CYBERCRIME:

What is it and what do we do about it?
- Mapping out and policing cybercrimes

Michael Molenda - http://www.flickr.com/photos/72388119@N00/3164460404/

Durham University

Professor David S. Wall,
Criminology, SASS,
Durham University, UK
0191 334 6983 d.s.wall@durham.ac.uk

OUTLINE : The objective of this talk is to explore the way that networked technology has transformed criminal behaviour.

Cybercrimes are informational, networked and global which and highly disorganised when compared to the organisation of more 'traditional' crimes. But cybercrimes also display some new characteristics including new forms of organisation which possess a different logic.

PART ONE – What is cybercrime?

1 The Internet and the information society

2 How has the internet transformed criminal behaviour?

3 Mapping out the contours of cybercrime/ Changes in the scope of criminal opportunity

4 The reorganisation of criminal labour by networked technology

PART TWO – What do we do about it?

5 What are the criminal justice challenges?

6 Who is Policing Cybercrime and how?

7 UK CyberSecurity and Cybercrime Strategy

PART 1
What is Cybercrime?

http://www.skinwalkerranch.org/blog/uploads/alien_computer.jpg

Durham University

THE RHETORIC – Cybercrime wave of 3m threats per year

THE REALITY - 300 CMA 1990 prosecutions in 20 years

Protect your business from the cybercrime wave

Updated 4/19/2010 7:57 AM | Comments 3 | Recommend 3 E-mail | Save | Print | Reprints & Permissions | RSS

By Steve Strauss for USA TODAY

Share

Yahoo! Buzz

Add to Mixx

Facebook

Twitter

Ask an Expert
Steve Strauss

Q: Steve – I really think you should warn people about the increasing dangers coming from scam artists who are targeting small business. Our business had several thousand dollars illegally transferred out of our bank account recently and my banker says

Latest News | CNET River | Webware | Crave

Home › News › Policy, law, & crime

November 12, 2003 5:52 AM PST

Zombie machines fuel cybercrime wave

Meet A-Z: The computer hacker behind a cybercrime wave - USATODAY.com - Mozilla Firefox

http://www.usatoday.com/tech/news/computersecurity/2008-08-04-hacker-cybercrime-zeus-identity-theft_N.htm

Meet A-Z: The computer hacker behind a cybercrime wave

BBC NEWS | Technology | Cybercrime wave sweeping Britain - Mozilla Firefox

http://news.bbc.co.uk/2/hi/technology/7697704.stm

Page last updated at 00:11 GMT, Thursday, 30 October 2008

E-mail this to a friend | Printable version

Cybercrime wave sweeping Britai

Cybercrime in the UK rose by more than 9% in 2007, according to a new report.

Online identity firm Garlik's cybercrime report claims that more

Sport phishing morphs into cybercrime wave - Mozilla Firefox

http://www.networkworld.com/research/2006/052206-phishing.html?brl

Firefox prevented this site from opening a popup window.

Sport phishing morphs into cybercrime wave

Organized criminals unleash armies of botnets to steal confidential information.

By Deb Radcliff, Network World
May 22, 2006 12:06 AM ET

Share/Email | Tweet This | Comment | Print

Traditional e-mail phishing exploits are still growing in numbers, but they seem aln compared with newer, more virulent malware used by cybercrime rings that trade account information.

Fighting back

These increasingly sophisticated and organized groups are using such tricks as k loggers, browser redirectors and Trojan horses to harvest, store and sell stolen in they're using automated, untraceable armies of botnets to help.

THE RHETORIC – Hackers can destroy society

THE REALITY – The risk is different to expected - spam

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / *Weekly World News*

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told *Weekly World News*.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America's ma-

scarier," Yabenson said.

"Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

Sickos can wreak death and destruction from thousands of miles away!

Arnold Yabenson.

http://whatifoundtoday.com/hackers-can-turn-your-home-computer-into-a-bomb

Could this be more like the reality of cybercrime

spam/spamming is the distribution of unsolicited bulk emails that deliver invitations to participate in schemes to earn money; obtain free products and services; win prizes; spy upon others; obtain improvements to health or well-being, replace lost hair, increase one's sexual prowess or cure cancer. They choke up bandwidth and present risks to the recipient should they respond.

http://www.play.com/Gadgets/Gadgets/4-/11417978/Spam-Fancy-Dress-Costume/Product.html?_%24ja=tsid:11518|cat:11417978|prd:11417978

Durham University

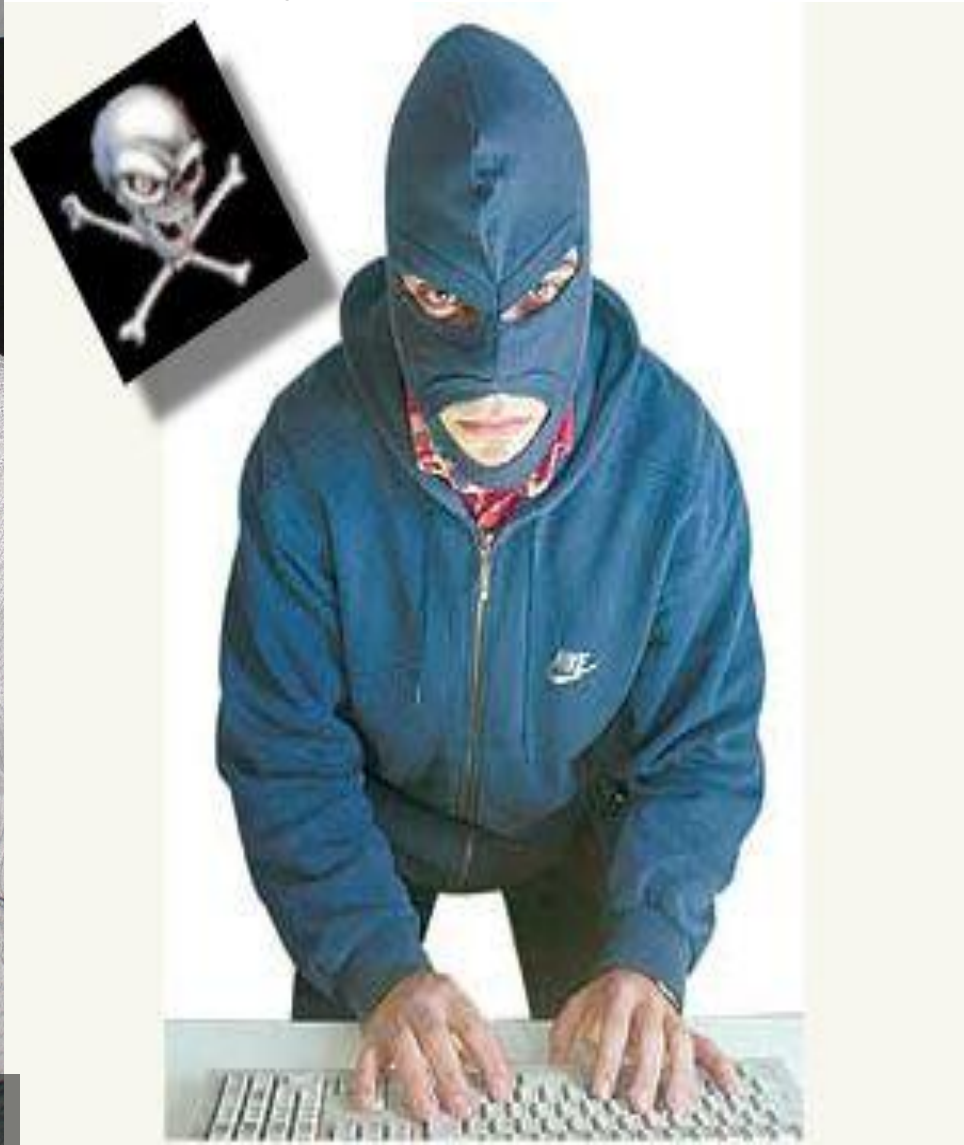
THE RHETORIC – Most of the dangerous hackers are Russian

THE REALITY – We don't really know – is it important?

What do hackers look like??

http://www.eurobsd.org/SummerCamp2003/reports/Henning/tn/evil%20russian%20hacker.JPG.html

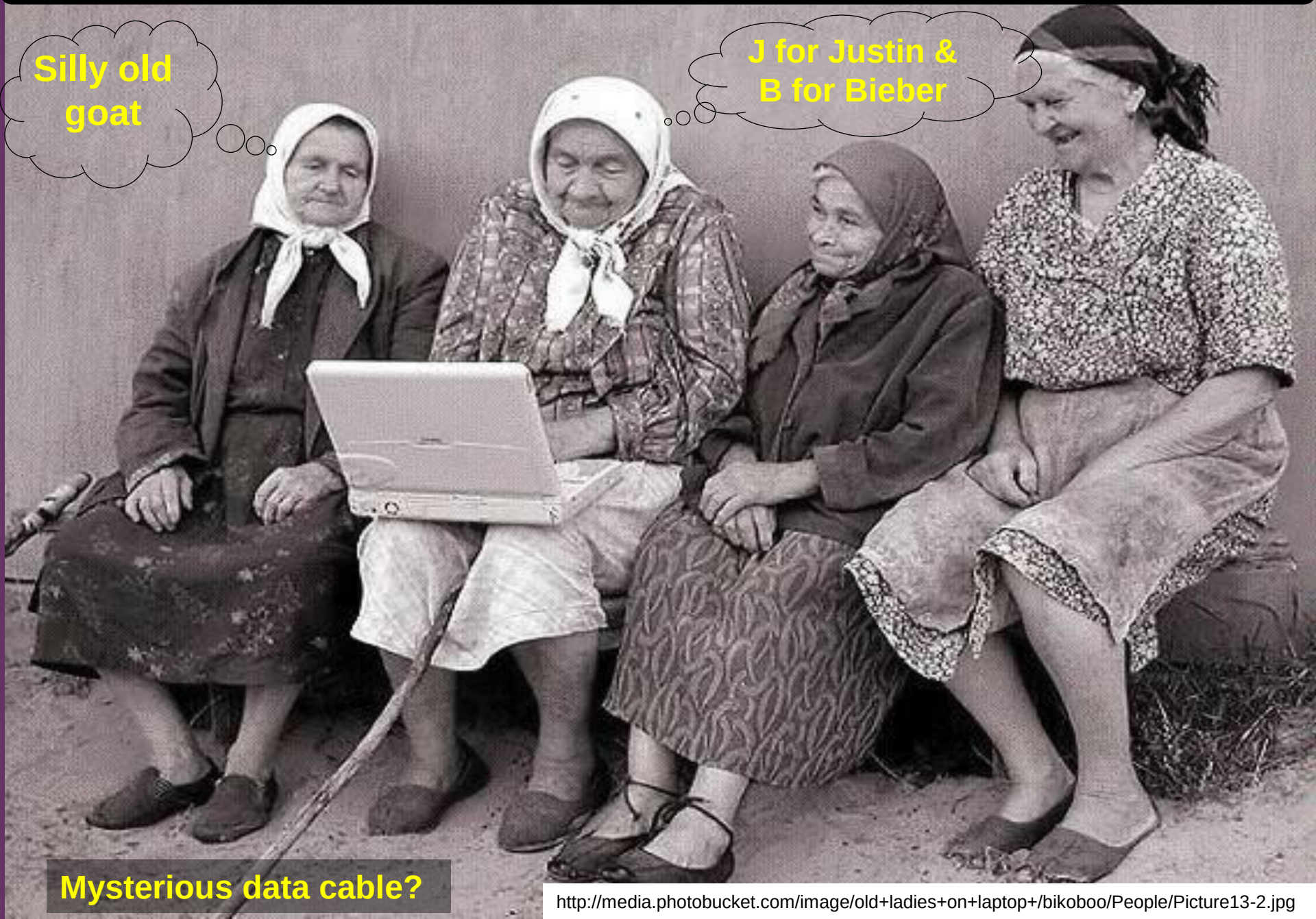
How they want us to see them



BUT DOES THE DEVIL DRIVE A LADA

OR ... DOES SHE?

You're through the firewall Doris, hack the sucker



http://media.photobucket.com/image/old+ladies+on+laptop+/bikoboo/People/Picture13-2.jpg

1:1 The Internet and the information societv - a) What is the internet?

Sir Tim Berners-Lee

- The internet is a network of networks
- Military origins then released to education & business before general use in late ‘80s
- The WWW is the combination of TCP/IP protocol (1978) - information transfer codes - plus Hypertext (HTTP, HTML, URL) (CERN 1989 - Sir Tim Berners-Lee: "I just had to take the hypertext idea and connect it to the Transmission Control Protocol and domain name system ideas and — ta-da! — the WWW”.
- What we now call the internet is really the common application of the WWW via the Graphic User Interface
- The internet represents the convergence of technologies - Bell and Babbage didn’t foresee the convergence of communications and computing technologies.
- The internet has created a virtual social space or cyber space in which we conduct business, work and leisure

1.2 How has the internet transformed social behaviour?

- **Informational exchanges**
  - **the internet is based upon intangible informational exchanges**
  - **everything leaves a data trail (disappearance of disappearance!)**
- **Globalisation and Glocalism**
  - **globalisation shapes the relationship between the global and the local (**hence the term glocalisation**)**
- **Networks**
  - **Distributed networks and grid technologies create new forms of commercial and emotional relationships between individuals. [Ideas such as Tipping Point, Wisdom of Crowds, Wikinomics]**
  - **Asymmetric not symmetric relationships-empowered single agent**
  - **Has both a Panoptic and Synoptic effect … …**

CYBERCRIMES exhibit similar characteristics

2.0 How has the internet transformed criminal behaviour?

- **Information** - Values online are linked to ideas, not physical property
  - Why bank robbery? Virtual theft (e.g. of intellectual property)?
- **Global** - Changes in the scope of criminal opportunity
  - There are generational differences cybercrime in terms of levels of mediation by technology
  - Substantive changes in types of criminal behaviour
- **Network** - Changes in the organisation of crime and division of criminal labour - reaching victims through networks
  - Gives one person control over the whole criminal process
  - Makes the organisation of criminal activity more efficient.
  - Broadens the span of criminal activity to give offenders a global reach – creates single empowered agent - 50m X £1 robberies??

Cybercrime Motivations – distance from victim – self-satisfaction - peer respect - revenge – protest/terror - criminal /financial gain

3.0 Mapping out the contours of cybercrime the scope of criminal opportunity

3.1 Comparing physical (kinetic) crime and cybercrime

- Values in cyberspace are in ideas, not physical property
- True cybercrimes are asymmetric not symmetric
- Cybercrimes are trans-national, have no boundaries
- Are instantaneous and free of a physical time frame.
- Cyber-crimes are also contentious in that there does not yet exist a core set of values about them.
- Cyber-crimes require systems (and not technical) knowledge reflecting changes in knowledge distribution.
- Discussion of cyber-crimes tends to be offence based, but police look for the hacker stereotype.
- Cybercrime profiles differ according to a) victim groups b) technology generation c) type of criminal behaviour

3.2 Levels of criminal activity/ victims

- **Personal Security**
- **Corporate/ Organisational Security**
- **National/ International security**

Each are very different groups with different stakeholders and require different approaches. Beware of cybercrime statistics and literature that generalise one type of victimisation from the experience of another.

Durham University

3.3 Generational differences in cybercrime

- ***1st generation*** **– Traditional Crime using computers - cybercrime within discrete computing systems (e.g. mainframe) b) to assist traditional crime – information, communications**
- ***2nd generation*** **– Hybrid cybercrime - across networked computing systems (hacking across networks) - new opportunities for traditional crimes**
- ***3rd generation*** **– True cybercrime *(Sui Generis)* - new forms of harmful activity** - Spams, Piracy, Phishing(ID Theft), Scareware … STUXNET, SCAREWARE and WIKILEAKS??

True Cybercrimes are networked, distributed, and automated (spam driven cybercrime – 'phishing') moving towards complete mediation by networked technologies (e.g.., 'phishing' into 'pharming' into 'smishing' and 'vishing').

3.4 Types of cybercrime

Three generic types of cybercrime

- **Crimes against the machine (Integrity related cybercrime) – e.g., HACKING, DDOS**
- **Crimes using the machine (Computer assisted cybercrime) – FRAUD, DECEPTION**
- **Crimes in the machine (Content related cybercrime) – OBSCENITY/ VIOLENT OR ABUSIVE SPEECH/ GROOMING, INFORMATION LEAKAGE/ ESPIONAGE?**

Durham University

3.5 Three contemporary examples of globalized cybercrime by crime type

- **Zeus Trojan** – *against the machine* - slick, professionally crafted, inventive also **Stuxnet** - autonomously searches global networks for its target (specific operating systems)
- **Scareware** – *using the machine* - slick, autonomously exploits global networks to reach victims in order to deceive them into thinking it is part of the operating system and defraud them. Sends money back to crooks
- **Wikileaks** – *in the machine* - autonomously exploits the crowd sourcing potential of the internet – illustrates the potential for malicious use.

3.5ai The Zeus Trojan: A crime against the machine (also called PRG, Zbot, Kneber, Wsnpoem and Gorhax)

- The Zeus Trojan is a form of crimeware / malware that can be bought off the shelf.
- If provides a 'ready-to-deploy' package for hackers to distribute through their own botnet. ZBOT
- The botnet is easily purchased or freely traded online
- It is updated to provide new features and functions.
- It can be used to create new botnets of zombie computers
- It also steals financial and other key information.
- Zeus's ease-of-use means it is used widely. It enables most novice hackers to get started.
- It is being replaced by crimeware as service. Bespoke crimeware that can include combinations of features chosen by the 'client'.

3.5aii Stuxnet: Another crime against the machine

The Stuxnet worm is a form of *malware* that can be used to sabotage industrial control systems (*SCADA)*. It represents a 'paradigm shift' in malware threats and is distinct from other malicious worms because:

a) its primary method of entry into operating systems is (amongst other potential entry means) through USB sticks

b) like other worms it establishes a rootkit as well as a backdoor connections which allows external control

c) unlike other worms, it aggressively attacks specific types of *SCADA* systems produced by particular manufacturers

d) the July 2010 Stuxnet worm had a kill date and limited scope and sought particular system configurations – indicating that it was intended to hit specific targets, but did not find its target this time.

N.B. In the absence of further information conspiracy theories quickly evolved to map the Stuxnet threat onto contemporary political divisions. A particular concern was that the 2010 attack was specifically targeted at Iranian (nuclear) processes. Verdict – Jury (of commentators) is still out

3.5b Scareware: A crime using the machine

- **'Scareware' is malicious software** that defrauds victims by scaring them into paying for fake anti-virus packages that purport to fix their computer. Incidents have risen by as much as seven-fold this year.
- **'Scareware' is a true cybercrime** as it is solely the spawn of the internet.
- **It is significant because (for the 1st time) the malware controls the whole criminal process** from scamming victims to passing gains to the offender.
- **It illustrates new forms of criminal organisation online.**
- **It has evolved during the past year** from purposefully distressing victims into parting with money to becoming so slick and covert that victims do not actually realise they have been victimised.
- **The organisation of a Scareware attack reflects the 'affiliate marketing' model** found throughout contemporary e-commerce.
- **Scareware victimisation is often hidden** & victim's complaints are ignored.
- **Scareware's *de minimis* (small) and global nature means that prosecutions are unlikely** yet it is a crime under the Fraud Act 2006 and s.2 or s.3 of the Computer Misuse Act 1990. Offenders are hard to trace and catch.
- **Scareware is preventable by users being internet savvy** and by keeping their computer security updated.

3.5c Wikileaks: A crime in the machine

Wikileaks is an global non-profit organisation that publishes secret and classified material from anonymous sources on its website in order to 'expose oppressive regimes'. It is significant because:

a) It uses the crowd sourcing potential of the internet

b) It illustrates how much control a few people can have over the process [the courts will define the criminal aspects of Wikileaks]]

c) It exists in the machine

d) It will not go away (easily) as it resists attempts to censor it (like hate speech and pornography – other crimes in the machine)

Wikileaks is also significant because it raises a number of issues:

e) It redefines the relationship between information, the individual, the machine (computer) and the state.

f) Its impact seems to be mainly about political reputation? Has the leaked info any real value, is it just a storm in a big global tea cup?

g) Highlights the shift in world power and rise of the developing world?

h) It illustrates how the nature of keeping secrets has changed

i) what are the responsibilities of those who publicize leaks?

ii) what are the responsibilities of those who keep the secrets?

4.0 The Future: The reorganisation of criminal labour by network technology – change drivers

- **Empowered single agents** have a global reach and total control
  - So why commit a local $50m robbery when you can commit 50m $1 frauds?
- **The power of the crowd can also be harnessed** in an number of different ways. ‘Crowd sourcing’ can be used to commit or prevent crime
- **New forms of flat criminal organisation appear online to** mirror online business processes. The relationship between offender and victim has become brokered by affiliates
  - **Affiliates rent out /give access to networks** of infected computers to install malicious software, or they install it at a cost
- **Easy online access to new specialist skills** via crimeware as a service – scarce skills once the preserve of a technological elite are now available to all online. Crimeware as a service mirrors software as a service in that attack viruses and software can be made to order.
- **Malicious software is more sophisticated than it used to be**. Blended threats, for example, now combine the characteristics of viruses, worms, Trojan Horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack.

What is Cybercrime - References

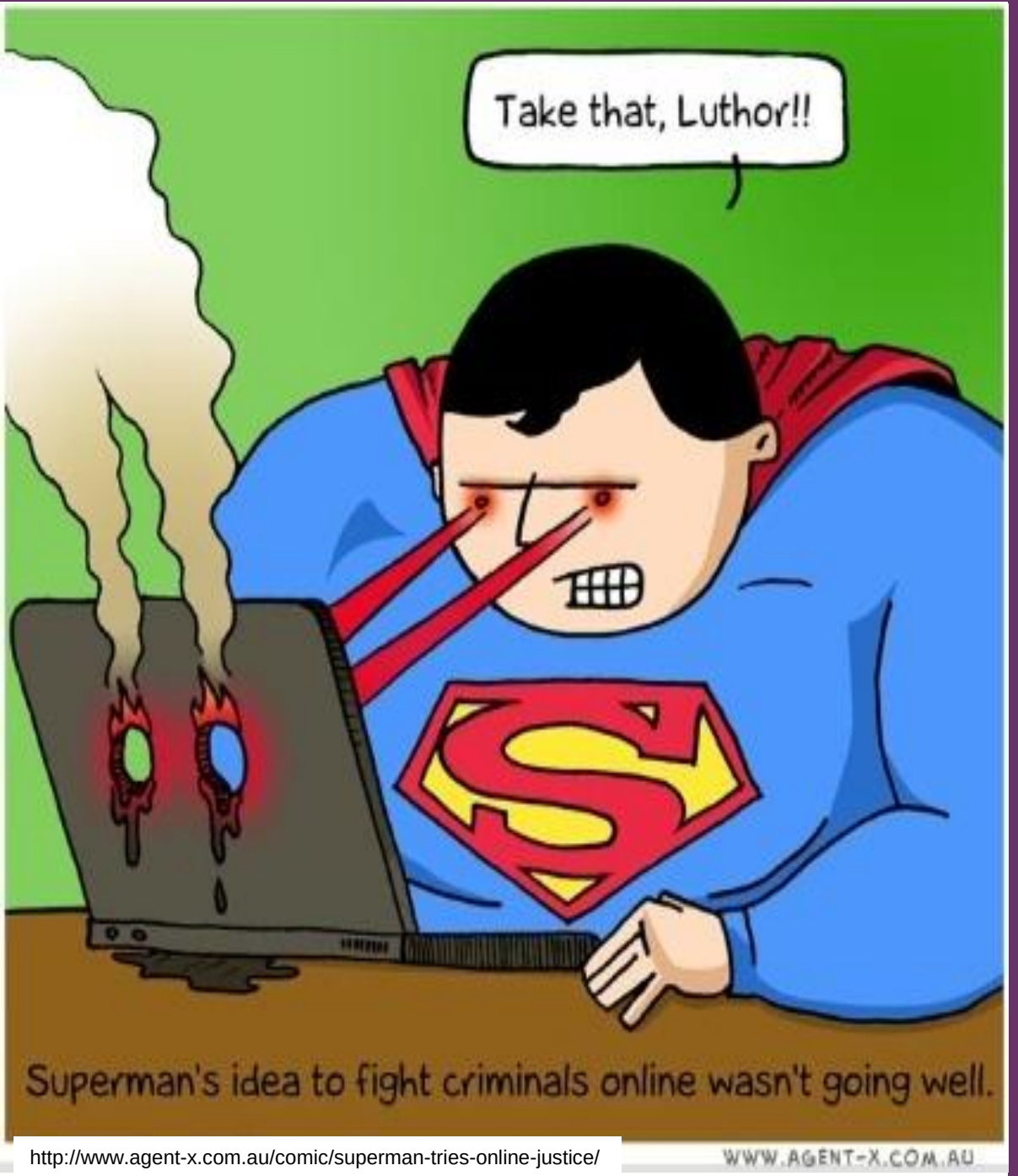
Chapters 1, 2 and 3 of Wall, D.S. (2007) *Cybercrimes: The transformation of crime in the information age*, Cambridge: Polity. ISBN 0745627358

ALSO see

- Wall, D.S. (2005/10) 'The Internet as a Conduit for Criminal Activity', pp. 77-98 in Pattavina, A. Information Technology and the Criminal Justice System, Thousand Oaks, CA: Sage (ISBN: 0761930191) (Revised March 2010) Available at SSRN: http://ssrn.com/abstract=740626
- Wall, D.S. (2008/10) 'Cybercrime and the Culture of Fear: Social Science fiction and the production of knowledge about cybercrime', *Information Communications and Society*, vol. 11, no. 6, pp 861-884 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155155

ALSO Follow through the references cited in these sources

PART 2
What can we do about Cybercrime



http://www.agent-x.com.au/comic/superman-tries-online-justice/

Durham University

5.0 What are the criminal justice challenges

Most cybercrimes avoid the Criminal Justice radar

- **De minimism** – crimes are too small in impact
- **Nullum crimen disparities** – no law, no crime?
- **Jurisdictional disparities** – where to prosecute?
- **Under-reporting** – a) embarrassment b) not serious enough c) corporate fear of exposing weaknesses
- **Conflict between private v public interests**
- **Non-routine activity and police culture** – not picked up by police so little experience develops in area

5.1 Technology, Crime and the Police

- **Historically**, the police have had a longstanding and uncomfortable and relationship with new technologies. See the *Police Review* at the turn of the C20th (and throughout the C20th) - it is full of police moans about criminals being one step ahead of them.
- **Technology changes things - i**t disrupts traditional policing practices, it threatens to shift the balance of power to the criminal unless police develop an appropriate response.
- **Knowledge is power** - Those who have the technology and the knowledge to use it can exert power over those who do not have that privilege- criminal or police.

5.2 Technology disrupts policing

- **Cybercrimes challenge laws and traditional police practice** because of the informational, globalised and networked nature of new crimes.
- **Cybercrimes are individually small but significant in their aggregate** – e.g.., scareware (fake anti-virus software) is a true cybercrime. It is fully automated crime in that it deceives the victim and sends the money to the crooks, one early example conned 30,000 people out of £15 each.

  Each is too small to complain about but in total represents almost half a million pounds. Much of this is written off, but important crime intelligence is lost.

  - Identifying jurisdictions for investigation and prosecution is problematic

  - Identifying victims is problematic – FBI enterprise approach

5.3 We over-problematize cybercrime

CyberCrime problems get blown out of proportion

- **Many networked news medias draw upon the same news sources - usually a press release. Over 70% are unchecked. ‘Churnalism’ Davies**
- **Threats become confused with reality & issues of personal, organizational and national security get mixed.**
- **News stories and the emotions they evoke give an impression of a constant crime wave.**
- **This eventually shapes the way people view crime and increases demands for action.**

5.4 Creates a reassurance gap in policing cybercrime

Combine the criminal justice challenges with

- **Media over-problematisation of cybercrime via 'CHURNALISM (and cultural construction of cybercrime and cybercriminal) and …**

a) Misconceptualization of the problem

b) Overestimation of police role in solving it

- **We get a Reassurance Gap in policing – where the demands made of the police and government to respond to cybercrime simply cannot be met.**

Why then do people still use cyberspace?

6. Policing Cyberspace through networks of security: How is the challenge being met?

Cyberspace is already subject to multi-tiered governance - reflects the plurality of policing in late modern society – combines elements of public and private models of policing.

- **Internet Users and User Groups**
- **Virtual environment managers and security**
- **Network Infrastructure Providers**
- **Corporate organisations and corporate security**
- **Non-governmental, non-police organisations**
- **Governmental non-police organisations**
- **Public police organisations**

The Public Police only play a small role in policing cyberspace but it is important and symbolic

6.1 Technology can also transform policing

This is the same slide as technology transforms crime

- **It globalises ideas about policing**
- **Extends the police reach across a global scale**
- **The dark cloud over the internet has a silver lining–** blue cloud computing??
- **Networked technologies:**

  a) help police resolve traditional crimes

  b) provide new opportunities for policing

  c) creates new ways of policing new crimes - some entirely new and of the internet – honeynets, spampots - but also new reporting, triage and response systems to deal with i) crimes against the machine (Hacking),

  - ii) crimes using the machine (frauds)
  - iii) crimes in the machine (e.g. extreme pornography)

– **SEE NEXT PPT**

- **Promotional tool** – Home Office and Force websites give the public and professionals information about police services on offer and how to obtain them
- **Communications tool** –***a) Inward communications*** - Public to police - Reporting Offending - Some police (or non-police – such as IWF) websites enable people to report offending – Making complaints - ***b) Outward communications*** - Police to others enables the police to communicate important messages to the public, other police forces and the wider police family
- **Engagement tool**-utilize crowd-sourcing potential to help police community
- **Investigative policing tool** – enables the police to investigate traditional offences more closely, not just true cybercrimes which are spawned by the internet such as hacking, online frauds and extreme pornography.
- **Proactive policing tool** – Honeynets, gotcha www sites
- **Crime Prevention tool** – it can be used to inform the public about taking security measures to prevent crime
- **Regulatory tool** – networked technologies, it can be argued, give the police too much power. Network technologies can be used to regulate police behaviour and also help to introduce reform.
- **Organizational tool** for bringing together a range of police services, some of which may be outsourced. See UK arrangements for policing fraud.

7.0 The UK Cyber Security Strategy 2009–origins

- **Digital Britain Report 2009** (BIS) – para. 69

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

- **National Security Strategy** -

http://www.cabinetoffice.gov.uk/reports/national_security.aspx

- **UK Cyber Security Strategy 2009** –

http://www.cabinetoffice.gov.**uk**/media/216620/css0906.pdf

- **UK Cyber Crime Strategy 2010 -**

http://www.officialdocuments.gov.uk/document/cm78/7842/7842.pdf

- **National e-Crime Programme - ACPO e-Crime Strategy 2009**

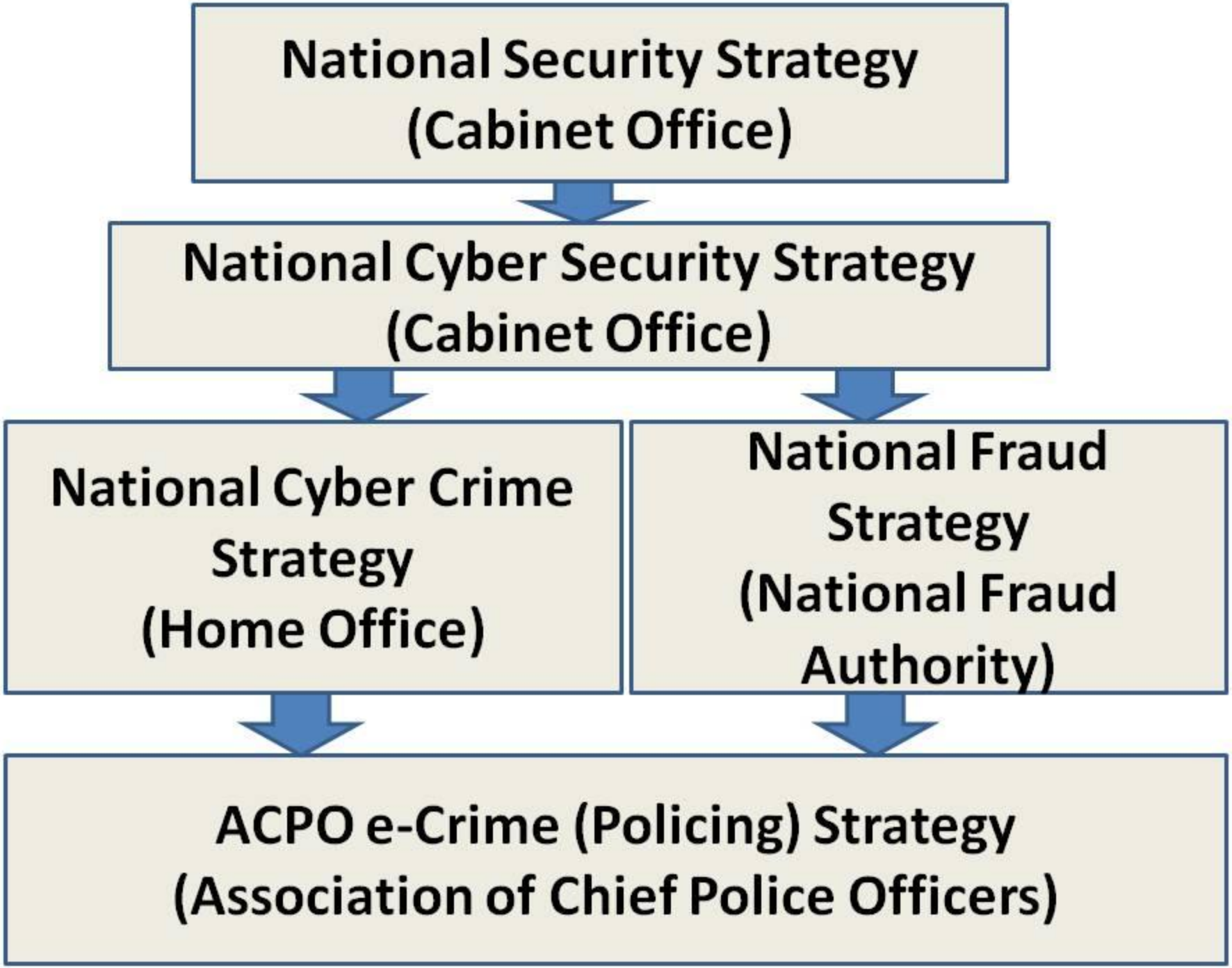
http://www.acpo.police.uk/asp/policies/data/Ecrime%20Strategy%20Website%20Version.pdf

DRIVERS

- **Data losses** let to outcry and embarrassment over the government data losses. CD found in a drawer but fear it had fallen into wrong hands.
- **Threat of terrorism** - Lord West (Security Minister) "We know terrorists use the internet for radicalisation and things like that at the moment, but there is a fear they will move down that path (of cyber attacks).
- **Threat of cybercrime** - e-crime crime costs the UK several £1B per year

Durham University

A SCHEMATIC FOLLOWS


National Security Strategy
(Cabinet Office)
National Cyber Security Strategy
(Cabinet Office)
National Cyber Crime
Strategy
(Home Office)
National Fraud
Strategy
(National Fraud
Authority)
ACPO e-Crime (Policing) Strategy
(Association of Chief Police Officers)

7.1 The UK cyber security strategy – Cabinet Office

- **The UK CyberSecurity Strategy emphasises need for Government, organisations across all sectors, international partners and the public to work together. The Government will:**
- ***Establish a cross-government programme to address priority areas in* pursuit of the UK's strategic cyber security objectives, including:**
  - **− Providing additional funding for the development of innovative future technologies to protect UK networks;**
  - **− Developing and promoting the growth of critical skills;**
- ***Work closely with the wider public sector, industry, civil liberties groups, the* public and with international partners;**
- ***Set up an Office of Cyber Security (OCS) to provide strategic leadership for and* coherence across Government;**
- ***Create a Cyber Security Operations Centre (CSOC) to:***
  - **− actively monitor the health of cyber space and co-ordinate incident response;**
  - **− enable better understanding of attacks against UK networks and users;**
  - **− provide better advice/information about the risks to business and public.**

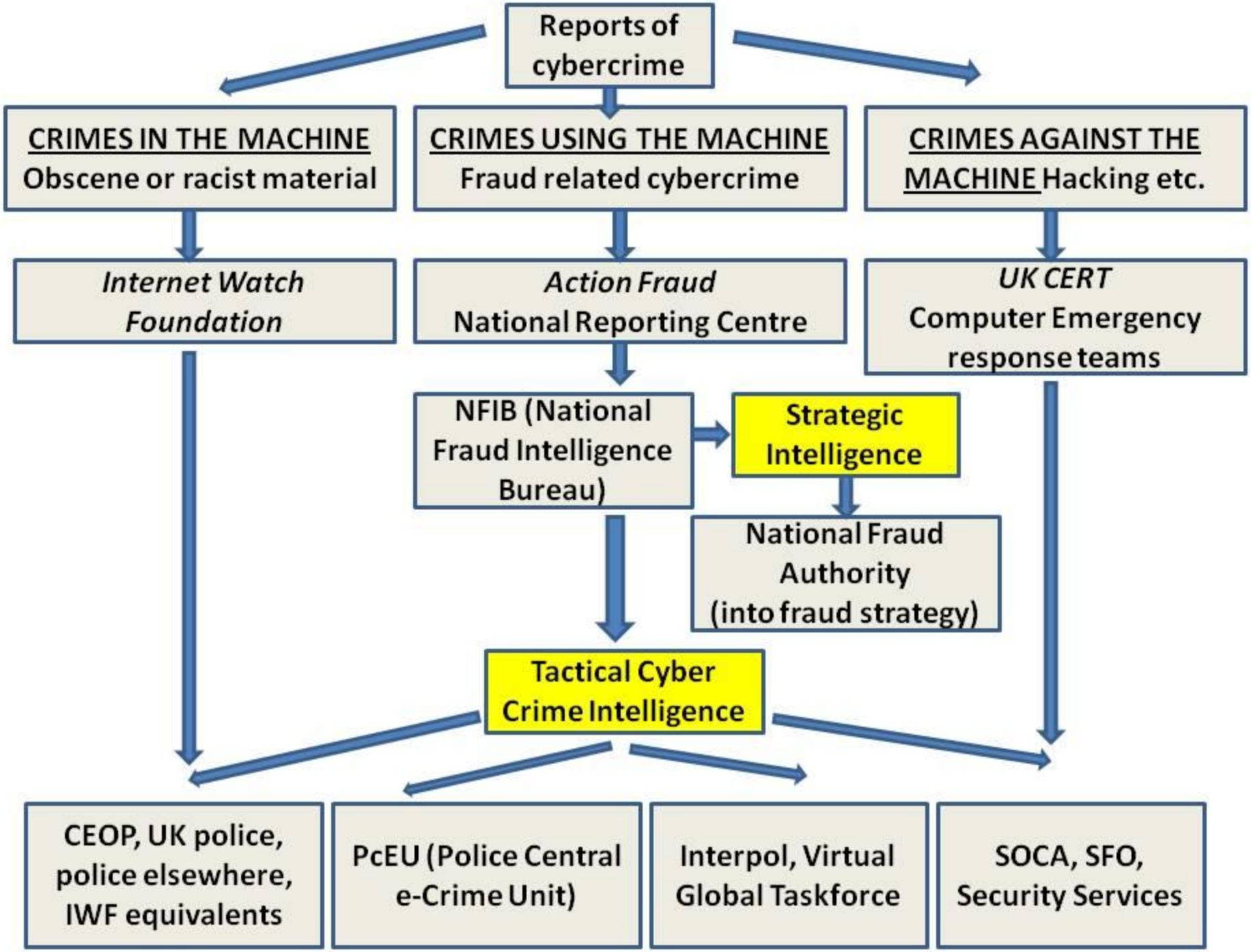
7.2 Police Central e-crime Unit [Part of ACPO's National E-Crime Programme]

- **PCeU sits next to the Met Unit provides specialist e-crime support**
- **Receives tactical information from the National Fraud Intelligence Bureau (NFIB) (CoL Police)** - the SPOC for intelligence and information (NFIB receives intel from Action Fraud)
- **Conduct e-crime intelligence development and analysis both on a strategic and tactical level.**
- **Manage and disseminate e-crime intelligence to ACPO police forces, law enforcement agencies and partners.**

COULD CHANGE VERY SOON WITH A) REVISION OF THE STRATEGIES AND B) THE PROPOSED FORMATION OF THE NCA (National Crime Agency) in the UK

7.3 UK Fraud Reporting Arrangements as a prototype for cybercrime policing

- Much criticised, the UK Fraud reporting arrangements nevertheless utilize information technologies to create a prototype system for reporting and policing cybercrime at a national level.
- It triages reports in terms of their strategic and tactical value. On the next slide Fraud reporting (a crime using machines) is in the central column. The provisions for reporting crimes against the machine and crimes in the machine are mapped onto them.
- If the Fraud reporting arrangements are successful then they could cover other cybercrimes.


Reports of cybercrime
CRIMES IN THE MACHINE Obscene or racist material
CRIMES USING THE MACHINE Fraud related cybercrime
CRIMES AGAINST THE MACHINE Hacking etc.
Internet Watch Foundation
Action Fraud National Reporting Centre
UK CERT Computer Emergency response teams
NFIB (National Fraud Intelligence Bureau)
Strategic Intelligence
National Fraud Authority (into fraud strategy)
Tactical Cyber Crime Intelligence
CEOP, UK police, police elsewhere, IWF equivalents
PcEU (Police Central e-Crime Unit)
Interpol, Virtual Global Taskforce
SOCA, SFO, Security Services

7.4 The National Crime Agency

- The proposed UK National Crime Agency incorporates the Serious Organised Crime Agency, CEOP and National Police Improvement Agency, PCEU?. It may also include a new Economic Crime Agency/Body.
- Home Office has takes over Treasury project to create new Economic Crime Agency to replace the Serious Fraud Agency.
- Decision still to be made whether to amalgamate it with the NCA
- Decision still to be made whether the new agency should have powers of prosecution as well as investigation. The proposal is out for consultation.
- Home Office is the lead department to work with the Attorney General's office, Ministry of Justice, the Treasury, Cabinet Office and others.
- The problem is that "[t]here are a number of agencies all doing things slightly differently and in consequence things are falling between the grilles" (Edward Garnier, solicitor-general).
- The intention is to coordinate various economic fraud bodies to cease the current "piecemeal" approach to tackling white-collar crime.
- Old Battle lines are still drawn, e.g., the City of London police will retain its role as the main anti-fraud force after the creation of the new agency, but will work closely with the new agency. Perhaps Met and PCEU also.

7.5 Oates, J. (2011) 'May promises £63m for cybercrime fight', The Register, 15 February,

http://www.theregister.co.uk/2011/02/15/uk_cybercrime_spending/

Home Secretary Theresa May has announced a £63m boost to police budgets for combating cyber crime.

The money will come from the £650m being spent on beefing up the UK's national cyber defences announced last year.

The move to a proactive, and attacking, form of cyber defence was explained to the *Reg* by "senior Whitehall officials" in 2009. They warned the newly-formed Office of Cyber Security, within the Cabinet Office, that the main threats to UK infrastructure comes from organised criminals, not terrorists.

Officials also made clear that attacks were no longer likely to be "online only" - 90 per cent of UK high street transactions are now "online" in some sense.

A potted statement from the Home Office said: "This proposed new funding will be used to develop the UK's overall response to cyber crime. The Government is determined to build an effective law enforcement response to the cyber crime threat building upon the existing expertise within SOCA and the Met Police Central e-Crime Unit.

"More details of the funding allocation will be made public in due course."

The Home Office press office was unable to confirm the figure of £63m, which was reported by eGovmonitor reporting comments made by Theresa May. ®

8. Conclusions

- **The problem is part of the solution -** networked technologies can assist the police services to close the reassurance gap between public demands for more action and delivery. But the problem is also partly the symbolic need for action (policing).
- **Technology assists the police in many ways**, including regulating them and possibly assisting in implementing reforms. The new fraud arrangements are a good example of the way that technologies can be used to join agencies.
- **IT is more than just re-assurance policing IT can also reassure the police**

Policing Cybercrime - References

Wall, D.S. (2007/11) 'Policing Cybercrime: Situating the public police in networks of security in cyberspace', *Police Practice and Research: An International Journal*, 8(2): 183-205 (Revised Feb. 2011) Available at SSRN: http://ssrn.com/abstract=853225

Ch 8 Wall, D.S. (2007) *Cybercrimes: The transformation of crime in the information age*, Cambridge: Polity

Wall, D.S. (2010) 'Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age', in T. Holt, T., and B. Schell (2010) (eds) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, Hershey, PA (USA): IGI Global - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1563626

Oates, J. (2011) 'May promises £63m for cybercrime fight', *The Register*, 15 February, http://www.theregister.co.uk/2011/02/15/uk_cybercrime_spending/