Cyber Crime Strategy

Cm 7842

£9.50

Cyber Crime Strategy

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

March 2010

Cm 7842 £9.50

ISBN: 978 0 10 178422 1

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID P002357681 03/10 19585 2649

Printed on paper containing 75% recycled fibre content minimum.

CYBER CRIME STRATEGY

Contents

FOREWORD 3

1 BACKGROUND 4

1.1 Purpose of this document 4
1.2 Why are we doing this now? 4
1.3 Why does it matter? 5

2 THE BROADER CYBER SECURITY CONTEXT 8

3 CYBER CRIME: CURRENT POSITION 9

3.1 What is cyber crime? 9
3.2 The nature of cyber crime 9
3.3 Perpetrators of online crime 11
3.3.1 Financially-based Crime 11
3.3.2 Non-financial crimes 12
3.3.2.1 Threats to children 12
3.3.2.2 Hate crimes, harassment, and political extremism 12
3.4 The threat to the public 12
3.4.1 Financial Crime 12
3.4.1.1 Online fraud 12
3.4.1.2 Identity theft 13
3.4.2 Non-financial crimes 13
3.4.2.1 Child protection 13
3.4.2.2 Hate Crimes and Terrorism 14
3.4.3 Contempt of Court 14
3.5 The threat to business 14
3.5.1 Fraud 15
3.5.2 Data security 15
3.5.3 Intellectual Property Theft 16
3.6 The threat to Government 16
3.7 Indirect Impacts 16

4 THE GOVERNMENT RESPONSE 17

4.1 Vision 17
4.2 How we will do this 17

5 HOW THE HOME OFFICE WILL TACKLE CYBER CRIME 19

5.1 Enhance Government coordination to tackle cyber crime 19
5.2 Create a hostile environment for cyber criminals 20
5.2.1 Provision of reporting/recording structures 20
5.2.2 Law enforcement response 22
5.2.3 Technical development for law enforcement 26
5.2.4 Prosecution 26
5.2.5 Consumer Protection 27
5.3 Raising public confidence 27
5.3.1 Financial and technical safety information 27
5.3.2 Child Safety and Education 28
5.4 Working with the private sector 29
5.4.1 Financial Crime 29
5.4.2 Child Internet Safety 30
5.5 International working 31

6 WHAT WE WILL DO 33

7 GLOSSARY 35

8 WHO DOES WHAT? 36

9 BIBLIOGRAPHY 37

Foreword

When the Government published the "Cyber Security Strategy" in June 2009, we recognised the need for the UK to develop an integrated approach to tackling the threats from the internet and associated technology. One of the major parts of this, also recommended in the "Extending our Reach" strategy for tackling serious organised crime, was that the UK should develop a strategy for dealing with cyber crime.

The Government is strongly committed to ensuring that everyone in the UK has access to the benefits of the internet. The internet has brought, and will continue to bring, huge benefits to the UK, and we will encourage the growth of access to it. However, there are threats to the public and businesses, from cyber criminals that it is the responsibility of Government, working with all sectors, to tackle.

Cyber crime is no longer about those who seek to access computer systems for fun or to prove it can be done. The criminals behind such crimes are organised, and seek to take advantage of those using internet services. Whether this is for financial gain, or as threats to children, the effect on the victims can be devastating. The most vulnerable members of our society are all too often the victims – from young people threatened by bullying or sexual predators to the elderly who provide easy prey for organised fraudsters.

There is already a significant law enforcement response to crime committed on the internet, through the Serious Organised Crime Agency (SOCA) e-crime unit, the Police Central e-crime Unit (PCeU), the Medicines and Healthcare products Regulatory Agency (MHRA), H.M. Revenue & Customs, and the Child Exploitation and Online Protection (CEOP) Centre. All of these are tackling online criminals and protecting the public.

However, we cannot afford to be complacent. The threat from cyber crime is constantly evolving – with new opportunities to commit 'old' crimes in new ways as well as high-tech crimes that did not exist five years ago. Now is the right time to update and strengthen our response. We will continue to support the existing law enforcement response, and will work closely with the Office of Cyber Security (OCS) to ensure that there is cross-Government working to tackle all threats. We will ensure that there is Ministerial leadership to tackle online crime, and we will bring together Government, industry and the third sector to help develop a coordinated approach across the economy. We will work internationally, both bilaterally and through multilateral institutions, to support other countries in dealing with this crime.

We will also do more to improve public awareness of cyber crime through working with Get Safe Online: what it looks like, who is doing it and what the public and business can do to protect themselves from cyber criminals.

These and other measures will allow us to take action against cyber criminals from the organised groups at the top end right through to the long tail of organised criminality that exists underneath. Cyber crime threatens our safety, undermines our economy, and the scope and sophistication of cyber crime in the 21st Century demands an equally sophisticated and ambitious strategy to tackle it.

ALAN CAMPBELL
Parliamentary Under Secretary of State for Crime Reduction

1 Background

1.1 Purpose of this document

1. The Government published the UK Cyber Security Strategy in June 2009[1] and established the Office of Cyber Security to provide strategic leadership across Government, and to develop and coordinate the delivery of the UK Cyber Security Strategy. The Home Office is the lead Department for developing policies to counter cyber crime and its impact on UK interests and specifically the citizen.

2. This Home Office Cyber Crime Strategy sets out the Department's plan for coordinating and delivering that policy. It recognises that the means of delivery will in some cases lie beyond the Home Office (for example, the Department for Business Innovation and Skills) and that it will be necessary to work collaboratively with other departments and agencies to ensure a coherent approach. Of particular significance is the need to ensure that the Cyber Crime Strategy continues to develop to keep pace with changing threats and also to remain consistent with the work which is evolving within the Office of Cyber Security. Therefore, the Home Office will work closely with the Office of Cyber Security to contribute to their thinking; and this Cyber Crime Strategy will be reviewed on a 6 monthly basis to ensure consistency with the maturing work on the National Security Strategy[2] and the UK Cyber Security Strategy.

3. The Cyber Security Strategy identifies criminal use of cyber space as one of the three principal threats to cyber security alongside state and terrorist use. We said in that Strategy that we would publish a Cyber Crime Strategy, to form part of that overall approach to securing cyberspace.

4. This document sets out the Home Office's approach to tackling cyber crime, showing how we will tackle such crimes directly through the provision of a law enforcement response, and indirectly through cross-Government working and through the development of relationships with industry, charities and other groups, and internationally.

5. This strategy does not seek to duplicate work already being undertaken to tackle issues such as those relating to regulation of the internet, or to content on the internet. The Home Office is working with a number of partners to consider how to tackle content that is upsetting or offensive, but does not contravene the law.

6. Some of the areas covered in this Strategy are the responsibility of the Devolved Administrations. This Cyber Crime Strategy does not intend to duplicate existing work undertaken by those Administrations. Instead it intends to provide a strategic enabling framework through which to examine the challenges and the opportunities we face, and ultimately identify where we as a nation should be focusing our efforts in cyber security.

1.2 Why are we doing this now?

7. Computers, the internet and electronic communications play an ever-increasing part in all our lives, with the use of the internet in the home, at work or in educational establishments now standard and continuing to grow. The impact increases as new, and often unpredicted, applications of technologies are quickly adopted by significant proportions of the population. Mobile internet devices, such as smart phones, are now common, and a growing number of services, such as location-based services, are being created to work with them.

---

[1] Cyber Security Strategy – June 2009
[2] National Security Strategy – June 2009

8. We expect the rapid development and exploitation of computers and electronic communication technologies to continue to accelerate. The UK has made considerable progress toward the Government's vision of a digitally rich UK[3]. In the last 10 years, the UK has become one of the world leaders in the digital environment, particularly in digital TV and mobile phone markets. As shown in the Digital Britain Report[4], which we published earlier this year, the UK has a vibrant, valuable digital economy. The Government made a commitment in that Report to a universal broadband standard, available in the UK by 2012, to ensure that everyone in the UK can benefit from access to the internet.

9. However, this has implications for safety and security, including crime and its prevention, detection, investigation and prosecution. Cyber criminals are quick to spot the potential vulnerabilities of new technologies and exploit them to commit offences, or to try to frustrate detection of their activities.

10. As more and more of the nation's public and private assets are stored electronically rather than physically, often outside our jurisdiction, there will be more opportunities for crime. However, the same technologies can be used to protect ourselves and by our law enforcement agencies to detect, investigate and prosecute offenders.

1.3 Why does it matter?

11. As the Digital Britain Report sets out, there are significant benefits to the UK in developing and growing the digital economy. As more services and trade move online, including those provided by government agencies, so criminals will try to exploit this for their gain, in the same way as markets and trading have always attracted those who would seek to profit from illegal behaviour. The public, businesses and government are all at risk from organised crime groups, and from those who would seek to harm individuals, particularly children. Whether the crime is fraud, data theft from individuals, businesses, or Government, or child sexual abuse committed through the online environment, the impact of crime initiated on the internet can be devastating for its victims. Government needs to be involved to ensure that, as with the offline world, there is an appropriate response to crime when needed. The internet is here for the long-term, and criminals will seek to exploit it and profit from it, not just financially, and we therefore need to plan a long term response. The difference between traditional crime and cyber crime is that generally traditional crime occurs in one place and has an impact on one set of victims whereas cyber crime can have an impact globally at the push of a button, hence the need for a coordinated and timely response.

12. The internet has transformed the way millions of consumers buy goods and services. The UK is the leader in Europe in terms of the size of the internet shopping market; in 2008, the value of online retail sales was £48 billion[5]. In that year, 57% of UK individuals had ordered goods or services over the internet for private use in the previous year[6]. However almost one in three UK internet users are not shopping on line, with lack of trust in the internet the biggest reason[7]. Users also cite fears over personal security and lack of trust in companies selling over the internet. Cyber crime reduces consumer confidence and the costs can be high; for example losses from credit card fraud where the consumer's card was used without them present were £328m in 2008[8] (an increase of 13% from the previous year), crimes that involve stealing the innovation and design of music and film in the UK were estimated at £180m in 2008[9] and the annual loss to the economy from unresolved delivery problems with online sales is estimated to be worth as much as £55m per year[10].

---

[3] "Connecting the UK – the Digital Strategy" – March 2005
[4] Digital Britain Report – June 2009
[5] *UK cards association*
[6] EU Commission Consumer Strategy
[7] Findings from Consumer Surveys on Internet shopping – Office of Fair Trading
[8] UK cards association
[9] BPI
[10] Findings from Consumer Surveys on Internet shopping – Office of Fair Trading

13. As the Digital Britain Report made clear, the Government is keen to see the UK realise the full benefits of the internet, and to ensure that the public can use the services offered on it. Government, under the Home Access[11] programme, and other such initiatives, is committed to ensuring that all UK citizens have access to the internet.

14. One of the major ambitions of the work from the Digital Britain Report was that the internet should be safe for business and consumers to use, to ensure that everyone can have confidence in using the internet for business and pleasure. This in turn will have significant benefits in supporting economic confidence and ensuring and protecting the economic recovery, through the factors identified in the Report

    - The intellectual property of businesses, universities and other institutions, which underpins a knowledge economy, will be better protected.
    - Businesses using UK networks will gain a competitive edge in the global marketplace, developing innovative products and services.
    - UK citizens and business will prosper as the volume of business transacted securely online continues to increase.
    - UK citizens will have greater confidence in public service transactions; thus yielding efficiencies and cost saving.
    - The businesses that have delivered secure functionality will have opportunities to sell their services globally on the back of UK success.

15. This strategy sets out how the Home Office, both directly and in collaboration with others, will ensure that consumers can have confidence in the internet through providing a response to crime committed through the medium.

16. As part of improving the efficiency of Government services, there is a drive towards better and more convenient provision of services in respect of a number of the Government's tax regimes, such as the provision of tax credits, VAT and income tax returns online. These improvements are potentially at risk from cyber criminals seeking to defraud public services or falsely obtain credentials, and we need to ensure that such services are protected from criminal exploitation.

17. The "Extending Our Reach" paper on tackling organised crime[12] identified that the threat from organised crime in particular is likely to grow as criminals utilise new technologies, and set out our determination that our response should not only keep pace but aim to stay several steps ahead. The paper set out a strategic approach to tackling organised crime, based on developing a comprehensive understanding of the scale of organised crime and the working methods of modern criminals, and putting in place a strategic structure to coordinate law enforcement and other government activity. The Strategic Centre for Organised Crime was launched in Summer 2009, to strengthen coordination of, and provide strategic direction for, Government work to tackle organised crime.

18. Cyber criminals are becoming more sophisticated, and continue to develop malicious software and devise improved methods for infecting computers and networks. This is not purely confined to technological advances: the criminals are also refining their social engineering techniques to improve infection rates. Cyber criminals will continually adapt their tactics, as new defences are implemented, in order to serve the illicit market in compromised private data. Infection of computers, although primarily aimed at harvesting identities for financial gain, is also a method of gaining control of tens of thousands of computers which are then used for attack on industry or infrastructure.

---

[11] Home Access Programme – www.homeaccess.org.uk
[12] "Extending our reach – a comprehensive approach to tackling serious organised crime" – July 2009

19. Child sexual offenders have adapted to the use of technology, and as the internet and its associated technologies have evolved so too has the offender's use of it, not only reacting to how young people occupy this space and the risks they generate themselves, but also becoming active creators and distributors of content generated through both their online and offline abusive behaviour.

20. The House of Lords Science & Technology Committee report into Personal Internet Security[13] made clear that Government cannot and should not do it all, and that we need to construct an environment that allows industry, Government, law enforcement and Non-Governmental Organisations (NGOs) to come together and look at the key developments with a view to understanding their potential both to facilitate crime and to facilitate its prevention and detection.

[13] House of Lords Science & Technology Committee Report "Personal Internet Security" August 2007

2 The Broader Cyber Security Context

21. Cyber security embraces both the protection of UK interest in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers. As set out in the Cyber Security Strategy, and supported by the Digital Britain Report, the Government believes that the continuing openness of the internet and cyberspace is fundamental to our way of life, promoting the free flow of ideas, and innovation of new products and services, to strengthen democratic ideals and deliver the economic benefits of globalisation. The Home Office approach seeks to preserve and protect the fundamental rights to which we are accustomed (including privacy and freedom of expression) because it is on these rights that our freedoms depend. A fundamental challenge for any government is to balance measures necessary to protect security and the right to life with the impact they have on the other rights that we cherish and which form the basis of our society.

22. Cyber security poses particular challenges in meeting the tests of necessity and proportionality, as the distributed, de-centralised and unbounded form of cyberspace means that a wide range of tools must be deployed to tackle those who wish to use it to harm the UK's interests or harm individuals in the UK. A clear ethical foundation and appropriate safeguards are essential to ensure that the public continues to support the work of those charged with tackling crime on the internet.

23. There are a significant range of threats to the UK from activity on the internet. As set out in the Cyber Security Strategy, as well as cyber crime there is potential for state-sponsored attacks on the national infrastructure, or the use of the internet by terrorists for recruitment and radicalisation. Cyber security is multi-faceted, and there are many groups across Government, and beyond, that work to ensure that the UK is protected online. The strategic direction for all of these groups will be developed and set under the auspices of the OCS.

24. The Home Office will ensure that its work to tackle cyber crime is coordinated with work to protect national security and the national infrastructure. This includes the development of overall strategies to prevent harm to the UK, to provide an effective Government response, and to ensure that all sectors of society work together to tackle the threats.

25. It is important to remember that cyber security is not an end in itself, but that it enables and protects economic and social activity, and should not discourage the use of new technologies. The Government's goal is to enable the full benefits of cyber space to be available for the UK, while protecting our society and allowing the UK digital economy to grow.

3 Cyber crime: Current Position

3.1 What is cyber crime?

26. There is a wide range of offences that can be committed through communication technology. Cyber crimes are commonly considered as falling into one of two categories: new offences committed using new technologies, such as offences against computer systems and data, dealt with in the Computer Misuse Act 1990; and old offences committed using new technology, where networked computers and other devices are used to facilitate the commission of an offence. In the former are crimes such as hacking or breaking into computer systems to steal or alter data; in the latter, crimes such as the transfer of illegal images or fraud. The former are often a precursor to the latter, based on motives of financial gain. However, while the focus is often on online fraud or child protection, there is a significant number of other offences committed through the internet, such as harassment, threatening behaviour and other anti-social activity.

27. The Home Office believes that actions should be legal or illegal according to their merits, rather than the medium used, so that what is illegal offline should be illegal online. The Home Office believes that the internet and other communication technologies are the conduit for the criminal activity for such groups, rather than being the cause. We are committed to ensuring that where additional legislative or regulatory tools are appropriate to tackle cyber crimes these are introduced swiftly and effectively.

28. For the sake of consistency, the term "cyber crime" will be used throughout this document, although there are other terms, such as e-crime, that are regularly used. We also recognise that the term cyber crime does not fully reflect the issues of child protection involving the internet and associated technologies.

3.2 The nature of cyber crime

29. The challenge posed by crimes initiated or committed through the online environment is not so much their identification as the nature of the environment in which they are committed. Cyber criminals can operate from anywhere in the world, targeting large numbers of people or businesses across international boundaries, and there are challenges posed by the scale and volume of the crimes, the technical complexity of identifying the perpetrators as well as the need to work internationally to bring them to justice. The internet opens up new opportunities to cyber criminals and enables aspiring criminals to enter the environment, based on a belief that law enforcement struggles to operate in the online world.

30. From a child protection perspective a key issue facing law enforcement is not simply the volume of child sexual abuse material that is being circulated, but the ease by which this medium offers child sexual predators the opportunity to network with each other to create and distribute content, as well as the opportunity to access new victims, either offline or through online spaces, such as instant messaging or social networking sites. Online paedophile networks can easily run into tens of thousands of suspects worldwide.

31. While the offence committed may be recognisable, cyber crime poses a number of significant difficulties for traditional policing across all types of crime committed on the internet. While not all of these apply in every case, they are recognisable as issues in many of the investigations run by law enforcement.

Cyber crime Tools

32. The number, sophistication and impact of cyber crimes continues to grow. These threats evolve to frustrate network security defences, and many business systems and home computers do not keep what protection they have up to date. "Hacking" has evolved from the activity of a small number of very technical individuals to an increasingly mature marketplace where technical skills and data can be purchased by criminal groups to carry out specific attacks. The trend therefore is for growth in the threat to internet security, as evidenced by the following figures[14]:

    - In 2008, 55,389 phishing website hosts were detected, an increase of 66% over 2007.
    - A 192% increase in spam detected across the internet, from 119.6 billion messages in 2007 to 349.6 billion in 2008. The most common type of spam detected in 2008 was related to internet or computer related goods and services, which made up 24% of all detected spam.
    - Active bot-infected computers – an average of 75,158 per day, showing an increase of 31% from the previous period. In 2008, bot networks were responsible for the distribution of about 90% of all spam e-mail.

33. Not only are criminals making or developing their own tools, but they also use legitimate or publicly available software, such as peer to peer, to network and to share files and illegal images.

Scale

34. The nature of the internet not only allows criminals to be located in a different country to the victim, but they can target many thousands of victims at once. A phishing e-mail can be sent easily to hundreds of thousands of people from one computer, and a single person can infect many computers with malicious software. The transmission and collection of significant numbers of illegal images is possible through the use of peer-to-peer networking.

International

35. The internet offers the potential for a criminal to commit offences across geographical and jurisdictional boundaries. This poses challenges for traditional law enforcement, even at a national level, as the same offence may be committed against individuals in many countries, at the same time; equally, the same act may be judged differently in each jurisdiction.

36. Those who commit cyber crime offences commonly seek to exploit this, undertaking their activities in one country but delivering the effect in another jurisdiction. This can assist in masking their undertakings and create difficulties for investigators in tracing them. In deliberately targeting their activities in or through jurisdictions where regulation or legislation is not strong, or where investigative or other co-operation is known to be poor, cyber criminals can minimise the risk of their activities being discovered or punishment being effected. International investigations require a time-critical response to help negate attacks as well as secure evidence.

Lack of compatibility of criminal offences and investigative methods

37. The compatibility of criminal offences and investigative measures across a range of jurisdictions is one of the most effective ways of enabling international co-operation. Within the United Nations, the Internet Governance Forum, the Council of Europe and the European Union much work has been undertaken to achieve progress towards this position in relation to cyber crime, but beyond that the

[14] "Internet Security Threat Report" – Symantec, October 2009

picture is not as positive. This can lead to the displacement of cyber crime to and through jurisdictions where lower standards exist, presenting the cyber criminal with enhanced opportunities to avoid detection, prosecution and imprisonment. In some areas, particularly child protection where the focus has been stronger, the position is better and much work has been undertaken to tackle the sexual abuse and exploitation of children and young people, but even here we are far from agreed international standards. Along with these issues are the operational protocols and the need for investigators and prosecutors to work quickly to gather evidence of criminal conduct from network operators and online service providers.

Technical complexity

38. The nature of cybercrime means that investigations are often technically complex, requiring access to specialist skills and / or the support of the private sector. Evidence gathering is difficult and time-consuming, especially when the data evidencing the crime has been routed through a number of countries. The work required by law enforcement, for example, to track down those behind fraudulent websites, and those running paedophile peer-to-peer filesharing networks, is significant.

Lack of good security/security practice

39. With many forms of crime, the public and business understand the need to have proper security in place to prevent it. The need for proper house locks, security on cars, and general anti-crime measures taken by business in the offline world are well understood, such as the Thatcham vehicle security standards. The same approach is required online, but the complexity of the technical solutions to provide security online can be confusing and difficult to understand for some users. Additionally, many data breaches have little to do with technology, but are caused by poor practice or carelessness.

40. The nature of the way that the internet is accessed, often from the comfort of the home or office, may lead to a relaxing of the awareness of threats that would not be the case if a person was offline.

3.3 Perpetrators of online crime

3.3.1 Financially-based crime

41. As “Extending our Reach” set out, cyber crime is being undertaken by serious organised criminals, who target government, business and the public to obtain money or goods. Their motivation is largely for financial gain, but it can also be to inflict personal harm. This can have a profound impact; the losses are significant, and provide criminals with funding which they can use in other areas.

42. The most significant cyber criminal activity is conducted within multi-skilled, virtual criminal networks, whose structures are different to traditional organised crime groups. Virtual criminal networks are often focused around an online meeting place, either a web forum or Internet Relay Chat (IRC) channel. Members rarely meet in person and individuals are known only by their online alias or nickname. The more sophisticated networks vet prospective members to prevent law enforcement officers infiltrating them and to ensure only trusted associates can gain access to the goods and services available or on sale.

43. Virtual criminal networks can have several thousand members, but they are usually run by a small number of experienced, specialist online criminals. The leading members of a network, often consisting of 10 to 30 online identities, will divide the different roles between themselves, for example hacking, spamming, compromising victim machines and trading compromised private data. This inner circle of technically-advanced and experienced criminals is responsible for supervising and policing activity in their own specialist areas and resolving disputes between individual members. Some "elite" networks are highly secretive and do not participate in online fora, since they have the resources to carry out cyber crime offences through the complete cycle (data theft, exploitation, fraud and money laundering) and have no need to engage outsiders. There is evidence that these organised crime groups are sophisticated in that they operate within a cellular structure, there are clearly controlling minds and there is collaboration across groups, as the crime is non-competitive.

44. The main purpose of these groups is financial gain, but some of this may be for use to fund terrorist activities.

3.3.2 Non-financial crimes

3.3.2.1 Threats to children

45. In terms of child sexual abuse and exploitation the picture of offenders is a complex one, which is related to the criminal interests of the individuals or networks that use the internet to seek out victims and acquire new material. There is no single type nor are the groupings below mutually exclusive, but they can be roughly translated into three main areas:

    - those that target children and young people in the online environment that they inhabit e.g. instant messaging, chat, and social networking sites;
    - those that engage in offline abuse, create images and share them online with networks of like-minded individuals or are recipients and collectors of such material; or
    - those that use the internet to link up and identify the best places in the world to travel to abuse children or young people or who use the internet to lure this vulnerable group into some form of exploitation.

46. Offenders can be interested in boys, girls or both.

3.3.2.2 Hate crimes, harassment, and political extremism

47. Other forms of harm-based crime, such as racial or religious hatred, harassment, or political extremism, may be carried out by individuals or by organised groups, and focus on particular issues.

3.4 The threat to the public

48. The public are targets of criminals or anti-social behaviour in various ways through the internet, and often have concerns about how they can keep themselves safe online, and where such information can be gathered from.

3.4.1 Financial Crime

3.4.1.1 Online fraud

49. There are many types of fraud targeted at the public, ranging from credit and debit card fraud, lottery scams, "419" fraud, non-delivery fraud and fraud perpetrated through online auction websites. Additionally, the public is at risk from fraud involving fake goods, such as watches or clothing, or more seriously from fake and unsafe pharmaceuticals bought online. None of these are unknown offline, but cyber criminals are able to use the internet to perpetrate these offences on a mass

scale, and are able to use the internet to hide their real identities and locations. This is not just a UK problem – according to the US Internet Crime Complaint Centre (IC3)[15], the total loss from fraud on the internet reported to them was $560m in 2009, with the most significant loss coming from non-delivery of goods.

3.4.1.2 Identity theft

50. The driver behind the majority of data thefts is the profitability of compromised private information, particularly detailed financial information. Criminals obtain large quantities of data, such as credit card data and sell it either directly to those able to realise its monetary value through fraud, or to those who act as data brokers, aggregating data from different sources and selling it to other criminals. Criminals of all types and levels, including individuals looking to carry out small-scale, high volume frauds are able to buy compromised private data directly from the primary sources. ID crime can also be used to facilitate virtually all forms of serious crime including money laundering and human trafficking.

51. Individuals are targeted primarily for user names and passwords to enable criminals to access, and in some cases to control online accounts. These are usually bank accounts but other types, such as online brokerage accounts, may also be compromised. Criminals also attempt to gain private details of their payment card accounts. This can be achieved by tricking the account holder into revealing private data through fake emails and websites ("phishing") or by infecting the account holder's computer with malicious software ("malware") that automatically intercepts and forwards data to the criminal. Individuals are also victimised by attacks on businesses, where data is stolen in bulk. Although public awareness of these threats is improving, the attacks are becoming increasingly sophisticated.

52. Identity fraud continues to increase, and in the first 6 months of 2009, there were 43% more victims of impersonations, a 74% increase in successful identity fraud and a 40% rise in facility takeover fraud (where criminals gain access to legitimately obtained accounts of innocent victims)[16]. The cost to the UK economy is at least £1.2 billion and accounts for a criminal cash flow of some £10m per day[17]. It can typically take 48 hours work for a victim to put their affairs in order[18].

53. The data is not only stolen online, but obtained through traditional forms of data theft, such as through purchasing records from employees or through theft. The data gathered through these methods can be used online.

3.4.2 Non-financial crimes

3.4.2.1 Child protection

54. The use of the internet by children is significant. They use it, for example, for social networking, gaming and as a research tool for school projects. However, it is a mechanism through which those who seek to harm children are able to operate. Children can use the internet, and meet people through it, without some of the traditional barriers that have in the past prevented them meeting what adults would term "strangers". Moreover, it is increasingly a place where child sexual abuse within families or extended families is recorded and shared through images or video with like minded individuals across the world.

---

[15] IC3 Annual Report 2009
[16] CIFAS survey based on analysis of over 50,000 victims of identity fraud
[17] Home Office Identity Fraud Steering Committee Oct 2008
[18] CIFAS – the UK's Fraud Prevention Service

55. As with other forms of crime on the internet, this poses a challenge for law enforcement. The same issues of not being geographically based, of being able to mask real identities, and being able to gather information on the victim without their knowledge are all common. What is not common is the motive. The perpetrators are not financially motivated, but seek to harm or sexually exploit children.

56. The transfer of illegal images of child sexual abuse as well as communications between offenders, is made easier by new technology, and there are times when the public accidentally see such images.

57. Harassment and bullying are significant issues, especially for children, who often cite these as their own areas of greatest concern. The nature of the technology, which children often carry with them all the time, allows bullying to take place not only in school but continue outside. This can make the victim feel threatened and unable to escape the bullying, leading to a feeling of powerlessness.

3.4.2.2 Hate Crimes and Terrorism

58. The internet facilitates the prolonged, consistent perpetration of "hate crime" and some victims can experience hate incidents and hate crimes over a prolonged period of time at roughly the same level of intensity. Whether this is an email sent anonymously or a website dedicated to spreading abhorrent messages, this can have a high impact on victims and communities when it is part of a pattern of repeat victimisation. Even when not part of a pattern of victimisation, research has found that 'minor' hate crimes can produce as much emotional harm for victims as so called 'serious offences'.

59. The accessibility, immediacy and popularity of the internet that makes it vulnerable to criminal exploitation are similarly attractive for those who wish to promote violent extremism of terrorism. Some of the material they produce may constitute a criminal offence, for example that which incites or glorifies indiscriminate violence. The use of the internet by terrorists is beyond the scope of this strategy but is covered in the Government's Counter-Terrorism Strategy, CONTEST[19].

3.4.3 Contempt of Court

60. The speed at which material can be disseminated on the internet and the role of the internet as an archive also raise potential risks to the criminal justice process and the right of defendants to a fair trial, or to the protection of vulnerable victims, witnesses or offenders.

61. This is covered by the contempt of court legislation which applies to individuals as well as to established news organisations and other businesses and to publications on the internet. As with paper publication, any material that might constitute contempt of court may lead to legal proceedings.

62. In addition, to minimise risks to a fair trial, judges give directions to juries only to consider the evidence heard in court and not to be influenced by external matters such as media reports and not to do their own research whether on the internet or elsewhere.

3.5 The threat to business

63. The commercial sector is dependent on the internet and electronic information, and is affected by cyber crime in a number of ways.

[19] CONTEST – The UK's Strategy for Countering International Terrorism 2009

3.5.1 Fraud

64. As with the threat to the public, fraud is a major concern for businesses. This may be through legitimate businesses being defrauded online, or through unfair competition from fraudulent businesses. The mechanisms for such frauds may be through goods being paid for with stolen or forged credit cards, or through credit card companies having to reimburse consumers who have had their details compromised.

3.5.2 Data security

65. The data that online criminals need to commit theft or fraud can be acquired from individuals or from companies. Commercial data breaches are a sensitive issue for companies that are the victims, and this makes it difficult to assess the scale of the threat and also to determine whether the biggest risk comes from external attackers or corrupt insiders. Successful data thefts result mostly from attacks on three vulnerable areas: data held by individual internet users; data stored centrally; or data in transit between an individual and an organisation, such as on laptops, memory sticks or other moveable media.

66. Centrally-held data typically consists of bulk payment card and identity data stored in a database. This data is targeted by criminal hackers who try to overcome security measures protecting the data so they can steal it in bulk. Highly skilled criminals are constantly scanning operating systems and application software for new security vulnerabilities. Once discovered, they develop and deploy new attack tools to breach the security of these systems. Where known security vulnerabilities are not addressed by organisations it can result in successful data breaches, leading to loss of data, intellectual property or other sensitive information. This, together with instances of inadequate implementation of data security standards, highlights the fundamental need for the public and private sectors to do more to protect the security of data they hold on customers and clients. As with attacks on individuals, stolen data is used for frauds, including identity crime.

67. The impact upon business from internet crime can be significant, and can lead to loss of money, reputation and disruption to businesses. According to the BERR Information Security Breaches Survey[20], across all UK companies, 45% had suffered some type of electronic security breach in 2008. This is lower than the figure of 63% for 2006. The breach figure is much higher (72%) for large companies, perhaps reflecting the much larger electronic networks that such firms have, the greater number and expertise of the IT staff in identifying incidents, and the potential gain for an offender breaching security on a large network. Of the large companies that had suffered a breach, 76% had suffered at least one 'serious breach'.

68. Estimating the cost of a security incident is problematic, but the costs can include resource spent investigating and responding to the incident, business disruption, damage to reputation and loss of data as well as compensation and other direct cash costs. In the BIS survey, the average cost of an organisation's most serious incident was between £10,000 and £20,000, slightly up on previous survey results. However, costs increase with the size of the business, with a range between £90,000 and £120,000 for large businesses, and £1m to £2m for very large businesses.

[20] BERR Information Security Breaches Survey 2008

3.5.3 Intellectual Property Theft

69. In the Digital Britain Report, the Government recognised the problems caused by the use of technology to allow intellectual property to be unlawfully copied and circulated via the internet. Illegal filesharing using peer-to-peer (P2P) technology over the internet affects the creative industries sector, which accounts for 6.4% of UK GVA (Gross Value Added). There is also the threat of intellectual property being stolen through illegal access to systems by people inside or outside a company, leading to a loss of revenue for the patent owners.

70. The protection of intellectual property rights (IPR) is important to industry as it often represents their net worth. Amongst others, high-tech industry needs to protect designs and software from theft and reuse for which they have invested significantly in many years of research and development. Highly sophisticated crime networks target high-worth information such as this for sale.

71. It is impossible to accurately calculate the cost to industry resulting from unlawful IPR theft and distribution given that estimates are based on survey data and counterfactual analysis of consumer behaviour. All figures therefore are subject to a degree of challenge and argument, not least due to the range of studies claiming different impacts of P2P on sales. However, even when allowing for some inaccuracy, the level of losses suffered is considerable. The British Phonographic Industry (BPI) claim P2P file-sharing costs the UK music industry £180m pa (2008) while the research company IPSOS gives a loss in the UK for TV and films of £152m (2007). Additionally, people inside or outside a company can steal intellectual property through illegal access to systems.

3.6 The threat to Government

72. As well as the threat posed to the general public, cyber crime poses a number of challenges for Government. Government can be the target of attacks from online criminals, who target the services provided by Government for the public with the aim of financial gain, or for gathering data on individuals. The increasing availability of government services online provides opportunities for criminals. Fraudulent applications for services such as benefits / tax credits, and tax repayments may be perceived by criminals to be less well monitored or to offer more anonymity and less human interaction than more traditional fraud would require. There is a risk that the increasing provision of services online by Government will lead to more attempts to defraud Government.

3.7 Indirect Impacts

73. The Government strongly supports the use of the internet, and recognises the benefits that it gives to our society, both the public and business. The Digital Britain Report made clear that crime on the internet is a concern, and has the potential to prevent the full take up of the benefits of the internet. There is also the possibility that some of the benefits already in place would be undermined if crime were to affect many more people than it does. Although the relationship between fear of crime on the internet and the use of the internet needs to be examined further, as shown by the OFT report it is reasonable to suppose that the fear of crime acts as a deterrent to use. This may be especially true for consumers and small businesses, who are the targets of attacks from criminals, but who have limited ability to defend themselves. There are also indirect costs to businesses that have invested in online capacity, but do not get a return on their investment due to the consumer's fear of using those services.

4 The Government Response

4.1 Vision

74. The Cyber Security Strategy set out the Government's vision for the future of cyber space as

Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience.

75. This document sets out how the vision will drive the work of the Home Office to tackle cyber crime.

4.2 How we will do this

76. To achieve this we will:

- Coordinate activity across Government to tackle crime and address security on the internet in line with the strategic objectives laid out in the UK Cyber Security Strategy.
- Reduce the direct harms by making the internet a hostile environment for financial criminals and child sexual predators, and ensuring that they are unable to operate effectively through work to disrupt crime and prosecute offenders.
- Raise public confidence in the safety and security of the internet, not only through tackling crime and abuse, but through the provision of accurate and easy-to-understand information to the public on the threats.
- Support industry leadership to tackle cyber crime, and work with industry to consider how products and online services can be made safer and security products easy to use.
- Work with international partners to tackle the problem collectively.

To coordinate across Government, the Home Office will:

- Provide clear ownership within Government, at ministerial level, for cyber crime and criminal conduct in the UK.
- Review all legislation affecting or relevant to cyber crime, to ensure that it is adequate to address our needs.
- With the Cabinet Office, Ministry of Justice and the Information Commissioner's office, establish standards of data handling and promote the requirement for a duty of care from all individuals and bodies that hold individuals personal data.

To create a hostile environment for cyber criminals the Home Office will:

- Provide an effective law enforcement and criminal justice response, through specialist units, and ensure that intelligence is shared where appropriate.
- Develop, over time, a clear understanding of the scale and scope of cyber crime, including robust and easily accessible reporting systems for both the public and business, which we will monitor for trends.
- Produce a regular strategic overview of the threat to children and young people from those who use technology to harm and abuse them.

- Develop tools, tactics and technology, working with the internet industry, to ensure that law enforcement are able to detect, investigate and pursue online criminals even when the technology changes.

To raise public confidence in the internet the Home Office will:

- Ensure the provision of safety information to the public on all types of cyber crime and internet harm, signposting to specialist units as appropriate.
- Continue to mount and support campaigns to raise awareness of internet safety issues.

To support industry leadership the Home Office will:

- Work with the internet industry and commercial business to ensure that safety and security are factors in designing services and that criminals are deterred from exploiting the online environment.
- Ensure that there is successful liaison between all groups working to protect the public.

To tackle cyber crime internationally the Home Office will:

- Work internationally to tackle cyber crime, including through effective collaboration with countries that have a well-developed understanding and capacity.

5 How the Home Office will tackle cyber crime

5.1 Enhance Government coordination to tackle cyber crime

77. As networked or internet enabled devices become ubiquitous, and a significant number of government departments provide some or all of their services via the internet, there is a responsibility upon Government to provide leadership in responding to cyber crime at a policy level.

78. We believe that we can and should enhance the fight against cyber crime at government level by ensuring an integrated response, led by the Home Office but working with other Government Departments and in line with the strategic objectives laid out in the UK Cyber Security Strategy.

79. The Office of Cyber Security within the Cabinet Office, has recently been set up to provide coordination of the overall response to threats from the internet. The Office of Cyber Security is the strategic lead for a broad programme of work to secure the UK's advantage in cyber space. Working with partners across government, including the Home Office, and industry, the Office aims to:

    - Reducing the risk to the UK's safe and secure use of cyber space.
    - Exploit opportunities in cyber space.
    - Improving knowledge, capabilities and decision-making.

80. In 2008, following the publication of the Byron Review[21], the Government set up the UK Council for Child Internet Safety (UKCCIS), to ensure that the protection of children online could be coordinated across Government through the joint leadership of the Department for Children, Schools and Families (DCSF) and the Home Office.

81. The Government believes that this has proved an effective model, and we will seek to ensure leadership of Government action to tackle other areas of cyber crime through similar models. In particular, the Home Office will work closely with the Department for Business, Innovation and Skills (DBIS), firstly to coordinate the law enforcement response to cyber crime, and secondly to lead work to ensure a safe internet environment for the public, business and industry to use.

82. There are already standards for data processing and data handling obligations in all sectors, and these are set out in the Data Protection Act 1998 and the Cabinet Office's Data Handling Review, published in 2008. In addition, the Information Commissioner has a statutory duty to promote the following of good practice in this area and the dissemination of guidance. In practice, this involves producing information aimed at the public about the need to protect their personal data; indeed, the Information Commissioner's Office has produced information for young people about keeping their information safe online, including advice on using social networking sites.

83. The Home Office will work with the Cabinet Office, Ministry of Justice and the Information Commissioner's office, to establish standards of data handling and promote the requirement for a duty of care from all individuals and bodies that hold individual's personal data.

What we will do:

- **Ensure consistency with the maturing work on the National Security Strategy and the UK Cyber Security Strategy.**
- **We will create a Ministerial Committee for cyber crime, led by ministers from the Home Office and BIS, who will work with ministers from other Government departments, and lead the cross-Government effort to tackle cyber crime. This Committee will work closely with OCS.**

---

[21] "Safer Children in a Digital World" – Dr. Tanya Byron, April 2008

- **We will review the current legislation with the aim of future-proofing it and ensuring the continued relevance of it to the fast-moving world of the internet particularly with regard to the ability to commit crimes on an industrial scale. We will ensure that legislation across relevant departments considers the impact of cyber crime.**

5.2 Create a hostile environment for cyber criminals

5.2.1 Provision of reporting/recording structures

Reporting

84. A major concern for the Home Office with regard to cyber crime is the lack of accurate information relating to the scale and scope of crimes committed through the medium, which makes it difficult to identify what action should be taken in response.

85. A number of areas have been very successful in acting as reporting points for crime or the threat of crime on the internet. The Child Exploitation and Online Protection Centre (CEOP) has developed considerable expertise in acting as a reporting centre for the public and particularly children who feel threatened online, and have been able to use the information gathered through those reports to identify and safeguard the children involved as well as help arrest the perpetrators. Their simple and effective CEOP "ClickCEOP" Report mechanism which, allied to a comprehensive education programme in UK schools, delivers reassurance to young users that they can access help, advice and, if required, police action at the click of a button and provides a strong deterrence message to would-be offenders. The Internet Watch Foundation (IWF) is the UK reporting point for websites containing illegal images, and as a result of its work, in partnership with law enforcement, the proportion of such websites hosted in the UK has dropped from 18% in 1997 to less than 1% now.

86. However, we recognise that there is still work to do in the online financial crime area, where the mechanism for reporting cyber crime is less developed. We believe that we need to consider the best way of gathering reports of financially-motivated cyber crime, which allows the public and business to report such crimes in a way that is easy and accurate.

What we will do:

- **We will learn from the experience of developing Action Fraud (the National Fraud Reporting Centre (NFRC)) and the Consumer Direct online reporting facility, as well as that of CEOP, and consider how best to receive and record reports of crime and attempted crime not only of fraud on the internet, but also for other internet crimes where there is no existing reporting centre.**
- **We will include questions relating to cyber crime in the British Crime Survey, to understand what the impact of these crimes is relation to other crime, and to identify changes in levels of confidence.**
- **We will continue to support CEOP, the Medicines and Healthcare products Regulatory Agency (MHRA) and other agencies which act as reporting centres for specific types of online offences.**

Classification/Recording

87. The House of Lords Science & Technology Committee report on "Personal Internet Security"[22] recommended that there should be a classification scheme for recording cyber crime. We recognise that there is a need to ensure that we can accurately measure crimes committed through the internet, to ensure that our response can be tailored to prevent it.

[22] House of Lords Science and Technology Committee Report on Personal Internet Security

What we will do:

- **We will work to develop a classification scheme for recording cyber crime, in conjunction with the law enforcement agencies and with the internet industry and business.**

ACTION FRAUD

The wide ranging Government review of fraud which reported in 2006 led to the creation of the National Fraud Authority (NFA) and the designation of the City of London Police as the national lead force for fraud. The NFA, an executive agency of the Attorney General's Office is the Government's strategic lead on counter-fraud activity. The first National Fraud Strategy was published in March 2009. The strategy's four aims are:

- building, sharing and acting on knowledge
- tackling the most serious and harmful threats
- holding more fraudsters to account while also improving support to victims, and
- improving the country's capability to prevent fraud.

Two key deliverables of this strategy are Action Fraud which is led by the NFA and the National Fraud Intelligence Bureau (NFIB) which is delivered by the City of London Police as part of its lead force responsibilities.

Action Fraud will provide a first point of contact for individuals and small businesses reporting fraud using the public facing name 'Action Fraud'. Action Fraud will not only provide guidance for victims of fraud but also the reports it receives will be fed into the National Fraud Intelligence Bureau. The NFIB will receive and analyse information from Action Fraud and also from a number of anti fraud organisations enabling it to provide comprehensive intelligence about fraud taking place across the country which may lead to targeted enforcement action.

As noted in section 3, on-line attacks account for an increasing level of identity theft which is a key enabler of fraud. In Summer 2009 the Inter-Ministerial Group on Fraud agreed an NFA proposal to set up an Identity Crime Taskforce for the next twelve months. The purpose of the Taskforce is to co-ordinate for maximum impact three strands of work currently undertaken to tackle identity crime: disruption, enforcement and awareness.

The Taskforce is overseeing the delivery of five key objectives agreed by Ministers:

- Improving intelligence about the scale and methods of operation of ID fraudsters, through a strategic threat assessment;
- Tackling the use of forged identity documents;
- Tackling the misuse of genuinely obtained identity documents;
- Improving the international effort to deal with ID crime; and
- Helping the public through improved communication on how ID crimes are perpetrated.

Intelligence

88. A number of agencies across Government deal with crime committed online, and we will work to ensure that all relevant intelligence is shared between groups, so that information can be aggregated and the major crime groups targeted. As part

of considering what the response to recording financial cyber crime should be, we will ensure that the need to collect information in a form that is useful to all law enforcement agencies is considered. Once the information has been gathered and analysed, it will be fed out to law enforcement agencies for further action, both in the UK and internationally.

- **We will ensure that information gathered through the different reporting centres is shared across law enforcement, as appropriate, and fed to awareness and education programmes.**

Internet Watch Foundation (IWF)

89. In the UK the internet industry themselves have been very successful in tackling certain types of online crime themselves, and support the work of the IWF.

IWF

The IWF was set up in 1996 by the UK internet industry as the UK Hotline for reporting child sexual abuse content hosted worldwide and criminally obscene and incitement to racial hatred content hosted in the UK.

The Government fully supports the work of the IWF, and is grateful to industry for their continued financial support for it.

In particular, the IWF has helped to make the UK a very difficult place from which to operate child sexual abuse websites. Less than 1% of the sites containing illegal images are hosted in the UK, as a result of the work of the IWF, law enforcement and industry.

5.2.2 Law enforcement response

90. The Home Office has the responsibility to provide the law enforcement response to cyber crime, through the provision of adequate police and other units to tackle the problem and ensure that the perpetrators of these crimes are brought to justice.

91. The Home Office has created a number of specialist units to help tackle cyber crime and protect the public. We believe that the creation of specialist units, such as CEOP, is the right approach, as it allows for the development of expertise in highly complex areas. This approach allows a flexibility of response, and an ability to understand the key drivers and criminal behaviours as well as the characteristics of victims who may be vulnerable to the crimes. As there are many types of crime committed on the internet, so across Government a number of specialist responses have grown up to meet them:

- The Home Office supports the safety of the citizen through the provision of law enforcement units to tackle online crime,
- The National Fraud Authority, an executive agency of the Attorney General's office, has launched Action Fraud.
- The Department of Health supports the work to tackle the sale of counterfeit drugs online, through the Medicines and Healthcare products Regulatory Agency.
- The Department for Business, Innovation & Skills is responsible for intellectual property policy and the Department for Culture, Media and Sport lead on on-line copyright protection in relation to the 2012 Olympics
- HMRC has a bespoke investigation capability to address fiscal fraud, including online attacks made against their tax regimes. HMRC are members of the ACPO e-crime group and support the work of the PCeU

92. The 2009 Consumer White Paper also announced the creation of an internet enforcement team to tackle ecrimes against consumers. This is being set up across the UK through Trading Standards and Regional Scambuster teams. They will also work closely with the PeCU and their Scottish equivalent. Developing this, the OFT is putting together a national e-consumer protection strategy by the end of 2010, to enable all relevant agencies in the consumer protection landscape to work together even more effectively, ensuring lack of duplication and better coordination of e-protection activities, including intelligence gathering, e-enforcement and other consumer protection tools.

93. The UK needs to have a law enforcement response that is capable of dealing with these issues, and has access to the right level of tools and support. The Home Office has recognised this, and has created the Police Central e-crime Unit (PCeU) to lead the police response within the UK, and the e-crime unit of the Serious Organised Crime Agency (SOCA) to work internationally. The ACPO e-crime strategy, published in 2009 set out the work of the PCeU in delivering an operational response to the most serious of e-crime incidents, the engagement with industry through the virtual task force and the establishment of the ACPO committee which consists of 9 strands of activity focused on improving law enforcements response to cyber crime.

94. The strands each led by ACPO representatives or equivalent are:

- Central PCeU structure and capability
- Olympics
- Training and recruitment
- Regional e-crime capability
- Forensics
- Legal
- Prevention
- Increasing knowledge of serious organised crime
- Research and Development

95. Law enforcement resources in this highly technical area are limited, and to address this the PCeU are progressing opportunities to brigade resources, intelligence and expertise by promoting the need for forces to establish regional capability. The Home Office fully supports this work, and recognises the efforts made by the Police Service and SOCA to tackle cyber crime. Other Departments, such as HMRC, also have specialist units dealing with fraud in their particular areas.

PceU

The Government and the Metropolitan Police Service (MPS) jointly fund the Police Central e-crime Unit (PCeU). The PCeU acts as the central unit for UK policing on promotion of standards for training, procedure and response to e-crime, and has brought together forces, the NPIA and other groups to develop training and to coordinate activity to build up the skill levels within policing.

The PCeU is working with Action Fraud and the City of London Police to develop a response to electronic fraud reported to the Action Fraud service and passed to the National Fraud Intelligence Bureau (NFIB). As the NFRC develops, protocols will be put in place that will set out the way that the PCeU will support the NFRC. The Unit works with SOCA, ACPO and ACPO(S) representatives, HMRC, the Crown Prosecution Service (CPS), CEOP and the NPIA, through the ACPO e-crime Committee.

SOCA

The Serious Organised Crime Agency (SOCA) is an intelligence-led law enforcement agency with harm reduction responsibilities. Harm in this context is the damage caused to individuals, communities, society, and the UK as a whole by serious organised crime.

SOCA assumed its full functions on 1 April 2006.

The mandate of SOCA's e-Crime Unit is to reduce the harm caused to the UK by online organised crime and is resourced to address the threat of technology enabled organised crime, and in particular to degrade criminal capability to use the Internet and IT networks as an operational enabler or means of influence. Additionally to use the Internet to obtain information on serious organised crime to improve understanding of how those involved operate and to use the Internet as a tool to assist in disrupting criminal activities.

The Unit has access to the wider operational capabilities of SOCA both within the UK and in nearly forty other countries worldwide.

Child Protection/CEOP

CEOP was created in April 2006, and was set up because the UK needed a national response to dealing with an issue which is not geographically based. Having a national centre with dedicated resources was seen as a way to move forward more effectively.

CEOP delivers a holistic, multi-agency but child-focussed response to the threat posed by child sexual offenders in the new, converged environment. One of its most important functions is to act as the UK single point of contact for international law enforcement activity, as well as a reporting centre for children, adults and the industry who wish to report grooming or other threats made against young people online. The information and intelligence gathered is used to tackle the perpetrators and develop harm reduction measures, which includes educational products for children, young people and their parents/carers, as well as those professionals who work with them. In addition, it also delivers a comprehensive set of training services covering a range of issues relating to offenders and young people at risk and includes an academically recognised professional qualification.

CEOP has had considerable success in tracking down those who would seek to harm children, those who provide or sell illegal images of child sexual abuse, and rescuing children from harm. Since it was created, and as of March 2009, CEOP has

- Rescued more than 500 children
- Arrested or supplied information leading to the arrest of 714 individuals
- Disrupted 166 sex offender networks.

CEOP runs the "Most Wanted" website for child sex offenders who have absconded. They have had considerable success in tracing such absconders through their own work and through reports made to CEOP by the public. CEOP has led the growth of the Virtual Global Taskforce (VGT), which is made up of representatives from law enforcement from 6 leading countries around the world, as well as Interpol which represents the interests of 187 other countries. This group helps to tackle international online networks of child sexual abusers, as well as the issue of travelling sexual offenders.

96. The Government recognised the need to ensure that children had a place to turn to if they felt threatened on the internet, both to report threats, and to be able to find information on how to keep themselves safe.

MHRA

In the UK, strict legal controls apply to the retail sale and supply of medicines and these controls apply equally to medicines sold via the Internet.

The MHRA is responsible for the regulation and control of medicines on the UK market. MHRA takes the view that on-line supply of medicines is acceptable, provided these legal controls are met, but warns patients that products obtained in this way cannot be guaranteed as safe.

Medicines legislation does not prohibit the remote prescribing of prescription only medicines by a prescriber. These prescriptions must meet the usual requirements set down in medicines legislation. The General Medical Council has issued guidance to doctors on good practice concerning prescribing where they are not in face-to-face contact with the patient.

MHRA Response

MHRA routinely monitor medicines being offered for sale on the Internet. Websites identified as dealing in medicines illegally are investigated dealt with robustly. Enforcement action can be taken against wrong-doing based in the UK but considerable illegal activity takes place outside UK control. Some websites are deliberately hosted in countries where there is little or no regulation. “Rogue” websites identified overseas are referred to the relevant country for any appropriate action. The MHRA works closely with EU and other international regulatory authorities to ensure that, wherever possible, offending websites are amended to reflect the law. The MHRA recognises that a multi-lateral approach to Internet issues will be most effective and participates in cross-Government and International groups set up to explore how best to combat Internet issues and exchange intelligence.

Prescription medicines purchased from overseas internet websites cannot be guaranteed for their safety, quality and efficacy. In order to communicate the potential risks involved, the MHRA is involved in several initiatives to better inform consumers and potential customers about potential risks involved in buying medicines from Internet sites, both by MHRA acting as regulator, or in conjunction with relevant organizations such as the Royal Pharmaceutical Society (RPSGB). These include national advertising campaigns with industry and patient groups to raise awareness and targeting vulnerable groups through specific articles in a variety of publications, including slimming and men’s health magazines. Internet auction sites are also used as a means of communicating perceived risks.

The MHRA works with those Internet Service Providers (ISPs) identified as hosting websites trading illegally, using their facility, with a view to having the site withdrawn. Additionally, the MHRA conduct “Internet Days of Action”, where operators of “suspect” websites across the UK are targeted, products seized, websites closed and individuals prosecuted.

The Royal Pharmaceutical Society has recently launched the Internet Pharmacy Logo which will help members of the public identify legitimate on-line pharmacies.

Information on buying medicines on line is also available through the MHRA website; Buying medicines over the Internet : MHRA

What the Home Office will do

- **We will continue to support these specialist units, and will work with the ACPO e-crime Committee to ensure that there is a police and law enforcement agency response to cyber crime.**

5.2.3 Technical development for law enforcement

97. Cyber crime is committed using communications between networked devices, with those communications conveyed in various applications such as e-mail or malware. The ability to trace offenders and victims, and to investigate and gather evidence of cyber crimes can depend on the ability to recover and analyse network data and, once an offence has been detected and reported, the ability to research and analyse historic data.

98. In a changing and increasingly complex communications environment investigators need to be able to continue to investigate communications data, and to be able to acquire and analyse complex network traffic data. The Home Office Communications Capabilities Directorate is leading a cross-government programme of work to ensure that investigators can continue to be able to investigate communications data to protect the public, investigate online crimes and prosecute offenders. The Directorate is working closely with the UK's law enforcement and security and intelligence agencies and with communications service providers to put in place and maintain arrangements permitted by law for the retention, retrieval and disclosure of communications data. Within the Directorate, the Interception Modernisation Programme is considering the implications for cyber crime detection of the increasing distinction between traditional networked services and newer application layer services.

5.2.4 Prosecution

99. Following the detection and investigation of cyber crimes it is important that offences are effectively prosecuted, that those involved in dealing with these cases receive appropriate training, and that the criminal justice system has knowledge of the complexities which hi tech crime cases can present and sufficient expertise to deal with them. It is also important that, as "Extending our Reach" made clear, the prosecuting authorities use all available tools to recover any assets and to limit the future activities of those responsible for the crimes.

100. In cases where there is a significant involvement of computers in the facilitation of an offence, it will usually be dealt with by a prosecutor who has undergone specialist training in this area and has experience of handling such cases. The CPS have now trained 120 high-tech crime specialist prosecutors across the regions, and over 45 cyber crime specialist caseworkers. Within the CPS further forms of continuous on the job training and development exist through a cyber crime bulletin board whereby prosecutors are informed of developments in cases with a hi-tech element by dissemination of case summaries.

What Home Office will do

- **Cyber crime is a major criminal business, and as with other forms of crime where criminals have sizeable assets, the Home Office will work with the prosecuting authorities to ensure that these can be recovered.**
- **The Home Office will also consider how other tools used to tackle offline crime, such as Serious Crime Prevention Orders, can be used in the online environment.**
- **As part of the work led by the Ministerial group to consider whether the existing legislation is adequate for tackling cyber crime, the Home Office will also consider whether the sentences for crimes committed on the internet fully reflect the seriousness of the crime, and the scale on which they are attempted or perpetrated.**

5.2.5 Consumer Protection

101. The Government has asked the Office of Fair Trading (OFT) to develop a longer term national strategy for consumer protection on the internet. The e-Consumer Protection Strategy will consider how relevant agencies can work together even more effectively, ensuring lack of duplication and better coordination of e-protection activities. The OFT will publish a public consultation document in spring 2010, where it will lay out the key challenges and options to address them. A completed e-Consumer Protection Strategy will be published by the end of 2010.

What the Government will do

- **The Government will continue to provide information on the rights of consumers purchasing goods online through the Office of Fair Trading and through Consumer Direct.**

5.3 Raising public confidence

102. The Digital Britain Report made clear that one of the issues that prevents individuals and businesses from making greater use of the internet is a lack of confidence in the safety and security of the technology and services.

103. We believe that where Government can best add value is where it can help in ensuring that the public has access to information on how to protect themselves, and that business and the internet industry are encouraged to take action to help protect consumers.

104. The key aim of cyber crime prevention is to ensure that information and education is made available to the public and businesses to help them keep themselves safe. As with the work to directly tackle crimes through law enforcement activity, there is a need to be able to provide safety information that is specific to a particular area or group, but also general messages that apply to safety as a whole. This includes working with internet service providers to develop an internet culture that stamps out unacceptable behaviour online, such as abuse, stalking and harassment.

105. We have taken the lead in bringing together different groups to provide education and develop a preventative response, which can include the relevant industry for a particular area, charities and the third sector, as well as civil society. We will continue to develop this approach.

5.3.1 Financial and technical safety information

106. The best way to stop cyber crime is to prevent it happening in the first place, and as part of that the public and business needs to be provided with accurate, relevant information on how to keep themselves safe online and to secure their devices and data. The Government is strongly supportive of growing the use of the internet, and recognises the need to provide adequate and accurate information on the risks to consumers should they decide to use internet services. The primary purpose of any of our safety information is to ensure that the public and business has accurate information to help them protect themselves. This applies whether the issues are relating to fraud, to protecting children, or to using standard services on the internet.

107. Individuals can protect themselves by controlling the amount of personal data they make available on the internet. However, the use of privacy enhancing technology in systems can also enhance an individual's privacy, help reduce the risks of privacy breaches and the significant costs associated with them and build trust between customers and clients.

108. A number of Government departments provide safety information relating to the internet, as part of the provision of their services, and many of these are particular to the problems faced by those departments. Across Government we will continue to maintain these sites, as appropriate, as they provide specific information to allow the public to protect themselves or have access to safety information.

109. Since 2005, the Government has sponsored Get Safe Online (GSO), in partnership with industry, to act as the information point for general online security.

GET SAFE ONLINE

The Government and business set up the Get Safe Online website in 2005, to provide information to the public and businesses on how to protect themselves online. The Get Safe Online websites provide information to the public on how to implement anti-virus software, content filtering and firewalls. This is written in plain language, and is aimed at providing practical and independent advice for the public and businesses.

110. The Home Office and other Government departments will continue to support Get Safe Online as the main provider of general information, and we will enhance the work it does, and the information it provides, by providing intelligence on threats gathered through the National Fraud Intelligence Bureau. GSO will make the information from this intelligence available to the public, to keep them informed of the latest scams and internet threats.

What the Home Office will do

- **We will work with Get Safe Online and business to raise awareness of the issues, and will consider how best to publicise the safety message through that website.**
- **We will encourage Get Safe Online to link with Consumer Direct and Direct. gov to ensure that this is available to the public**
- **We will seek to engage a wider part of the user community, particularly small businesses, to ensure that they are able to keep themselves safe online.**
- **We will work with industry to ensure that Get Safe Online contains clear guidance on where to go to get further information on specific topics, and where to get practical solutions, such as anti-virus software and updates for existing software.**
- **We will work to make sure that Government webpages contain a link to Get Safe Online, and that Get Safe Online also shows links to other Government activity, such as CEOP, to protect children. We will identify how the GSO message can be communicated effectively.**

5.3.2 Child Safety and Education

111. The internet and associated technologies are used by children to communicate, have fun and do research. Schools are encouraging the use of the internet, and as part of that work they are devoting time to providing children with the right information to keep themselves safe. Across the UK, a significant amount of work is being done to ensure that children are taught about keeping themselves safe online, including

- The Welsh Assembly Government published guidance about online safety for schools in October 2008.
- The Scottish Government launched 'Glow', the Scottish schools' intranet which provides pupils and teachers with a safe and secure online facility allowing for joined-up networking. By April 2009 over 420,000 pupils and staff had been issued with Glow accounts.
- After the Rose Review21 was published in May 2009, online safety was included in the revised Primary School Curriculum in England. In Wales the revised National Curriculum, introduced in September 2008, makes strong reference to online safety. Introduced in September 2009, the new curriculum in Northern Ireland includes online safety.

- School inspectors will now assess how well online safety is taught in primary schools in all parts of the UK.
- A new e-safety resource for primary teachers produced by Childnet, 'Know IT All for Primary Teachers' was launched by Professor Tanya Byron in June 2009. It has been sent out to every primary school in England.
- The Training and Development Agency for Schools (TDA) has revised its annual survey for newly qualified teachers in England to include questions on online safety. This will measure how teachers' knowledge is improving.
- The TDA has included elements on online safety in its ICT skills test for newly qualified teachers. This means that all newly qualified teachers have to demonstrate understanding of the issues and ways to stay safe online
- The OFT provides the Skilled-to-go support tools for teaching children their online rights

CEOP – THINK U KNOW PROGRAMME

Since 2006, CEOP has overseen the delivery of the ThinkuKnow education and public awareness internet safety programme to nearly 5 million UK children aged between 5 and 16 years. It consists of offline resources for delivery into schools and other youth environments by specially trained and CRB checked local professionals, including teachers, police and child protection workers. This is complemented and supported by an online resource which provides the public with a "one stop shop" approach to child internet safety where children, young people and those who care for them can access a range of help and advice from specialist services in areas such as bullying, hacking and mobile phone issues, as well as the ability to report directly to CEOP on concerns over child sexual abuse or exploitation. It also allows professionals to register for training to deliver ThinkuKnow, download the range of resource available for all target groups and receive up to date information on trends, themes and patterns. The resources and updates are informed by CEOP's intelligence and operational work. The government will continue to support CEOP's delivery of this key crime prevention and reduction programme aimed at children and young people and those who look after them.

5.4 Working with the private sector

5.4.1 Financial Crime

112. In the "Extending our Reach" report, the Home Office emphasised the need for all sectors to work together to tackle cyber crime, and to make internet crime unattractive to criminals. The House of Lords Science and Technology Committee report into Personal Internet Safety also recognised that no single sector can do all of the work to prevent crime on the internet. Law enforcement can do a significant amount, but the big gains in preventing crime will come from the use of multiple layers of defence and disruption, as well as education.

113. There are a number of reasons why we need to bring industry, government and law enforcement together to tackle cyber crime. The internet infrastructure is owned by the private sector, and the business community operates services over it. The industry is the repository of technical skills and attack trend information, and has the knowledge to help deliver a safer internet. In return, industry needs to have access to information and intelligence that will be developed through the National Fraud Intelligence Bureau (NFIB), to both protect itself and to develop defences.

114. To tackle cyber crime effectively, we need to understand both:

- The changing legitimate uses of these technologies (to identify the potential crime risks and the use criminals will make of them); and
- What crimes are being committed using or facilitated by these technologies and the impact they have.

115. The nature of the technology is that these change quickly (much more quickly than in more traditional sectors) as take-up of a technology changes or as a new technology is introduced. New crime patterns develop and proliferate quickly and we need to track these to ensure we can respond effectively to reduce their impact and prosecute offenders.

116. We believe that it is more effective to have specialist groups working to tackle specific areas, than to have a single organisation dealing with industry liaison. Groups such as the UK Council for Child Internet Safety have been very successful in developing strategies between the industry and government, and will ensure that learning and technical tools are shared.

E-crime Reduction Partnership

The Digital Britain report considered how the UK should respond to the growth of the digital economy, and how best to ensure that the country takes advantage of the opportunities provided by the digital world.

The report proposed that there should be more coordination of initiatives to tackle crime on the internet, and promote safety, and that an E-crime Reduction Partnership and Security Initiative, bringing together industry, law enforcement and parliamentarians, should be set up to lead this work. This grouping will bring together knowledgeable and committed representatives of industry, government and law enforcement, and should not be a large body but one where there can be a frank sharing of experience and willingness to agree on actions.

There are a number of areas where the E-crime Reduction Partnership will consider working, such as how to incentivise good security, how information on malicious websites can be shared, and what practical steps can be taken by industry working together to tackle cyber crime. Through the E-crime Reduction Partnership we will work with industry and business to develop safe products and to tackle issues such as spam and phishing attacks.

5.4.2 Child Internet Safety

117. The Government has taken the online protection of children very seriously, and has set up the UK Council for Child Internet Safety (UKCCIS) as a forum that enables everybody involved with online child safety – including government, industry, law enforcement, and the third sector – to work together and contribute jointly to the development and delivery of a strategy for child internet safety. UKCCIS has recently published "Click Clever, Click Safe"[23], the first UK internet safety strategy, which sets out the work that members of the Council will do to help keep children safe online.

118. The Government has worked with the internet industry to ensure that consumers cannot access illegal images of child sexual abuse, as defined on the Internet Watch Foundation list. The response from the internet industry has been significant, and we believe that 98.6% of consumer broadband lines are now covered by blocking based on that list. We will continue to work with ISPs to tackle this problem.

[23] Click Clever, Click Safe – clickcleverclicksafe.direct.gov.uk

UKCCIS STRATEGY

UKCCIS has recently launched the first UK child internet safety strategy "Click Clever, Click Safe" which sets out what the Government, industry and charities are collectively doing to keep children safe online. This is the first strategy of this kind produced anywhere in the world.

The Council has also launched the first stage of the "Click Clever Click Safe" campaign, with the online version of the Green Cross Code: "Zip it, Block it, Flag it". We want to see the digital code become as familiar as 'Stop, Look, Listen.'. Additionally, for the first time, key players from industry, charities and Government will be independently reviewed against standards to keep children and young people safe online.

5.5 International working

119. Cyber crime is an international problem, with the UK public, business and government being targeted by criminals outside the UK as well as within. National Governments cannot solve this problem alone, and while Governments can regulate within their own borders, they cannot regulate externally. There is a need to ensure that countries are able to support the fight against cyber crime, and that there are international standards for operational work. International co-operation is most easily facilitated where different legislative systems have common offences which allow for the investigation and prosecution of an offence regardless of the jurisdiction it may have been committed in or wherever the evidence of an offence may be located. Common offences also allow for the possibility of extradition by providing for dual criminality requirements. One commonly experienced difficulty is in making requests for data to other law enforcement agencies or data owners outside the UK. This process varies in its success, speed and complexity dependent on the country, or more frequently the company concerned. Many exchanges are facilitated by personal contacts or the reputation of the organisation or individual requesting the data. The success of a request is not always dependent on whether a country has signed an international Convention or agreement which indicates it will provide the co-operation sought.

120. Criminals are increasingly utilising a variety of technical communication methods for the facilitation of offences and also for the purpose of criminal communications. Tracing the source of communications is essential to discovering offender identity and as intelligence. These communications may be made via ISPs in any part of the world. If any jurisdiction makes it more difficult for law enforcement to obtain details of information, such as subscriber information, then investigations and possible prosecutions will potentially falter.

121. The UK works closely with other countries, including through the G8, EU and the Council of Europe to set these standards. At policy level, we will continue to work with national and international institutions to ensure that there is a standard approach to tackling cybercrime. The Ministerial Committee will oversee a cross-Government approach to international work at a policy level. We will complete the ratification of the Council of Europe Cybercrime Convention, which is the standard international agreement to tackle cyber crime. We will continue to work with Governments to help them develop their response to Cybercrime.

122. In the arena of child protection international law enforcement cooperation has been successfully established, despite some of the differences in law and approach between countries. The VGT, of which CEOP is a founder member, is a good example of a light touch operational approach which has contributed to successful investigations into international online child sexual offenders networks and action to tackle those that travel to abuse children and young people. The Government will continue to support CEOP in promoting membership of the VGT amongst the wider international community.

Internet Governance Forum

123. The UK's policy has been to encourage international cooperation on governance of the internet rather than placing it under the control of a centralised supra-national agency. Through the creation of the UK IGF we have tried to show the benefits of a less formal approach which harnesses dynamic coalitions and enhanced cooperation between Government, Parliamentarians, Industry and Civil Society. That approach is now being applied increasingly widely in the creation of new national and regional IGF's in various parts of the world. The UK's belief is that we can only sustain a high level of international support for this flexible approach if it can be demonstrated that the IGF process can tackle the big issues such as criminal and antisocial activity on the internet.

ICANN/ITU

124. The UK will work with the International Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunication Union (ITU) to ensure that the work of those organisations takes into account the need to tackle crimes committed across national and international networks.

Work of the Attorneys-General

125. The Attorneys General of the UK, Australia, Canada, New Zealand and the United States of America have recognised the scope for all five countries to work together more closely to promote cooperation on legal frameworks at the international level and agreed to work jointly on international challenges such as organized crime and cyber crime, and will meet annually to discuss these issues.

Global Posecutors E-crime Network (GPEN)

126. The CPS and the International Association of Prosecutors [IAP] have established a global network of specialists called the Global Prosecutors E-Crime Network (GPEN). GPEN not only encourages enhanced international cooperation in the e-crime arena; but it enables all jurisdictions to develop a co-ordinated approach for dealing with e-crime that supports effective prosecutions and promotes the principles of the Council of Europe Cybercrime Convention.

What we will do:

- **We will consider, with international partners, whether the existing arrangements for securing data for use as evidence are quick enough.**
- **At a law enforcement level, we will continue to support the work done by CEOP, SOCA, HMRC, the OFT and the PCeU in developing international working practices and through the 24/7 network operated for the UK by SOCA**
- **Through international negotiation we will seek further changes to ensure that unacceptable, damaging and harmful conduct against computers and committed through computers is effectively criminalised, that international co-operation is readily facilitated and that investigatory powers are effective to assist in investigating computer crimes.**
- **We will seek to improve the standards of international legislation cyber crimes, international co-operation and associated investigatory powers through the UK's participation in international fora, and overseas influence and assistance.**
- **The Government will continue to support CEOP in promoting membership of the VGT amongst the wider international community**

6 What we will do

Number	Action	Owner	Implementation Date
1	Ensure consistency with the maturing work on the National Security Strategy and the UK Cyber Security Strategy	Home Office	September 2010
2	Create a Ministerial Committee for cyber crime, led by ministers from the Home Office and BIS, who will work with ministers from other Government departments, to lead the cross-Government effort to tackle cyber crime.	Home Office / BIS	July 2010
3	We will review the current legislation with the aim of future-proofing it and ensuring the continued relevance of it to the fast-moving world of the internet particularly with regard to the ability to commit crimes on an industrial scale. We will ensure that legislation across relevant departments considers the impact of cyber crime.	Home Office	September 2010
4	We will learn from the experience of developing Action Fraud (the National Fraud Reporting Centre (NFRC)) and the Consumer Direct online reporting facility, as well as that of CEOP, and consider how best to receive and record reports of crime and attempted crime not only of fraud on the internet, but also for other internet crimes where there is no existing reporting centre.	Home Office / AGO	September 2010
5	We will include questions relating to cyber crime in the British Crime Survey, to understand what the impact of these crimes is relation to other crime, and to identify changes in levels of confidence	Home Office	September 2010
6	We will continue to support CEOP, the Medicines and Healthcare products Regulatory Agency (MHRA) and other agencies which act as reporting centres for specific types of online offences	Home Office / DH	Ongoing
7	We will work to develop a classification scheme for recording cyber crime, in conjunction with the law enforcement agencies and with the internet industry and business.	Home Office / AGO	December 2010
8	We will ensure that information gathered through the different reporting centres is shared across law enforcement, as appropriate, and fed to awareness and education programmes.	Home Office	December 2010
9	The Government will continue to support these specialist units, and will work with the ACPO e-crime Committee to ensure that there is a police and law enforcement agency response to financial crime.	Owning departments	Ongoing
10	Cyber crime is a major criminal business, and as with other forms of crime where criminals have sizeable assets, we will work with the prosecuting authorities to ensure that we are in a position to recover these.	Home Office / CPS	October 2010
11	We will consider how other tools used to tackle offline crime, such as Serious Crime Prevention Orders, can be used in the online environment.	Home Office / CPS	October 2010

Number	Action	Owner	Implementation Date
12	As part of the work led by the Ministerial group to consider whether the existing legislation is adequate for tackling cyber crime, we will also consider whether the sentences for crimes committed on the internet fully reflect the seriousness of the crime, and the scale on which they are attempted or perpetrated.	HO / BIS / CPS / MoJ	October 2010
13	We will continue to provide information on the rights of consumers purchasing goods online through the Office of Fair Trading and through Consumer Direct	BIS / OFT	Ongoing
14	We will work with Get Safe Online and business to raise awareness of the issues, and will consider how best to publicise the safety message through that website	Cabinet Office / Home Office / BIS	November 2010
15	We will encourage Get Safe Online to link with Consumer Direct and Direct.gov to ensure that this is available to the public	Cabinet Office / Home Office / BIS	November 2010
16	We will seek to engage a wider part of the user community, particularly small businesses, to ensure that they are able to keep themselves safe online.	Cabinet Office / Home Office / BIS	November 2010
17	We will work with industry to ensure that GSO contains clear guidance on where to go to get further information on specific topics, and where to get practical solutions, such as anti-virus software and updates for existing software	Cabinet Office / Home Office / BIS	October 2010
18	We will work to make sure that Government webpages contain a link to Get Safe Online, and that GSO also shows links to other Government activity, such as CEOP, to protect children. We will identify how the GSO message can be communicated effectively	Cabinet Office / Home Office / BIS	October 2010
19	We will consider, with international partners, whether the existing arrangements for securing data for use as evidence is quick enough	Home Office	March 2011
20	At a law enforcement level, we will continue to support the work done by CEOP, SOCA, HMRC, the OFT and the PCeU in developing international working practices and through the 24/7 network operated for the UK by SOCA	Home Office	Ongoing
21	Through international negotiation we will seek to further changes to ensure that unacceptable, damaging and harmful conduct against computers and committed through computers is effectively criminalised, that international co-operation is readily facilitated and that investigatory powers are effective to assist in investigating computer crimes.	Home Office / AGO / BIS	March 2011
22	We will seek to improve the standards of international legislation pertaining to e-crimes, international co-operation and associated investigatory powers through the UK's participation in international fora, and overseas influence and assistance.	Home Office / AGO	March 2011
23	**The Government will continue to support CEOP in promoting membership of the VGT amongst the wider international community**	**Home Office**	**March 2011**

7 Glossary

Advanced fee fraud	Fraud where a person is targeted with the promise of large sums of money if they provide relatively small payments up front. These include lottery scams and 419 frauds.
Botnets (robotic networks)	A collection of computers infected with malicious bots which can be remotely controlled by the attacker (the owner of the botnet).
Bots	A computer that has been infected with a piece of malware such that it carries out certain actions upon receiving a command – normally used without the knowledge or consent of the owner.
Denial of Service attacks	A malicious attempt to disrupt the operation of a specific computer, network, web site or other entity in cyber space.
Distributed Denial of Service attacks	Using multiple attacking computers to achieve the same effect as a Denial of Service attack.
Hacking	A common term usually used to describe unauthorised entry on to a computer, network or website.
Malware	Malicious software including computer viruses, worms, trojans and spyware.
Peer-to-peer (P2P)	Technology used to share files, such as music or images, between users.
Phishing	A process whereby social engineering is used to trick an organisation or customer in to imparting confidential information, generally by persuading a victim to perform a series of actions which unwittingly provides the attacker with access
Social engineering	The use of social factors to persuade people to reveal information or give money
Spam	Bulk sending of e-mails to users

8 Who does what?

ACPO	Association of Chief Police Officers. The ACPO e-crime Committee issued the ACPO e-crime strategy in July 2009
Action Fraud	Action Fraud is the UK's national fraud reporting centre, where the public can report fraud, which will be fed into the National Fraud Intelligence Bureau
BIS	The Department for Business, Innovation and Skills (BIS) supports UK business and industry, and acts as the Government lead in ensuring that these groups are represented in programmes to tackle crime.
CEOP	The Child Exploitation and Online Protection (CEOP) Centre is is dedicated to eradicating the sexual abuse of children. It is part of UK law enforcement and safeguarding children and tracking and bringing offenders to account either directly or in partnership with local and international forces.
CSOC	The Cyber Security Operations Centre (CSOC) will bring together existing functions: to actively monitor the health of cyber space and co-ordinate incident response; to enable better understanding of attacks against UK networks and users; and to provide better advice and information about the risks to business and the public
DCSF	The Department for Children, Schools and Families is responsible, with the Home Office, for the UK Council for Child Internet Safety, which brings Government, industry, law enforcement and the third sector together to tackle threats to children online.
Get Safe Online	A public-private organisation that provides information on cyber crime threats and how members of the public and business can protect themselves.
Home Office	The Home Office is responsible for provision of law enforcement response to cyber crime, and owns the Government's cyber crime strategy
ICANN	The Internet Corporation for Assigned Names and Numbers. To reach another person on the Internet you have to type an address into your computer – a name or a number. That address has to be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination it would not be possible to have a global internet.
ITU	The International Telecommunications Union was created in 1865 to provide standards for connecting telephone systems internationally.
IWF	The Internet Watch Foundation was established in 1996 by the internet industry to provide the UK internet Hotline for the public and IT professionals to report criminal online content in a secure and confidential way.
MHRA	The Medicines and Healthcare products Regulatory Agency (MHRA) is the government agency responsible for ensuring that medicines and medical devices work, and are acceptably safe. The MHRA tackles illegal sales of drugs online.
NFIB	The National Fraud Intelligence Bureau takes the reports made to Action Fraud and creates intelligence packages for law enforcement.
OCS	The Office of Cyber Security provides strategic leadership for and coherence across Government on cyber issues. The OCS will establish and oversee a cross-government programme to address priority areas in pursuit of the UK's strategic cyber security objectives

OFT	The Office of Fair Trading aims to protect consumers by equipping consumers and businesses with the knowledge they need to protect themselves against unlawful practice, both online and offline.
PCeU	The Police Central e-crime Unit was set up to create a national centre of excellence to combat e-crime in England, Wales and Northern Ireland. It has the aim of improving the police response to victims of e-crime by developing the capability of the Police Service across England, Wales and Northern Ireland, co-ordinating the law enforcement approach to all types of e-crime, and providing a national investigative capability for the most serious e-crime incidents.
SOCA	The Serious Organised Crime Agency contains the SOCA e-crime unit responsible for tackling serious organised crime on the internet. SOCA e-crime also acts as the UK 24/7 network liaison point for other countries.
UKCCIS	The UK Council for Child Internet Safety brings together organisations from industry, charities and the public sector to work with the Government to deliver the recommendations from Dr Tanya Byron's report – Safer Children in a Digital World

9 Bibliography

National Security Strategy
http://www.cabinetoffice.gov.uk/reports/national_security.aspx

Cyber Security Strategy
http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx

Digital Britain Report
http://www.culture.gov.uk/images/publications/digitalbritain-finalreport-jun09.pdf

Extending our Reach
http://www.homeoffice.gov.uk/documents/extending-our-reach/index.html

ACPO e-crime strategy
http://www.acpo.police.uk/asp/policies/data/Ecrime%20Strategy%20Website%20Version.pdf

Safer Children in a Digital World
http://publications.dcsf.gov.uk/eOrderingDownload/DCSF-00334-2008.pdf

UKCCIS Strategy
http://www.dcsf.gov.uk/ukccis/

House of Lords Science & Technology Committee Report into Personal Internet Security
http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf

Council of Europe Cybercrime Convention
http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm

CONTEST Strategy
http://security.homeoffice.gov.uk/news-publications/publication-search/contest/contest-strategy/contest-strategy2009.html

Findings from consumer surveys on Internet Shopping
http://www.oft.gov.uk/shared_oft/reports/Evaluating-OFTs-work/oft1079.pdf

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Parliamentary Bookshop
12 Bridge Street, Parliament Square
London SW1A 2JX
Telephone orders/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: http://www.bookshop.parliament.uk

TSO@Blackwell and other Accredited Agents

Customers can also order publications from:
TSO Ireland
16 Arthur Street, Belfast BT1 4GD
Tel 028 9023 8451 Fax 028 9023 5401

ISBN 978-0-10-178422-1