "Every five years a major bust like this is made and victory is claimed for the good guys. Dark Market forum, while a great sting, is merely one of many similar forums. I am not aware of any foreign parties being arrested in this operation, especially from countries where a significant source of this organized crime hails from, namely Eastern European countries. I do not see this as putting even a dent in the level of online fraud. That being said, the FBI and Federal Trade Commission (FTC) should be commended for this operation, as well as for a great deal more arrests that have been made recently for spam rings and botnet herders. It would be nice if non-US counterparts stepped up their investigations as well."

Case Study **Dark Market – International Triumph or the Tip of the Iceberg?**

In October 2008, an internationally coordinated crime operation saw the arrests of 56 members of a transnational criminal network used to buy and sell stolen financial information. The "carder" forum hosted on the Dark Market website had attracted more than 2,500 registered members before its closure.

In addition to the arrests, police seized compromised victim accounts to prevent $70 million in economic loss through identity fraud.

The FBI conducted the two-year operation with the assistance of the Computer Crime and Intellectual Property Section of the US Department of Justice, the UK's Serious Organized Crime Agency (SOCA), Turkish National Police – KOM Department, Bundeskriminalamt (German Federal Criminal Police) and the Landeskriminalamt Baden (State Police of Baden-Württemberg).

FBI Cyberdivision Assistant Director Shawn Henry said: "In today's world of rapidly expanding technology, where cybercrimes are perpetrated instantly from anywhere in the world, law enforcement needs to be flexible and creative in our efforts to target these criminals. By joining forces with our international law enforcement counterparts, we have been, and will continue to be, successful in arresting those individuals and dismantling these forums."

Without Global Communication, Information is Being Siloed and the Problems Are Expanding Exponentially

Cyberhacking, warfare, and crime are inherently transnational problems, presenting enormous problems to law enforcement in tracking down the perpetrators, collecting evidence, negotiating jurisdiction between investigating agencies and in courts, and arranging extraditions.

At the moment, effective policing by a national authority regarding a transnational crime requires mounting a joint operation every time from scratch, a highly expensive and time-intensive process. Interpol exists but does not seem to have a high profile in cybercrime policing.

As Richard Clayton from Cambridge University Computer Centre in the UK outlines: "Interpol is a fax passing mechanism – it has a limited intelligence function of its own these days, but doesn't aspire to leadership. Although its mechanisms can be used to coordinate, it does not itself attempt to set priorities, or choose when and where to deploy resources most effectively."

There is, therefore, the argument for the set up of a global task force specifically for transnational cybercrime investigations to go beyond the treaty and ensure action. It would help track and coordinate cybercrime across borders and help speed up response times.

Clayton continues: "The basic idea is to establish a central coordinating body with full-time members from all relevant forces. Essentially their role would be twofold, first to help achieve consensus, or at least high levels of support, on what criminality to deal with; and second to be able to liaise back with their home forces to provide appropriate logistical support to particular operations and to feed forward the ability or inability to assist to ensure that central planning is reasonably efficient. Whether it all worked in practice would come down to the effectiveness of the leadership for the coordinating body; along with sufficient high profile support from politicians in key states. But with support amongst at least the G8 players would help regain control along with the main hotbeds of wickedness."

However, given the number of bureaucratic bodies already involved in cybercrime, perhaps what is needed more is to rationalize and harmonize existing organizations.

CHAPTER FOUR
Next Steps

While the Council of Europe Cybercrime Convention is acting as a global model law where not directly adopted, and while most significant jurisdictions now have laws in place, legislation alone is not enough to reduce cybercrime to acceptable levels.

Where laws are too technology-specific, they go out of date quickly, their efficacy is heavily dependent on successful investigation and prosecution, and they struggle with the transnational nature of cybercrime.

There is the need for a holistic solution that goes beyond the criminal law.

Countries must be encouraged to harmonize laws at the highest level while putting massive effort into international cooperation.

The Need for a Collective and Holistic Approach to Combating Cybercrime

Media literacy programs for informed consumer choice are not enough to ensure users prioritize security over convenience or short term goals

Experts recommend that the following steps be considered and implemented at both a local and international level:

- Significantly more **training and resourcing for cybercops, prosecutors, and judges**, alongside the mainstreaming of cyberevidence gathering and prosecution.
- Legal or co-regulatory incentives for **Internet Service Providers** to follow best practice in network design and operation – Incentivizing ISPs in turn to work both with other service providers and their customers to improve levels of security. ISPs should also be encouraged to work closer with police as the gatekeepers of the Internet.
- **Security breach disclosure requirements** – We cannot expect a market in secure products and services to develop without the information needed to allow customers to quantify security levels. The new EU rules are a start but need widening beyond the telecoms sector and scrutinized to make sure they are not implemented in a token way, and to avoid customer 'security fatigue.'

  In the US, there are stopgap measures on a state level for data breach notification. Dozens of states have passed different laws. A simple, straightforward data breach notification standard is needed to help companies respond uniformly and seamlessly, and to ensure citizens get the widest level of protection, regardless of which state they are from. In addition, enterprises that hold sensitive personal information should meet a common security standard so the possibility of a breach is reduced.
- Legal responsibility for both **businesses and government agencies** when customers suffer Internet-related security losses, except in cases of gross negligence by customers. Banks in particular must be given strong legal and commercial incentives to introduce more secure technology and better fraud detection systems, or they will inevitably cut margins on security as they struggle to ride out the credit crunch and economic downturn. Clear bank liability would reward banks that are taking security seriously, greatly reduce the problems customers have faced, and correspondingly increase online trust and convenience – vital for e-commerce and e-government to flourish in future.
- **Continued consumer education** through focused programs. However, systems must be designed to make it difficult for users to make security mistakes – we cannot expect the average Internet user to become a security expert. Media literacy programs for informed consumer choice are not enough to ensure users prioritize security over convenience or short term goals.
- Limited liability for **software vendors** when they are not following best security practice in their system design and operation. We cannot stop the flood of malware until operating systems and key applications, especially browsers and email clients, are significantly more secure.
- The use of **government procurement power** to demand significantly higher standards of security in software and services – Incentivizing security enhancements that will spill over to private users. Government information assurance agencies should follow the example of the US National Security Agency in working with software companies to significantly increase software security levels.

CONTRIBUTORS

EMEA:

Dr. Ian Brown – Research Fellow at the Oxford Internet Institute, Oxford University, UK

Dr. Ian Brown is a research fellow at the Oxford Internet Institute, Oxford University, and an honorary senior lecturer at University College London. His work is focused on public policy issues around information and the Internet, particularly privacy, copyright, and e-democracy. He also works on the more technical fields of information security, networking, and healthcare informatics.

He is a Fellow of the Royal Society of Arts and the British Computer Society and an adviser to Privacy International, the Open Rights Group, the Foundation for Information Policy Research and Greenpeace. He has consulted for the US government, JP Morgan, Credit Suisse, the European Commission, and the UK Information Commissioner's Office.

In 2004 he was voted as one of the 100 most influential people in the development of the Internet in the UK over the previous decade.

Lilian Edwards – Professor of Internet Law, University of Sheffield, UK

Lilian Edwards leads a program of research and teaching at Sheffield University, focusing on the law relating to the Internet, the web and new technologies.

Her research interests are generally in the law relating to the Internet, the web, and communications technologies, with a European and comparative focus. Her current research focus is on the role of intermediaries and ISPs on the Internet, privacy and data protection online, cybercrime and cybersecurity, "Web 2.0" and the law, digital IP, and e-commerce. She has co-edited two editions of her bestselling book *Law and the Internet* (the third is due out in early 2009) and a third collection of essays *The New Legal Framework for E-Commerce in Europe*. Her work on online consumer privacy won the Barbara Wellbery Memorial Prize in 2004 for the best solution to the problem of privacy and transglobal data flows. She is an adviser to BILETA, the ISPA, FIPR, and the Online Rights Group, and has consulted for the European Commission and WIPO.

Matthew Bevan – Reformed Hacker and Computer Consultant

Mathew Bevan is a British hacker from Cardiff, Wales. In 1996 he was arrested for hacking into secure US government networks under the handle Kuji. He was 21 when he hacked into the files of the Griffiss Air Force Base Research Laboratory in New York. Intent on proving a UFO conspiracy theory, his sole tool was a Commodore Amiga loaded with a blueboxing program called Roxbox. He was one of two hackers said to have "nearly started a third world war," according to Supervisory Special Agent Jim Christy, at the time working for the Air Force Office of Special Investigations. He now runs his own computer consultancy business.

Sharon Lemon – Deputy Director, Serious Organized Crime Agency (SOCA), e-Crime, UK

Deputy Director Sharon Lemon of the Serious Organized Crime Agency (SOCA) is Head of e-Crime and Crime Techniques Departments.

Sharon started her career with the Metropolitan Police and has served at many busy inner London divisions at all ranks, until she joined the National Crime Squad (NCS) in 1999. She has held a number of key portfolios, including the Head of Firearms and the Pedophile On-Line Investigation Team – a precursor to the Child Exploitation and Online Protection Centre. She also played a key role in the formation of the Virtual Global Taskforce (VGT), an international law enforcement collaboration comprising Australia, Canada, Interpol, the UK and the USA.

Until April 2006, Sharon was head of the National HiTech Crime Unit (NHTCU), the first national unit responsible for the investigation of high tech crime. Since then she has developed the e-Crime Department within SOCA by encouraging a range of alternative interventions to compliment traditional prosecutions. More recently, she has taken on the additional responsibility of managing the Crime Techniques Department, which explores creative approaches to tackling organised crime by exploiting weaknesses in criminal networks and anticipates future crime threats.

Bob Burls – Detective Constable, Metropolitan Police Computer Crime Unit, UK

The Computer Crime Unit is a center of excellence in regard to computer and cybercrime committed under the Computer Misuse Act 1990, notably hacking, maliciously creating and spreading viruses and counterfeit software. The unit provides a computer forensic duty officer and offers computer evidence retrieval advice to officers.

Peter Sommer – Visiting Professor at the London School of Economics' (LSE) Information Systems Integrity Group and Visiting Reader at the Open University, UK

Peter Sommer's main research interest is the reliability of digital evidence, a subject which encompasses forensic computing and e-commerce. He has helped developed the LSE's social-science orientated courses on information security management. In the last Parliament he was Specialist Advisor to the UK House of Commons Trade & Industry Select Committee while it scrutinized UK policy and legislation on e-commerce. He was part of the UK Office of Science Technology's Foresight Study, Cyber Trust, Cybercrime. He sits on a number of UK Government Advisory Panels. Recent research contracts have been carried out for the UK Financial Services Authority and the European Commission's Safer Internet Action Plan. He is currently part of the European FIDIS Network of Excellence and also a member of the Reference Group (review mechanism) of another European Commission initiative, PRIME.

He is an external examiner at the Royal Military College of Science and an advisor on a number of law enforcement and other committees concerned with cybercrime and emergency response. He has advised Centrex, which provides high-tech crime training to UK law enforcement, and TWED-DE, a US DoJ-funded exercise to develop training on digital evidence. He has also lectured at UK and US law enforcement seminar on cyberevidence and intelligence matters.

He was on the program committee for FIRST 2000 in Chicago.

Peter Sommer acts as an advisor and surveyor for leading insurers of complex computer systems. His first expert witness assignment was in 1985, and his casework has included the Datastream Cowboy / Rome Labs international systems hack, the Demon v Godfrey Internet libel, NCS Operation Cathedral, Operation Ore and many other cases involving such diverse crimes as multiple murder, forgery, software piracy, bank fraud, credit card cloning and the sale of official secrets.

He is on the Advisory Council of the Foundation for Information Policy Research, a UK-based think tank.

Richard Clayton – Cambridge University Computer Laboratory, UK

The Computer Laboratory at Cambridge is the computer science department of the University of Cambridge. The Cambridge Diploma in Computer Science was the world's first taught course in computing, starting in 1953. Richard Clayton is a leading security researcher and a long-time contributor to UK security policy working groups.

Philip Virgo – Secretary General, EURIM, UK

Philip has been associated with EURIM since it was relaunched in January 1994. He was the first executive officer to be appointed and has carried the designation Secretary General since 1996. Philip was Finance Executive of PITCOM from 1982–2006 and remains on the Council and Program Committee. He was an external advisor to the High Tech Unit of Barclays Bank (1983–89), Campaign Director for the Women in IT Campaign (1989 – 92), IT Skills Advisor to the West London TEC (1991 – 2, a Specialist Advisor to the Information Committee of the House of Commons (1993–4), has been Strategic Advisor to the Institute for the Management Information Systems (IMIS, previously IDPM) since 1993 and has served on various advisory boards and committees.

Matthew Pemble – Security Architect and Advisor, UK

Matthew is an experienced security architect and operational manager, having worked for numerous international commercial and voluntary organizations, as well as for the UK government. Much of his recent experience has been in the combating of online fraud and other attacks against e-commerce and banking systems. Having led the Information Security Incident Response Team for Royal Bank of Scotland Group for five years, he has now returned to consultancy, working in the security unit of an independent software testing company. A Fellow of the British Computer Society and a founder member of the Institute of Information Security Professionals, Matthew holds a Bachelor of Engineering degree from Heriot-Watt University in Edinburgh, and is a European Engineer, a Chartered Engineer, and holds the Certified Information Systems Security Professional (CISSP), Certified Fraud Examiner (CFE) and Certified Information Security Manager (CISM) credentials.

James Blessing – COO, Entanet International and Council Member of the Internet Service Providers' Association (ISPA), UK

James Blessing is Chief Operations Officer for Entanet International, part of the IT distribution and communications services group Entagroup. An innovative and creative IT professional, he has more than ten years experience of deploying Internet technologies and takes an active role in the Internet industry. He has been a council member of the Internet Service Providers' Association (ISPA) since 2004 and is Chair of the ISPA broadband sub-group. James was elected to the Board of the UK Enum Consortium in March 2008.

Peter Milford – Regulatory Affairs Manager, Newnet, UK

Peter joined the company in April 2001 working as a member of NewNet's senior management team with responsibilities for regulatory and corporate affairs.

Before joining NewNet, Peter was Chief Executive of the Hampshire On-Line Learning project and formerly Director of Learning Resources at St. Vincent College, Gosport.

Peter was seconded to BT plc from 1995 – 1997 to develop online services for education. He has a BA degree in Physics and Information Technology, a Masters degree in Law (LL.M Intellectual Property), holds a post-graduate diploma in Educational Technology, is a Chartered Physicist, Member of the Institute of Physics, and Member of the British Computer Society.

Dr. Marco Gercke – Professor, University of Cologne and UN and Council of Europe expert on the Cybercrime Convention, Germany

Dr. Marco Gercke is an attorney-at-law admitted to the German bar. He is teaching Law related to Cybercrime and European Criminal Law at the University of Cologne and is visiting lecturer for International Criminal Law at the University of Macau.

5 5622350479 658. 7895200.02. 33695 454868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656 546 78952 565.369 21
77787 4651

54868.45 5 48 4528782 45 4582 688.54 58 89 8 4568

4528782 45 4582 688.54 58 89 8 4568 44 822.656 54868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656

Marco is a frequent national and international speaker and author of more than 50 publications related to the topic cybercrime. His main areas of research are international aspects of cybercrime (especially the challenges of fighting cybercrime and legal responses) and comparative law analysis regarding the implementation of international standards. The latest researches covered the activities of terrorist organizations on the Internet, identity theft, money laundering on the Internet, and legal responses to the emerging use of encryption technology. He is Secretary of the Criminal Law Department of the German Society for Law and Informatics, member of the ITU High Level Expert Group, and works as an expert for the Council of Europe, the International Telecommunication Union, and other international organizations.

Marc Vilanova – CSIRT Member
at e-la Caixa, Spain

Marc Vilanova is a member of CSIRT (Computer Security Incident Response Team) at e-la Caixa, one of the most important savings banks in Europe.

He was previously and IT security consultant and auditor at GMV Soluciones Globales Internet S.A and a volunteer at The Institute for Security and Open Methodologies (ISECOM).

Haim Vismonski – Lawyer,
Ministry of Justice, Israel

Haim Vismonski is a lawyer at the Ministry of Justice and a Senior Deputy at State Attorney.

Ferenc Suba – Chairman of the Board,
CERT, Hungary

Since 2004, Ferenc Suba is Special Envoy of the Minister, Ministry of Informatics and Telecommunications; General Manager of CERT-Hungary, the government's computer emergency response team; and Vice-chair of the Management Board of the European Network and Information Security Agency.

Erka Koivunen – Director of CERT-FL, Finland

Erka Koivunen is an experienced professional in the field of information security. His current position is head of CERT-FI, the Finnish national information security authority. His area of expertise is incident response and response coordination.

UNITED STATES:

Eugene H Spafford – Professor of Computer Sciences, Purdue University and Executive Director of the Centre for Education and Research in Information Assurance and Security (CERIAS)

Eugene H. Spafford is one of the most senior and recognized leaders in the field of computing. He has an ongoing record of accomplishment as a senior advisor and consultant on issues of security, education, cybercrime and computing policy to a number of major companies, law enforcement organizations, academic and government agencies, including Microsoft, Intel, Unisys, the US Air Force, the National Security Agency, the GAO, the Federal Bureau of Investigation, the National Science Foundation, the Department of Energy, and two Presidents of the United States. With nearly three decades of experience as a researcher and instructor, Professor Spafford has worked in software engineering, reliable distributed computing, host and network security, digital forensics, computing policy, and computing curriculum design. He is responsible for a number of 'firsts' in several of these areas.

Andrea Matwyshyn – Assistant Professor of Legal Studies and Business Ethics, The Wharton School, University of Pennsylvania

Andrea Matwyshyn is assistant professor of legal studies and business ethics at the University of Pennsylvania. Andrea's research focuses on corporate information security and risk management; information technology regulation; and policy and contracts. Current projects include transformation in the corporate form and its relationship to the information technology revolution and data vulnerability, and legal strategies for combating information crime.

She was previously assistant professor of law at the University of Florida and executive director of Florida's Center for Information Research (CIR).

CANADA:

Mary Kirwan – CEO Headfry Inc. and journalist, former cybercrime prosecutor

Mary Kirwan is an Irish international lawyer and risk management consultant. She is a qualified lawyer on three continents, with extensive litigation and senior management experience.

She practiced commercial litigation in Toronto, Canada, for several years, where she worked on a number of high-profile commercial and international white-collar crime, tax evasion, and fraud cases. She was also a Senior Federal Crown Attorney in the wiretap and money laundering division at the Department of Justice in Toronto.

She has a degree in German and Irish (Gaelic) from Trinity College Dublin, and she holds several IT security certifications, including the CISSP. She has a first class honours Masters Degree in Business and MIS (Management Information Systems) from the Michael Smurfit Graduate School of Business at University College Dublin, Ireland.

68 44 822.656 546 78952 565.369 21
8.45 5 48 4528782 45 4582 688.54 58 89 8 4568

4528782 45 4582 688.54 58 89 8 4568 44 822.656 54868.45 5

She actively participates in the Toronto Computer Lawyers Association and the American Bar Association (ABA) Science & Technology (SciTech) Section. She has contributed to several ABA publications in the IT, information security and biotechnology fields. She is the Chair of the ABA Science and Technology ECommerce Payments Committee, and a member of the SciTech book publishing board. She has a special interest in online banking, payments fraud, the global ATM and debit card markets, and evolving payments methods.

She is currently completing two books for the ABA for publication in January 2009: *Guide to ATM and Debit Card Legal Issues* for the US mass market, and The Business Case for Data Security for broad release.

Ms. Kirwan is a regular contributor to the *Globe and Mail*, Canada's national newspaper, and she has written extensively about data security, risk management, compliance, corporate governance, law enforcement, and consumers issues. She has spoken at conferences around the world, and has appeared on radio and TV.

Leo Adler – Toronto Criminal Lawyer

While Leo Adler's practice is almost exclusively criminal, he has also appeared before various boards, tribunals and inquests and he has been retained or consulted in cases involving extradition matters, trials and administrative and quasi-criminal hearings throughout Ontario, as well as in Quebec, Manitoba, New Brunswick, the Northwest Territories, Alberta and British Columbia, right up to the Supreme Court of Canada. He has represented individuals arrested in the U.S. in courts from Florida, to Michigan, to New York, California, North Carolina and elsewhere, including Europe, and his advice has been sought out in numerous instances. His experience in DNA cases and other forensic issues has caused him to be consulted by other counsel.

He is an adjunct professor at Osgoode Hall Law School of York University, and a participant in the Intensive Law Program of that school. Several of his cases have been reported as legal precedents.

He is a member of the Criminal Lawyers Association, the National Association of Criminal Defense Lawyers, the International Association of Defence Attorneys and the Canadian Forensic Society.

LATIN AMERICA:

Dr. Paulo Marco Ferreira Lima, Brazil

Dr. Paulo Marco Ferreira Lima is a Notary Public in São Paulo city. Since 1997 he has been advisor for several offices in Brazil. He has been the secretary for the Commission of Legislative projects monitoring digital crimes.

Dr. Lima is the author of the book *Computer Crimes and Computer Security (Crimes de computador e segurança computacional,* published by Millennium), launched in 2007. He is also a teacher at University of Santos (city in São Paulo state) for a post graduation course. The Notary Public has majored in law school at Mackenzie University, has a Masters in Criminal Law, a Ph.D. in Criminal Law at the University of São Paulo, and is also a doctoral candidate for Digital Criminal Law at the University of Rome, UNIROMA3.

Adriana Scordamaglia Fernandes Marins, Brazil

Dr. Adriana Scordamaglia has been a federal prosecutor since 1997. She has also worked in the criminal activity area in Ministério Público Federal (Brazilian Federal Prosecution), in the 2ª Vara Criminal da Seção Judiciária de São Paulo (2nd Criminal Judicial Section of Sao Paulo). Prior to this, the Prosecutor worked as Bureau Official in the Gabinete da 21ª Vara Federal (21st Federal Criminal Judicial Agency) from 1993 to 1997.

Dr. Scordamaglia graduated in law school at the Faculdades Metropolitanas Unidas in Brazil and did her post-graduate work at the University of Lusíada Porto in Portugal. In 2008, she organized a workshop on crimes against children that are facilitated by the computer, and also gave a seminar about psychological pedophile profiling. Additionally, she participated in the International Workshop on Legislation on Cybercrime in Bogotá, Colombia, through the Department of Justice of the United States.

Renato Opice Blum – Opice Blum Advogados Associados, Brazil

Opice Blum Advogados Associados has years of solid experience in law, especially in technology, electronic law, information technology, and its variations. As a pioneer in those matters, his firm is also active in mediations, arbitration, oral sustaining in Court, bio-law, typical technological contracts, and cybercrimes. The organization operates throughout the Brazilian territory and has international correspondents in the main international financial centres, such as Miami and New York.

As a member of several institutional organizations, it contributes to the evolution of the law related to technological development. He is founding partner of the Brazilian Chamber of Electronic Commerce, member of the Computation Brazilian Society, among other institutions.

8 4568 44 822.656 546 78952
565.369 21

ASIA-PACIFIC

Alana Maurushat – Acting Director of the Cyberspace Law and Policy Centre of the University of New South Wales, Australia

Alana Maurushat is Acting Academic Director of the Centre, sessional lecturer, and PhD candidate at the Faculty of Law at UNSW. She was Assistant Professor and Deputy Director of the LLM in Information Technology and Intellectual Property at Hong Kong Faculty of Law. She teaches Advanced Legal Research. Her current research is focused on technical, ethical, and legal dimensions of computer malware building on past research projects on the impact of surveillance technologies on free expression and privacy. She is a partner investigator in the Regulating Malware research project.

Peter Guttman – Security Researcher, The University of Auckland, New Zealand

Peter Gutmann, Ph.D., is a researcher with the Department of Computer Science at the University of Auckland, specializing in the design and analysis of cryptographic security architectures. He helped write the popular PGP encryption package and, more recently, created the Cryptlib Security Toolkit, an OS-independent open-source security and encryption toolkit that offers high-speed encryption, key exchange, digital signatures, key and certificate management, smart card support, S/MIME and PGP email encryption, SSL and ssh session encryption, timestamping, CA management and various other features. Cryptlib, internationally used and recognized, is the only New Zealand product to have received a FIPS 140 security certification from the US government.

Andrew Adams – Lecturer in Systems Engineering, Reading University, Visiting Professor at Meiji University, Japan

Andrew Adams is a lecturer in the School of Systems Engineering at the University of Reading, where he is a member of the Informatics Research Group, the Informatics Research Centre, and the Computer Science and Informatics Subject group. He is the chair of the Informatics Research Group and Programme Director for the Information Technology Degrees.

He has given seminars at University of Cambridge Computer Laboratory, Oxford Internet Institute, University of Bath Computer Science Department and the University of Southampton Law School in the UK based on his work on privacy in Japan, funded by the Royal Academy of Engineering under their Global Research Awards scheme, and carried out in collaboration with Prof K. Murata of Meiji University and Dr Y. Orito of Ehime University.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054

888.847.8766

www.mcafee.com

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. It delivers proactive and proven solutions and services that secure systems and networks around the world, allowing users to browse and shop the Web securely. With its unmatched security expertise and commitment to innovation, McAfee empowers home users, businesses, the public sector and service providers by enabling them to comply with regulations, protect data, prevent disruptions, identify vulnerabilities and continuously monitor and improve their security. http://mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee's customers. We endeavor to ensure that the information contained in the *McAfee Virtual Criminology Report* is correct; however, due to the ever changing state in cybersecurity the information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.


442 5.4567
1/25/78
89.6 7 15
-926.89
$556,000
56
-12.38