Cybercrime in the UK

new technology ● new opportunities ● new threats

Conservatives

Cybercrime in the UK

A massive Chinese cyber-espionage attack on both government and commercial computer systems in Britain, Germany, Australia, New Zealand, India and the USA; a ‘cyber-riot’ which shut down banking and government websites in Estonia for weeks; the deployment of new, sophisticated software such as the so-called ‘Storm Worm’ that has hijacked hundreds of thousands, if not millions, of computers, creating a massive network of computing power that can be deployed to mount so-called ‘botnet attacks’; and the creation of thriving markets that trade identity details at extraordinary cheap prices.

Those are just some of the ‘headline’ threats to personal, commercial and national security that are known to exist in these days of the web-enabled society. More are coming. They will include so-called p-to-p industrial espionage, a range of new crimes, up to and including paedophilia, arising from the intrinsic insecurity of social networks such as Facebook, and potentially new forms of terrorism attacking critical infrastructure through worms and viruses on public networks.

Much of this cyber-crime feeds on cyber-carelessness. Companies underestimate the risk. People may not be fully aware - or just careless - about protecting their private data. But most of all, governments – most obviously the British Government – irresponsibly underestimate both the value and the risk inherent in the vast database of personal information that they insist on creating. And out of this cyber-carelessness comes cyber-crime, cyber-terrorism, and cyber-chaos.

Against these threats the Government will need to take aggressive, intelligent and persistent action. This action will need to be international, since this is a criminal market that recognises no frontiers. It will need to be forward looking and imaginative, and extraordinarily flexible in the face of rapid change.

Consider the problem of cyber-terrorism. So far we have not witnessed a cyber-terrorist attack, but it is almost certain that we will. Cyber attacks are cheap, potentially hugely destructive, and can be initiated from ‘safe’ countries anywhere in the world. They might have been designed for the sort of asymmetric warfare that terrorists favour.

Take as an example the attack on Estonia. It was not a terrorist attack, but it could be the template for one. It was precipitated when the Estonian government removed a Soviet-era war memorial of a Russian solider from a square in Tallinn.

The Distributed Denial of Service (DDOS) attack sent so many requests to target computers that they could not respond, and locked up. The attack lasted almost a month. At its peak on 9 May 2007, 58 government and banking websites were shut down at once. This was done by a network of 20,000 hijacked computers, in America, Canada, Brazil and elsewhere, and almost certainly initiated and co-ordinated from within Russia.

In the words of an Estonian journalist, “It was extremely frightening… You couldn’t get information; you couldn’t do your job. You couldn’t reach the bank; you couldn’t check the bus schedule.”

This attack demonstrated the fragility of modern, web dependent societies. It also demonstrates how weak our ability to respond is, if a national state is willing to give succour, or even just turn a blind eye, to people determined to do such harm.

Modern technology has been harnessed to ancient prejudices. The attack on Estonia was provoked by an affront to Russian national pride. Imagine an even more threatening scenario – when, perhaps, the USA has taken action against a middle-eastern state, and Britain is seen to be supportive or compliant in such action. The Middle Eastern state allows a terrorist group, Al-Qaeda or some-such, to act from within its borders to set up networks of corrupted computers – botnets – in other countries. They then use this series of networks to assault the information networks in Britain.

In America, hackers have broken into the Pentagon's computer systems, in India into government ministers' files; in Germany into the Chancellery. Such attacks could be designed to compromise safety systems in critical national infrastructure, to overwhelm communication systems, or cause a run on a bank.

It is doubtful that we have taken enough care to protect Britain from such attacks, let alone the pervasive and persistent criminal threat.

Worse still, the Government's naïve over-reliance on massively centralised data systems and its recklessness with the personal data held on such systems – demonstrated over the last few months – has left us vulnerable, both as individuals and as a society.

The Government's strategic approach has managed, at one and the same time, to create data systems that are valuable, vulnerable, and attractive to attack.

To protect ourselves - against both the persistent criminal threat and the rarer but more devastating terrorist threat - will require a shake up in attitudes and strategy, including the whole mindset of government.

The Cybercrime Threat

The ‘playground of criminals’. That was how the House of Lords Science and Technology Committee recently described the internet.[1] The description implies that cybercrime is some sort of past-time - something that organised gangs do in their time off for enjoyment or fun. The reality is much more serious than that. It's more like an electronic shopping mall for criminals with plenty of well-stocked ATMs open 24-7.

The migration of entertainment, services and communication from the physical environment to a more virtual one has also led to a migration of a more damaging and harmful kind. The growth in internet use and reliance on the on-line world has spawned a burgeoning illegal business in cybercrime.

The thieves, fraudsters and organised criminal gangs exploit ignorance, carelessness and the lack of awareness of the online risks. Individuals, businesses and other organisations don’t generally protect against cyber intrusion with the same vigilance as if it was their house or car or some other important or valuable possession. This is despite the fact that our personal details and information are now the currency of the digital age.

The HMRC scandal with the loss of data discs containing the personal details and banking information of up to 25 million child benefit recipients has also brought into stark focus the dangers of identity fraud – a risk made worse when vast quantities of information are combined in one place and stored in electronic format facilitating speedy distribution to those intent on causing harm. Yet the Government appears oblivious to the dangers and seemingly unperturbed by issuing regular updates to its Discgate 2.0 fiasco program.

The advent of broadband and wireless technology has opened up the internet for millions. It has transformed the way business operates. It has even forced government to re-think the way in which it provides public services. Put simply, it has revolutionised the way in which we work, communicate – even share our experiences. From email to file sharing from social networking to on-line shopping, most of us now live at least part of our lives on-line.

Use of the internet in the UK has grown at a phenomenal rate. In 2007, 15.23 million UK households had Internet access. This represents nearly two thirds of all households.[2]
People are purchasing goods online in greater numbers than ever before. In 2007, 53 per cent of adults had purchased goods or services over the Internet.[3]

But people are feeling increasingly unsafe.

The risk to individuals

Polling for the Government's online safety website "Get Safe Online" paints a picture of insecurity. More than one in five people surveyed said they felt most at risk from crime on the internet than any other crime.[4] Higher in people’s minds than the risk of having their home burgled, their car broken into or being mugged on the street. A further survey of UK internet users found that 12%

[1] House of Lords Science and Technology Committee – Personal Internet Security, August 2007.

[2] National statistics – Internet Access 2007 Households and Individuals http://www.statistics.gov.uk/pdfdir/inta0807.pdf

[3] National Statistics, First Release, Internet Access 2007, Households and Individuals, 28th August 2007 http://www.statistics.gov.uk/pdfdir/inta0807.pdf

[4] Get Safe Online - http://www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf

had been victim to on-line fraud in the last year. This would mean that 3.5 million people had been the subject of a fraud using the internet as the means of perpetrating the crime.[5]

But it's not just fraud. It's the on-line bullying, the posting of offensive materials that promote violence or other abuse and the distribution of viruses and other malicious software or 'malware' that can disable your computer, allow your key-strokes to be monitored or abuse your system by using it and thousands of other compromised machines to perpetrate co-ordinated so called 'botnet' attacks on others.

A recent report, by online identity experts Garlik, suggests that more than three million online crimes took place in Britain last year - one every ten seconds.[6] Yet nine out of ten offences go unreported because victims believe the police will be unable or unwilling to investigate.[7] A view reflected within the police, with a report to the Metropolitan Police Authority on e-crime stating that:

> *"There is an issue of under-reporting across the UK. There is an unspoken public perception that e-crime is so pervasive that the police service does not have the capacity to investigate each individual allegation. The public have reported difficulties in reporting e-crime to the police. Also many organisations may be unaware of their computer being compromised, making it difficult to establish definitive annual financial harm."*[8]

But even when someone does try to report an on-line incident it isn't straightforward. Garreth Griffith the Head of Trust & Safety at eBay UK summed up the position well when he gave evidence to House of Lords Science & Technology Committee:

> *"We ask our community of users to go to their local police stations, get them to contact us – and we give them numbers, email addresses and everything they need to contact us – and then we can work with the police. What we find is the users coming back to us, saying, "They're not interested". It is only a £500 laptop, or whatever the issue might be."*[9]

The internet platform is a great way of sharing stolen data with other like-minded criminals. There is a growing trade in illicit information and other items obtained through clandestine means using the internet as a means of conducting this unlawful business. A recent investigation by one newspaper identified more than 100 websites trafficking British bank details. Banking information belonging to 32 people including a High Court deputy judge and a managing director was made available for download for free. The private account numbers, PINs and security codes were offered as tasters by illegal hacking sites in the hope that purchases would follow.[10]

There is public awareness of the threat from criminals on the internet. Many people do try and protect themselves from viruses on the internet. But this level of engagement is still insufficient. Vigilance itself is not enough.

Malicious emails and websites infected with corrupt software change all the time with the effect that unless anti-virus software is up to date it is of limited effect. Even then, the protection offered by anti-virus products is not full-proof. Research from Team Cymru which monitors malicious programmes has indicated that 6,200 new samples of malicious computer code are being added to their databases each day of which only around 28% was detected immediately by anti-virus software with detection rates rising to around 70% a month later even after notification of the threats to software protection companies. [11]

Our home PCs are not as much of a castle as we might like to think they are.

[5] 'Get Safe Online' - press release, 26th March 2007 http://www.getsafeonline.org/nqcontent.cfm?a_id=1449
[6] Garlik, 'UK Cybercrime report', 6 September 2007 https://www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf
[7] Ibid
[8] Report to Metropolitan Police Authority, 25 January 2007
[9] House of Lords Science & Technology Committee Report – Personal Internet Security, August 2007
[10] The *Times 3 December 2007*.
[11] House of Lords Science & Technology Committee Report – Personal Internet Security, August 2007

When combined with:

- the threat of networks of thousands of computers that can be deployed by criminal gangs to carry out specifically targeted attacks on IT systems to hack into them or disrupt them;

- the risk of misuse of wireless networks to download offensive material and conduct fraud; and

- the use of personal information gleaned from social networking sites and more clandestine sources to create more and more sophisticated and individualised email fraud attacks

it is clear that a policy based largely on individual self help, which is the Government's approach, is entirely inadequate.

The risk to business and industry

According to APACS, the UK Payments Association, shoppers are thought to have spent over £5 billion on line during Christmas 2007 with the number of people buying on the internet having doubled in the last five years to 30 million.[12] In 2006 internet sales increased by 29% to £130bn according to estimates from the latest annual e-commerce survey published by the Office for National Statistics (ONS).[13]

The rise in those using the internet for their banking has been even more dramatic. People using online banking services increased by 174% in five years - from 6.2 million in 2001 to 17 million in 2006.[14] This includes a 350 per cent increase in usage amongst the over 55s. Those using online banking now exceed the number using telephone banking.

But confidence in the platform is starting to come into question. This poses a risk to business which has invested heavily in developing an on-line presence and the facility for customers to buy and sell electronically. One poll of internet users suggested that nearly one in three internet users have not done their banking on the internet due to their fears about safety and security[15].

84% of large businesses are thought to have suffered a malicious security incident in the last year with the Metropolitan Police estimating the average losses to a large company of an e-crime attack as between £65,000 and £130,000 rising to up to £1 million for a very large corporate.[16] The *DTI Information Security Breaches Survey*, published in April 2006, found that 52 per cent. of businesses suffered premeditated and malicious breaches in 2006.[17] The survey indicated that the average cost of all incidents, both criminal and non-criminal, rose from £10,000 in 2004 to £12,000 in 2006 and estimates the total cost of all incidents in the order of £10 billion per year, up roughly 50 per cent. since 2004.[18]

At the end of last year hundreds of websites were shut down temporarily when the web hosting company Fasthosts was forced to perform an emergency shut-down when it became apparent that hackers had tried to use information obtained from its servers.

The Corporate IT Forum has criticised the Government for failing to take business e-crime seriously. The professional body for industry computer experts has criticised the way in which on-line crimes have to be reported to local police stations. David Roberts, Chief Executive of the Corporate IT Forum commented that:

[12] APACS press release, 26 November 2007, http://www.apacs.org.uk/07_11_29.html
[13] National Statistics press release - http://www.statistics.gov.uk/pdfdir/ecom1107.pdf
[14] APACS press release, 24 August 2007
[15] Get Safe Online
[16] National Statistics Online 'Digital Age', March 2007, http://www.statistics.gov.uk/cci/nugget.asp?id=1717
[17] DTI, Information Security Breaches Survey 2006, April 2006, http://www.berr.gov.uk/files/file28344.pdf
[18] Ibid

> "*You can imagine the response an IT officer would get reporting a complex attack at their local police station - how is your local PC going to cope? It's a damning indictment of how little the Home Office understands 21st Century high-tech crime.*"[19]

And not a single member of the Information Systems Security Association (ISSA) believes that the UK is equipped to deal with cybercrime, with two thirds of members believing the situation to be wholly inadequate.

The risk to government

Government itself isn't immune from attack. Increasingly the public are engaging with government through computers and the internet as part of the drive to promote "e-government". In 2005 almost 6 out of 10 people had visited a Government Department's website .[20] Yet the various different governmental IT systems and portals are as susceptible to the same risks and threats as any commercial organisation with a web or on-line presence.

In 2005 the Tax Credits website was closed down by ID fraudsters.[21] Poor security and ID checks on the Revenue and Customs e-portal allowed criminals to make fraudulent claims for tax credits as well as stealing the identities of 13,000 staff at the Department of Work & Pensions and Network Rail.[22] According to information given to the House of Commons Treasury Select Committee, the website is unlikely to be reinstated before the Summer of 2008.

There are other threats from criminals using new technologies to dupe people into giving away personal information. There are attempts by hackers to break into people's computers and steal the information held on that computer. There are also attempts by international cyber-gangs to cause mass disruption to networks of computers and whole countries have been targeted by these attacks.

Cybercrime and cyberterrorism are simply two sides of the same coin. The approaches, the techniques, the methods are substantially the same. It is only the motivation that is different.

If you accept cybercriminality you heighten the risk of cyberterrorism.

[19] http://news.bbc.co.uk/1/hi/technology/7128491.stm
[20] National Statistics, 'E-government', http://www.statistics.gov.uk/CCI/nugget.asp?ID=1716&Pos=4&ColRank=2&Rank=1000
[21] 'Online tax credit system closed', 2 December 2005, http://news.bbc.co.uk/1/hi/business/4493008.stm
[22] 'The assault on tax credits', 21 December 2005, http://news.bbc.co.uk/1/hi/business/4532682.stm

Cybersecurity – the international dimension

Cybercrime by its very nature crosses borders. The internet simply doesn't recognise international boundaries. And nor do the cybercriminals.

The threats posed to government are not limited to domestic hackers but are increasingly emanating from overseas. Perhaps most serious and disturbing is the risk of overseas cyber attacks being used to undermine key elements of the national infrastructure or the economy of a country.

In May 2007, Estonia appealed for help from NATO and EU partners after being subjected to sustained attacks from cyber hackers which it claimed had links to Russia. Government, political and business websites were shut down after being hit by distributed denial of service attacks with websites being bombarded with fake email traffic to such an extent that they were disabled.

Estonia was perceived to be more vulnerable to this type of attack because of its move to paperless e-government and its reliance on an internet banking system. It is thought that the sustained botnet attack was triggered by a decision to move the 'Bronze Solider', a Soviet war memorial in Tallinn commemorating an unknown Russian who died fighting the Nazis. It is believed to be the first time that any state has been subject to such an extensive and sustained cyber attack on its infrastructure linked to a political issue.

A range of incidents in 2007 have highlighted the seriousness and sophistication of the threats facing government IT systems.

- In June it was reported that there had been a "detected penetration" of the Pentagon military computer network.[23] Described by some as the most successful cyber attack on the US defence department, it followed a stream of attacks on US government departments from China which were given the codename 'Titan Rain'. The incident was described as a 'wake up call' on the potential for Federal computer systems to be hacked or disrupted.

- The German Chancellor Angela Merkel is thought to have raised the issue of computer attacks on German computer networks during a recent visit to Beijing. It follows reports that the Chancellor's computer system as well as the computers in three other government ministries were infected with malicious software to spy on them. McAfee notes that "The German Federal Office for the Protection of the Constitution (BfV) conducted a comprehensive search of government IT installations and prevented a further 160 giga-bytes of information being transferred to China. They described it as being 'the biggest digital defense ever mounted by the German authorities'".[24]

- In the UK Chinese hackers are thought to have been behind an attack on Government computer networks which was revealed in September. Computer networks at the Foreign Office and other key departments were reported to have been subject to a cyber assault although the impact of the attack has not been revealed.

- A US nuclear weapons laboratory suffered a cyber security incident in October. Employees at the Oak Ridge National Laboratory in Tennessee were sent numerous phishing emails containing hacking software some of which were opened compromising the computers with the malicious software and allowing third parties to infiltrate the system and remove data.

[23] Cyber attack on pentagon e-mail - 22nd June 2007 - http://news.bbc.co.uk/1/hi/world/americas/6229188.stm
[24] McAffee, 2007 Virtual Criminology Report, "Cybercrime: The Next Wave"

The incident prompted US Computer Emergency Readiness Team (US-CERT) to issue a confidential warning to computer security officers warning of the level of sophistication, scope and co-ordination of cyber security incidents.

- At the start of December 2007 Jonathan Evans, the Director General of MI5 was reported to have sent a confidential letter to chief executives and security chiefs at banks, accountants and legal firms that they were under attack from "Chinese state organisations". A summary of the letter was posted on the website of the Centre for the Protection of the National Infrastructure (CPNI) saying that Mr Evans, wrote to business leaders "warning them of the electronic espionage attack" adding that: "The contents of the letter highlight the following: the Director-General's concerns about the possible damage to UK business resulting from electronic attack sponsored by Chinese state organisations, and the fact that the attacks are designed to defeat best practice IT security systems." China has protested about the report in the strongest terms denying that it is engaged in any cyber crime and asserting that its own networks have been the target of attacks.

In its 2007 Virtual Criminology Report - “Cybercrime: The Next Wave”, software security provider McAfee notes that:

> “*There is now a growing threat to national security as Web-espionage becomes increasingly advanced, moving from curiosity probes to well-funded and well-organized operations out for not only financial, but also political or technical gain*.”[25]

[25] McAffee, Virtual Criminology Report, ‘Cybercrime: The Next Wave’

A Government with its head in the sand

The current Government's approach to the increasing threat of cybercrime lacks co-ordination, focus or urgency. There is a strong sense that it is 'in denial' over the extent and nature of the challenges facing this country from organised cybercrime networks. It has left us vulnerable and exposes us to attack.

They don't know the full nature of the problem. They haven't bothered to assess the scale of the threat. They've reduced the effectiveness of organisations and procedures combating the on-line danger. They've abdicated responsibility in a number of important ways.

They don't even seem to regard the issue as serious.

When combined with a lack of any clear leadership and responsibilities spread out over various different departments it gives the clear message that the Government either can't cope or can't be bothered with e-crime.

Either way this negligent approach puts us all at much greater risk.

Lack of Policing

- The National Hi-Tech Crime Unit (NHTCU) which was set up in 2001 in response to the threat of on-line crime and provided a link with police forces and business. The NHTCU worked to combat national and international serious and organised hi-tech crime including software piracy, hacking and virus attacks, fraud, blackmail and extortion, on-line paedophilia and identity theft. Despite criticism that it would leave a yawning gap between local forces and national level policing leaving victims of some computer crimes unsupported, the NHTCU was absorbed into the Serious Organised Crime Agency (SOCA eCrime) at the start of 2006.

- The dissolution of the NHTCU has been widely criticised by business organisations including Microsoft which commented that:

  > "*With the changes around SOCA, the proposed re-structuring of police forces and the disappearance of the NHTCU it is unclear how cybercrime and reporting mechanisms are being systematically addressed. There is no single reporting mechanism in the UK (as there is in the US), thus, no reasonably supported statistics aside from anecdotal information and surveys*."

- There are now calls for the NHTCU to be re-established with the Metropolitan Police (as ACPO lead on cybercrime) promoting a new Police Central E-Crime Unit and seeking £4.5 million annual funding from the Home Office, although the Government has failed to support the move.

- Ring-fenced funding for computer crime units in each police force in England and Wales was cut off in April 2007.

Lack of intelligence

- Perversely the Government has created "double inertia" in the reporting of cybercrime. From April 2007 on-line financial fraud can no longer be reported to the police directly. It first has to be reported to the financial institution concerned. It is then up to the bank or credit company to decide whether the matter should be reported to the police for further action to be taken. It is then at the discretion of individual chief officers to decide which crimes will be investigated. Therefore it is now harder for an individual to report on-line financial fraud as the law enforcement channel has been shut off with police officers directing people to their bank or other financial institution suggesting that this isn't a matter for them. And even if the information is provided in this way there is no incentive for it to be referred to the police for recording or investigation.

Lack of urgency

- Despite signing the Cybercrime Convention in 2001, the Government has failed to ratify the treaty which is intended to promote greater co-operation between governments in dealing with on-line crime. Countries that have implemented the measure include the United States. The Home Office has recently stated that it will start the process of ratification from this April – seven years late.

Lack of co-ordination

- There are at least seven different Government departments/offices involved in developing policy to combat cybercrime and cyberabuse: Home Office (enforcement); Department of Justice (legislation); Attorney General (leading fraud review including on-line fraud); Cabinet Office (responsible for the "Get Safe On-line" website); Department for Business, Enterprise & Regulatory Reform (regulation and business); Children Schools and Families (child protection), Culture, Media and Sport (on-line copyright piracy). Each appears to be developing initiatives in a vacuum without co-ordination or leadership. The result is Government cyber-chaos.

Lack of priority

- Apparently, the Government doesn't consider cybercrime as a serious offence. Despite suggesting that the Serious Crime Act 2007 would help deal with cyber hackers,[26] offences under the Computer Mis-Use Act 1990 are not listed as "serious crimes" under the new act whereas illegal salmon poaching is.

- Whilst the Government is intending to establish a national fraud reporting centre, this initiative appears to be directed at more traditional types of frauds using postal or telephony services and will not encompass non-fraud related cybercrimes such as botnet denial of service attacks.

Lack of enforcement

- Between 2001 and 2006 there have only been 89 convictions under the Computer Mis-Use Act 2000 - the key piece of legislation introduced by the Government to combat hacking and computer enabled crime. This averages at just 15 convictions a year.

- Police databases don't distinguish between crimes committed electronically or not, nor do Home Office or prosecution figures distinguish between the two. So the Government doesn't even know how many criminals are being brought to justice for cybercrime offences.

[26] House of Commons Library Note on Cybercrime

What all of this betrays is a complete lack of strategy.

The House of Lords Committee on Science and Technology recently described the Government as having its “head in the sand” over cybercrime.[27]

This approach merely makes the UK more of a target for the organised criminal networks who view this country as a soft touch and lacking any determination to get to grips with this serious threat.

The core responsibility of the Government is to protect the public from harm. Yet at a time when other countries are developing more and more structure, sophisticated and co-ordinated ways to face down the on-line threat. The Government is singularly failing in this duty.

[27] House of Lords Science & Technology Committee Report – Personal Internet Security

The nature of Cybercrime

Malicious E-mails (Viruses, Spam and Phishing attacks)

Malicious emails can come in a number of different forms. They may be incorporated in an attachment which once opened infects a PC with a virus or other malicious software. This 'malware' can disable the computer, installing software to monitor its use (spyware) or even enable the infected PC to be used as part of a directed attack on other IT systems. Other spam emails may purport to offer drugs, scam lottery wins, fraudulent requests for financial assistance and other bogus services.

Phishing attacks are where thousands of false emails are sent out directing people to confirm passwords and other sensitive data such as passwords. To give an air of authenticity they usually purport to come from a bank, a credit card company, a retailer or some other well known name. The emails may also direct the potential victim to a fraudulent website mirroring the look of the real website of the company concerned, providing a further sense of legitimacy and reinforcing the impression that this is a genuine communication. These emails usually claim that it is necessary to ‘update’ or ‘verify’ your customer account information and they urge people to click on a link from the email which takes them to the bogus website. Any information entered on the bogus website will be captured by the criminals for their own fraudulent purposes. This may also lead to malicious software being downloaded onto PCs enabling sensitive information to be accessed through the monitoring of the key stokes used on an infected computer.

According to APACS, the UK Payments Association, in the first six months of 2007 phishing incidents increased by 42% as compared to the same period in 2006.[28] Software security company Symantec claims to have blocked over 2.3 billion phishing messages in the first half of 2007, an increase of 53 percent over the second half of 2006.

These scam email attacks are becoming more and more sophisticated with the contents of the email becoming more individually targeted. Some seemingly give the veneer of legitimacy by incorporating personal information gleaned from social networking sites or through details on individuals obtained from stolen identity information traded through criminal networks. They've even been given a new term – 'spear phishing'. And with the volume of fake emails being sent out all the time only a relatively small proportion need to be acted on to make it big business.

Botnets

Botnet is a term used to refer to networks of compromised computers which have been infected by malicious software enabling a third party to control their actions remotely without the owner being aware of what is going on. These networks of hijacked computers can then be commanded to operate as a group to send out spam emails, to target vulnerabilities or weaknesses in third party IT systems or to disrupt or take down websites or networks by bombarding the target with thousands of messages.

And Botnets are available for hire. Information supplied by the Center for Information Technology Research in the Interest of Society (CITRIS) at the University of California, Berkeley suggests that

[28] APACS Press Release, October 2007, ‘Fraud abroad drives up card fraud losses’

5% of all machines worldwide could be compromised - up to 20 million in total – with the cost of hiring a botnet for spamming being a as little as 3-7 cents per compromised computer per week[29].

Contaminated websites (Pharming).

According to research from the security software supplier Sophos, cyber-criminals are shifting from email to web pages to compromise computers through malicious software with 30,000 new malicious web pages a day - a six-fold rise in six months. Internet search company Google is reported to have removed thousands of pages from its search results after uncovering a scheme which manipulated Google's algorithm to drive more users to websites infected with malicious programmes. The software downloaded was designed to steal bank codes, send spam and engage in fraud.

Online Fraud

The creation of new ways of buying and selling goods using the internet has opened up new opportunities for fraud. This has led to more traditional frauds being transferred to the on-line environment such as bogus prize schemes, fraudulent share investments and requests for money transfers. But it has also opened up new opportunities to commit scams on-line.

In 2005 a London-couple were jailed after making £300,000 by selling non-existent cars and concert tickets on eBay, whilst a teenager made £45,000 by selling electrical items on the web auction site.[30] eBay has responded by promoting secure payment methods on-line through the PayPal system.

ID fraud risk from social networking sites

One third of all internet users are registered to a social networking website, such as Facebook, Bebo, MySpace or Friends Reunited. Over 10.8 million people across the UK are registered to these sites.[31] Of these, one in four are estimated to have posted confidential or personal information such as their phone number, address or email, on their online profile, making them vulnerable to identity fraud. The information can also be used to target individuals with increasingly sophisticated phishing and cyber email scams being used adding to the risk that someone will be conned.

It is estimated that the police investigate less than 1% of identity fraud cases.[32] The criminal activity often crosses police authority boundaries and just one case can involve the investigation of hundreds of bank accounts, and the tracing of the same number of victims.

Unsecure networks

Around 19 million internet users in the UK access wireless (Wi-Fi) networks.[33] The increasing popularity of Wi-Fi networks, if not properly secured, can also open up new avenues for criminals. Over 7.8 million people in the UK have left their own internet access unsecured and open for anyone to use. If unsecured, criminals can use the network to hijack the PC or laptop to perpetrate frauds, delete or add malicious software onto the machine or use the network to download offensive or obscene images.

[29] House of Lords Science & Technology Committee Report – Personal Internet Security (p.14)
[30] http://www.thisismoney.co.uk/money-savers/article.html?in_article_id=407276&in_page_id=5.
[31] Get Safe Online
[32] http://www.cifas.org.uk/default.asp?edit_id=556-56
[33] Get Safe Online

Cyberabuse

Whilst video file sharing websites have transformed the way in which we can share experiences, there has been a disturbing trend in using these services for more sinister purposes. Images of violence, 'happy slapping', racist abuse, bullying and intimidation and other offensive incidents are all too commonly available for download and viewing.

Just a few months after the tragic killing of 11 year old Rhys Jones, youngsters in Liverpool were still posting images glorifying violence and gun crime. In the video, gang members brazenly show off an array of lethal weapons including different guns, knives, samurai swords and knuckle dusters. Other highly offensive images posted on video-sharing websites encouraging violence, abuse and hatred towards members of minority communities have also been highlighted.

Some have sought to support the right to post this material as some sort of defence of free speech and in keeping with the anarchic 'Wild West' tradition of the way in which the internet has developed. Yet with the migration of more traditional broadcast media to the internet platform which are subject to specific regulation on issues such as taste and decency (including the BBC making some of its programming available for download on You Tube) expectations are changing.

File sharing websites do operate 'take down' policies to remove offensive images notified to them. The Internet Watch Foundation (IWF) also undertakes extremely important work in identifying and flagging up offensive content, most notably in the context of the posting of images of child abuse. But complaints have been made about the speed with which ISP's and file sharing websites remove material or whether they remove it at all. Operators have taken the view that it is not their responsibility to make judgements on taste and decency. There is also no incentive for internet service providers to be pro-active. The defence in law under the EU E-Commerce Directive that they are a ‘mere conduit’ in supplying material almost acts in a way to discourage them from taking an interest, because once they are on notice legal liability may accrue.

Provisions in the Public Order Act 1986 make it an offence to distribute, show, play or broadcast threatening, abusive or insulting visual images or sounds intended to stir up racial hatred or where the circumstances are such that racial hatred is likely to be stirred up thereby. The Communications Act 2003 makes it an offence to send by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.

Yet the Home Office are unable to confirm if any prosecutions have been brought under this legislation for the uploading or posting of such material on the internet or how many formal complaints have been made by the police to internet service providers requiring that they remove images from their sites.

What action is being taken elsewhere?

European Convention on Cybercrime

The European Convention on Cybercrime was opened in November 2001 in Budapest, recognising the need to pursue a common criminal policy aimed at protecting against cybercrime by adopting appropriate legislation and fostering cooperation between countries and private industry. It is the first international treaty on crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

The Convention requires that at a national level measures should be taken to establish criminal offences on matters such as unauthorised access to a computer, unauthorised interference with data stored on a computer, unauthorised hindering or interference with a computer and the possession and sale of devices intended for use in connection with such offences. As well as aligning legislation with e-crime internationally, one of the core benefits is the ability to progress cyber-based investigations across borders with other participating countries, extending the reach and speed of investigations.

Whilst the UK was a signatory to the Convention, it has yet to ratify its provisions.

The Virtual Global Taskforce

The Virtual Global Taskforce is made up of international law enforcement agencies working together to fight child abuse online. The aim of the Taskforce is to build an effective, international partnership of law enforcement agencies that helps to protect children from online child abuse. Its objectives are:

- to make the Internet a safer place;
- to identify, locate and help children at risk; and
- to hold perpetrators appropriately to account.

The Virtual Global Taskforce is made up of the Australian High Tech Crime Centre, the Child Exploitation and Online Protection Centre in the UK, the Royal Canadian Mounted Police, the US Department of Homeland Security and Interpol.

France

In the last few weeks France has announced an action plan to combat cybercrime. The measures detailed by the French Minister of the Interior on 14 February included new criminal offences for hacking and identity fraud and changes to the French legal framework covering data capture and co-operation with law enforcement. Improvements are also proposed in the way in which the French police and the Gendarmerie work together to combat cybercrime with the establishment of a new group to handle internet fraud. A new advice and safety website is to be established from September which will also enable users to flag up illegal content. The French authorities have also announced that they will use their forthcoming Presidency of the EU to promote greater co-operation across Europe in the fight against cybercrime.

United States

The United States has had an Internet Crime Complaint Centre or "IC3" for some seven years. IC3 was established as a partnership between the FBI and the National White Collar Crime Centre to serve as a means to receive internet related criminal complaints. Last year it received over 207,000 complaint submissions with the total loss amounting from all referred cases of fraud amounting to just under $200 million.[34]

IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving internet related crimes.

The Computer Crime and Intellectual Property Section (CCIPS) within the Department of Justice is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. The Computer Crime Initiative is a comprehensive programme designed to combat electronic penetrations, data thefts, and cyberattacks on critical information systems. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts. Attorneys work to improve the domestic and international infrastructure-legal, technological, and operational-to pursue network criminals most effectively.

In 2001, following a successful model developed in the Northern District of California that demonstrated the benefits of a unit of prosecutors working closely with the FBI and other agencies to establish a relationship with the local high tech community and encourage them to refer cases to law enforcement, the Department expanded the program in ten cities by designating Computer Hacking and Intellectual Property (CHIP) units.[35] These units are specifically charged with building relationships with the FBI, other agencies, and the local high tech community.

The Division of Privacy and Identity Protection, the newest of the divisions of the Federal Trade Commission, oversees issues related to consumer privacy, credit reporting, identity theft, and information security. The Division enforces the statutes and rules within its jurisdiction, engages in outreach and policy development, and educates consumers and businesses about emerging privacy, credit reporting, and information security issues, as well as identity theft prevention and assistance. It also operates the Identity Theft Data Clearinghouse, which houses the US federal government's centralized repository for consumer identity theft complaints.

In addition the FBI has been running a concerted campaign against botnets. 'Operation Bot Roast' was launched in June 2007 and since then more than a million hijacked computers and more than $20 million in economic loss has been identified.[36] The operation also included joint working with the New Zealand authorities to target a suspected botnet ringleader.

Canada

The Royal Canadian Mounted Police have formed a distributed network of computer crime response units under the banner of a Technological Crime Program. The group research and develop computer forensic tools and provide forensic assistance to domestic and international accredited agencies and police services.

Reporting Economic Crime On-Line (RECOL) provides a single Website for reporting everything from credit card fraud to major corporate corruption. Crime complaints filed at the RECOL site are

[34] IC3, Internet Crime Report 2006, http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf

[35] United States Department of Justice – Computer Crime and & Intellectual Property Section, http://www.usdoj.gov/criminal/cybercrime/chips.html

[36] FBI Press Release, November 2007, http://www.fbi.gov/pressrel/pressrel07/botroast112907.htm

prioritized automatically and forwarded to the relevant RECOL partners selected by the complainant. Information flows freely and almost instantly to where it's most valuable. In this way, RECOL allows for improved communication between law enforcement jurisdictions, helping eliminate barriers and stopping criminals who might otherwise evade investigation and prosecution.

Support for those filing complaints to RECOL is provided by PhoneBusters, the Canadian Anti-fraud Call Centre. Aside from the RCMP and Phonebusters, other RECOL partners include the Ontario Provincial Police, the U.S. Internet Fraud Complaint Center, MasterCard Canada and the Canadian Health Care Anti-Fraud Association.

Australia

Australasian Police agencies have established the Australian High Technology Crime Centre (AHTCC). Its role is to provide a nationally coordinated approach to combating serious, complex and multi-jurisdictional high tech crimes (especially those beyond the capability of single jurisdictions); to assist in improving the capacity of all jurisdictions to deal with high tech crime; and to support efforts to protect the National Information Infrastructure. The AHTCC is staffed by members of the Australian Federal Police and State and Territory police from throughout Australia, as well as representatives from private industry and government departments.

The role of the AHTCC is to:

- Provide a national coordinated approach to combating serious, complex and multi-jurisdictional technology enabled crimes, especially those beyond the capability of single jurisdictions.
- Assist in improving the capacity of all jurisdictions to deal with technology enabled crime.
- Support efforts to protect the National Information Infrastructure (NII).

The AHTCC fulfils this role through the co-ordination of technology enabled crime matters between Australian law enforcement, the Federal government and international agencies. Serious and complex matters are either investigated by the AHTCC or through cooperation or referral to a partner agency. The AHTCC also an intelligence function a strengthen understanding of the technology enabled crime environment. An integral part of the AHTCC is the Joint Banking Finance Sector Investigation Team (JBFSIT) combating internet banking fraud.

New Zealand

The National Cyber Crime Centre (NC3) is being established and aligned with the Electronic Crime Laboratories (ECL) under a single national structure. A nationally focussed unit will improve Police's coordination with Government and key industry groups within New Zealand and other international groups and jurisdictions – both at strategic and operational levels. The National Cyber Crime Centre (NC3) will provide a single reporting point for e-crime able to be accessed through traditional telephone reporting channels and through enhanced Internet contact points, enabling the collection and investigation of complaints, coordinate Police's response to e-crime in New Zealand and technologies involved in the commission of an offence.

What would Conservatives do?

Conservatives recognise that current Government inaction and inertia is putting us at greater risk. We need both tactical and strategic improvement to deal with the growing threat of cybercrime. We need a response that addresses gaps in our knowledge and the scope of the problem and which places the concepts of on-line risk assessment and risk mitigation as a much higher priority within government, business and amongst individuals.

Improving Enforcement

- **We would create a new Police National Cybercrime Unit (NCU)**. Law enforcement against cybercrime needs to be strengthened. This requires specialist support and co-ordination. The NCU would be responsible for analysing trend and threat information received, supporting hi-tech crime investigations carried out by individual police forces and promoting higher levels of understanding and recognition of cybercrime implications in all police activities. We would ensure that the new cybercrime unit is fully equipped to combat cybercrime in conjunction with the e-crime unit of the Serious Organised Crime Agency (SOCA).

- **We would establish a cybercrime team within the Crown Prosecution Service**. This team, drawing on existing specialists within the CPS, would work closely with officers from the new police National Cybercrime Unit to further enhance capabilities and improve potential outcomes from prosecutions. We would also examine sentencing guidelines on cybercrime to ensure that the courts have proper regard to the fact that in a significant proportion of on-line crimes small individual offences occur on a serial, almost production line, basis and in sentencing the courts should take account of the whole picture and the intrusive nature of the crime committed.

Improving Reporting

- **We would establish a Fraud and Cybercrime Complaint Centre – a single reporting centre for cybercrime along the lines of the US Internet Crime Complaint Centre (IC3).** The reporting of cybercrime and cybersecurity incidents needs to be made much more straight-forward and accessible. In order to fight cybercrime we need to obtain a much clearer understanding of the scale, nature and extent of the threat and ensure that victims of cybercrime know how to report a crime or malicious on-line incident. We would establish an on-line complaint centre to enable users to provide real time complaints of spam, fraud, malicious software or website incidents. This would form part of a combined Fraud and Cybercrime Complaint Centre.

- **We will improve the way in which the Police record cybercrime and reverse changes that prevent the public reporting on-line financial fraud to the police**.

Promoting Greater Prevention

- **We would significantly upgrade the Government's on-line safety and advice website.** This on-line 'portal' would offer the public the most up to date information on cyber security and to help them protect themselves on-line. The website would be linked to the Fraud and Cybercrime Complaint Centre to enable people to report cybercrime on-line and to ensure that emerging threats are communicated quickly. We would develop this facility in conjunction with private sector partners to draw together best practice advice from industry on cybersafety as well as examining more effective ways in which to make consumers aware of the information that is available.

- Education and awareness of the potential risks in the on-line environment need to be enhanced. **We would promote cybersafety and cybersecurity as a core part of all ICT training in schools and colleges**.

- **We would work with industry to promote common standards and preventative software tools. This would be enhanced by the adoption of a BSI – approved Kite Mark recognising certain standards in internet security and on-line safety**. For example legitimate emails from large organisations could be recognised through electronic signatures embedded in the emails enabling more effective screening of fraudulent phishing emails by internet service providers preventing them from hitting consumer in-boxes. We would put in place mechanisms to maintain the viability and suitability of standards to take account of the changing nature of new and emerging cybercrime threats.

Providing leadership and promoting co-operation

- **We would designate a single minister for cybercrime**. Leadership within government and the emphasis placed on cybercrime needs to be strengthened to ensure that it is given the focus and priority it requires. That is why a Home Office minister reporting to the Home Secretary would be given responsibility for co-ordinating policy on cybersecurity, cybercrime prevention and international co-operation.

- **We would create a new framework to promote closer co-operation between government and business with the shared aim of reducing the risk of cybercrime**. We would create a Cybercrime Compact overseen by the Cybersecurity Minister bringing together government, the financial sector, hardware and software manufacturers and other business groups to promote closer working on initiatives to improve cybersecurity. In particular this forum would seek to develop common standards and more effective joint working between government and industry.

Promoting international partnerships

- **We would ratify the Cybercrime Convention and strengthen international partnerships with law enforcement agencies around the globe**. Because international co-operation and common standards between countries are such an essential part in bearing down on cybercrime wherever it may be originating from, we would also promote improved international co-operation and standards through the Internet Governance Forum and the G8.

Strengthening Cyberlaw

- **We would review existing legislation to ensure that it provides effective sanctions and offences against developing cybercrimes**. In particular, we would legislate to put beyond doubt that the hiring of botnets for the purposes of conducting or facilitating cyber attacks on others is a criminal offence.

- **In conjunction with the Financial Services Authority we would impose an obligation on financial service companies to report all malicious security incidents affecting their computer systems**. We will require all companies and businesses holding personal data on individuals who suspect that their systems have been hacked into and that personal information could have been compromised to report such incidents to the Information Commissioner and the Fraud and Cybercrime Complaint Centre and to make notification to their customers when required by the Commissioner.

- **We would create an offence of reckless handling of personal data by government, making it an offence for a Crown Servant or a government contractor to lose personal data from their control.**

Combating Cyberabuse

- The public need to be confident that appropriate measures are being taken regarding the posting of images which incite abuse, violence and race hate crime. However, virtually nothing is being done by the Government to address this serious issue. In order to promote strong social cohesion and to ensure greater public protection, it is essential that firm action is taken by internet service providers, the police and other law enforcement agencies to prevent attacks inspired or encouraged by such reprehensible activity.

- **A Conservative Government would conduct an urgent review of the existing criminal sanctions regulating the broadcast or publication of material which is intended to promote violence or hate crimes to ensure that the law is being enforced robustly and effectively.**

- **We would reform the 'mere conduit' defence for Internet Service Providers under the E-Commerce Directive as it is unsustainable in its current form.**

- We recognise that there is a balance to be struck between the need for freedom of expression whilst protecting the public from harm. But there is a clear shared social responsibility on the operators of file sharing websites and internet service providers to ensure that grossly offensive images are not made available for download. This responsibility extends not only to file sharing but to taking action against fraudulent websites and email accounts being used to perpetrate cyber-attacks on others.

- **We will assess what penalties (whether criminal or civil) should apply to internet service providers which fail within a specified time to act on requests to take down images or comply with requirements to remove bogus or inappropriate websites or to act on spam or other malicious email notified to them as originating from their services.**

We will consult on these proposals with both industry and users.

In addition to these specific measures we will examine the current data protection framework and arrangements to ensure that personal data and information is properly protected and secured. We will also undertake further detailed analysis on the protection of critical infrastructure from cyber attack and measures required to enhance national cyber security.

Cybercrime is a growing and serious threat to individuals, business and government. It is a problem that will continue to escalate as technology changes.

The Labour Government has failed in its duty and remains with its head stuck very firmly in the sand.

Conservatives will take action and treat the online threat with the priority that the future security economic and personal interests of this country demand.

The time to act is now.