Policing Cybercrimes: responding to the transnational challenges of cybercrime

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

Presentation to Dartmouth College, Institute for Security, Technology and Society, 21st October 2010

Durham University

Cyberpunk, 1990
© Steve Pyke

Outline

1. The shaping of public expectations of the police – the rhetoric vs. the reality
2. Understanding the cultural construction of cybercrime and distortions in our view of it
3. Mapping Cybercrime to make sense of it
4. The Policing challenges of cybercrime and policies being implemented to deal with them
5. Identifying emerging problems

Durham University

THE RHETORIC – up to 3million threats per year
THE REALITY - 300 CMA 1990 prosecutions in 20 years

Most Visited | Getting Started | Latest Headlines

BBC NEWS | Technology | Cyberc... | Microsoft Outlook Web Access

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

start | BBC NEWS | Technolo... | Downloads | dissertation 3.doc - M... | 15:08

THE RHETORIC – Hackers can destroy society
THE REALITY – The risk is different to expected

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 it to blast apart like a large hand grenade.

"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 major cities.

"As dangerous as this technology is right now, it's going to get much 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 against you or just plain doesn't like your looks, can kill you and never be found out."

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

Arnold Yabenson.

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

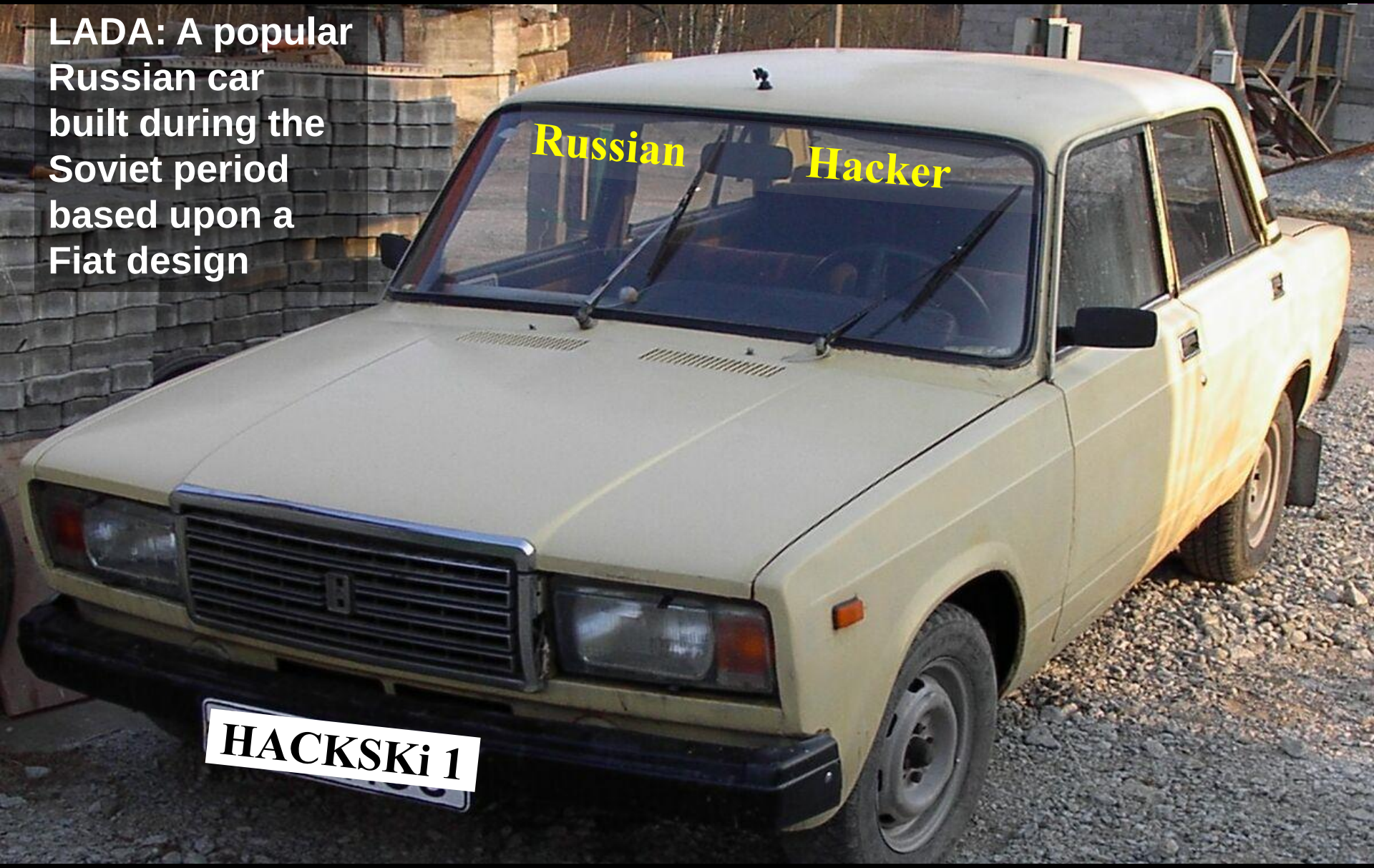
THE RHETORIC – Most of the dangerous hackers are Russian
THE REALITY – We don't really know – is it important?

What the 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

1. The shaping of public expectations of the police - uncritical acceptance of cybercrime myths

- Is the internet actually criminogenic?
- Does the internet corrupts normally law abiding individuals who go on a moral holiday when on the internet ?
- Is cybercrime overwhelming us ?
- Are hackers omnipotent super-users, who are anonymous and go unpunished & are they male?
- Is organised crime is taking over the internet ?

EACH IS MYTH CONTESTABLE – THE REALITY IS MORE COMPLEX

We need more critical questioning of conventional wisdoms

Durham University

1.1. What fuels the rhetoric & myths – Over-problematizing and under-reporting

- **Over-problematizing – Automatically reported threats represent breach of scientific rules not crimes**
- **Lack of reliable statistics – disintermediation of data**
- **Lack of reliable news – disintermediation – 'Churnalism'**
- **Under-reporting by individual and victims**
  - ***Individual*** – displacement – not considered serious - embarrassment – danger not evident
  - ***Corporate*** – private interests – not show weakness – loss part of business model
- **Jurisdictionality a) definitions b) degrees of co-operation**
- **Viral Information Flows**

EACH CONTRIBUTES TO THE CULTURE OF FEAR

Durham University

2.0 Understanding the cultural construction of cybercrime and distortions in our view of it – The Cultural Construction of the Hacker

- **Victorian Science Fiction**
  - the savant – hacking time and space
- **Dystopic Post-war Science Fiction** – e.g. 1984
- **Futureshock ('faction')**
  - **fear of future and of change (Toffler)**
- **Panics/ Moral Panic**
  - **see Viral Information Flows**
- **Culture of fear**
  - **expectation of crime (Furedi's Culture of Fear/ Garland's crime complex)**

2.1 From meatcrime to cybercrime

- The origin of the term ‘cybercrime’ is unclear, turn of 1980s/ 1990s in late cyberpunk media.
- Cyberpunk defined cybercrime as a harmful activity taking place in virtual environments.
- It made the ‘hi-tech low-life’ hacker narrative an entertainment norm in ‘haxploitation’ movies.
- Gibson’s model of cyberspace has become the conceptual norm and has:
  - a) shaped the public imagination through the visual media
  - b) begun to influence social theory

Durham University

2.2 Expressions of cyberpunk and cybercrime

1. **Science fiction forums** - *Omni Magazine* (1978 – 1998)
2. **Science fiction novels,** – *Neuromancer* (Gibson), *Snowcrash (Stephenson)*
3. **Comic books** – *Dark Avenger*
4. **Haxploitation Movies –** generational ideal types

– ***1st generation*** hacker films defined by "the hack" (Billion Dollar Brain, 1967; Italian Job, 1969; Superman III, 1983 etc.)

– ***2nd generation*** films defined by the gender specific "hacker" (War Games, 1983; Electric Dreams, 1984; Real Genius, 1985).

– Later **2nd generation** films shifted to hacks in a cyberspace – hackers still young but less gender specific and less likely to adopt moral high ground than in earlier films (Goldeneye, 1995; Hackers, 1995; The Net, 1995 etc.)

– ***3rd generation*** films defined by both "hacker and hack" in virtual environments (Tron, 1982; The Matrix, 1999 etc.) but also Die Hard 4.0?

5. **TV Movies, TV Programmes**
6. **Video Games**

"Contemporary movie and media imagery subconsciously orders the line between fact and fiction and has crystallized 'the hacker' offender stereotype as the archetypal 'cybercriminal' (2007:16)

2.3 Distorted perceptions of cybercrime

Perceptions of cybercrime get distorted by

a) the uncritical coupling of social science fiction hacker narratives with

b) the ambiguous scientific conceptualisation of networked virtual space viewed in terms

c) of a traditional Peelian crime and policing perspective (e.g. dangerousness), against a

d) dystopic social science fiction backdrop.


Sir Robert Peel

"The conceptualisation of cybercrime in social science fiction as dramatic, futuristic and potentially dystopic proscribes public expectations of cybercrime as beyond the capabilities of normal folk. As sensational, disempowering victims and being beyond the scope of state protection (e.g., policing).

When these perspectives are placed against a backdrop of contemporary cultural reactions to technological change they create ideal circumstances for the creation and maintenance of mythology."

2.4 The result of the distorted perceptions of cybercrime

- Low level of public knowledge about risks
- Low offender profiles
- Few common definitions of cybercrimes/ Myths
- Raised public expectations of government to act
- Raised expectations of the police to act

The emergence of a REASSURANCE gap between what the public demand (shaped by the culture of fear) and what the police and government can provide.

3. So, How do we map out the contours of cybercrime & scope of criminal opportunity

- Values in cyberspace are in ideas, not physical property
- True cybercrimes are asymmetric not symmetric
- Cybercrimes are trans-national, have no boundaries
- They 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 considerable systems knowledge. [resulting from changes the distribution of knowledge].
- Discussion of cyber-crimes tends to be offence based.

WE CAN APPLY THE FOLLOWING THREE SETS OF DIFFERENTIATORS WHEN MAPPING OUT CYBERCRIME

Durham University

3.1 Levels of criminal activity /victim group

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

Each are very different debates with different stakeholders and require different responses – both issues and priorities are regularly confused in debates.

Durham University

3.2 Differences in cybercrime - mediation

- **Traditional Crime using computers** - **cybercrime within discrete computing systems (e.g. mainframe) b) to assist traditional crime – information, communications**
- **Hybrid cybercrime** - **across networked computing systems (hacking across networks) - new opportunities for traditional crimes**
- **True cybercrime** ***(Sui Generis)*** **- new forms of harmful activity** - Spams, Piracy, Phishing, Scareware … also STUXNET??

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').

3.3 Different Families of Cybercrime

- **Crimes against the machine** (Integrity related cybercrime) – e.g., Hacking, DDOS
- **Crimes using the machine** (Computer assisted cybercrime) – Deceptions/ Frauds
- **Crimes in the machine** (Content related cybercrime) – Obscenity/ Violent or abusive speech / grooming?

EACH REFLECT DIFFERENT BODIES OF LAW

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

4. 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?
- **Non-routine activity and police culture** – not picked up by police – develop little experience in area
- **Under-reporting** – a) embarrassment b) not serious enough c) corporate fear of exposing weaknesses
- **Conflict between private v. public justice interest**

4.1 HOW IS THE CYBERCRIME CHALLENGE BEING MET 1? Policing Cyberspace through networks of security

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**

Durham University

4.2 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**

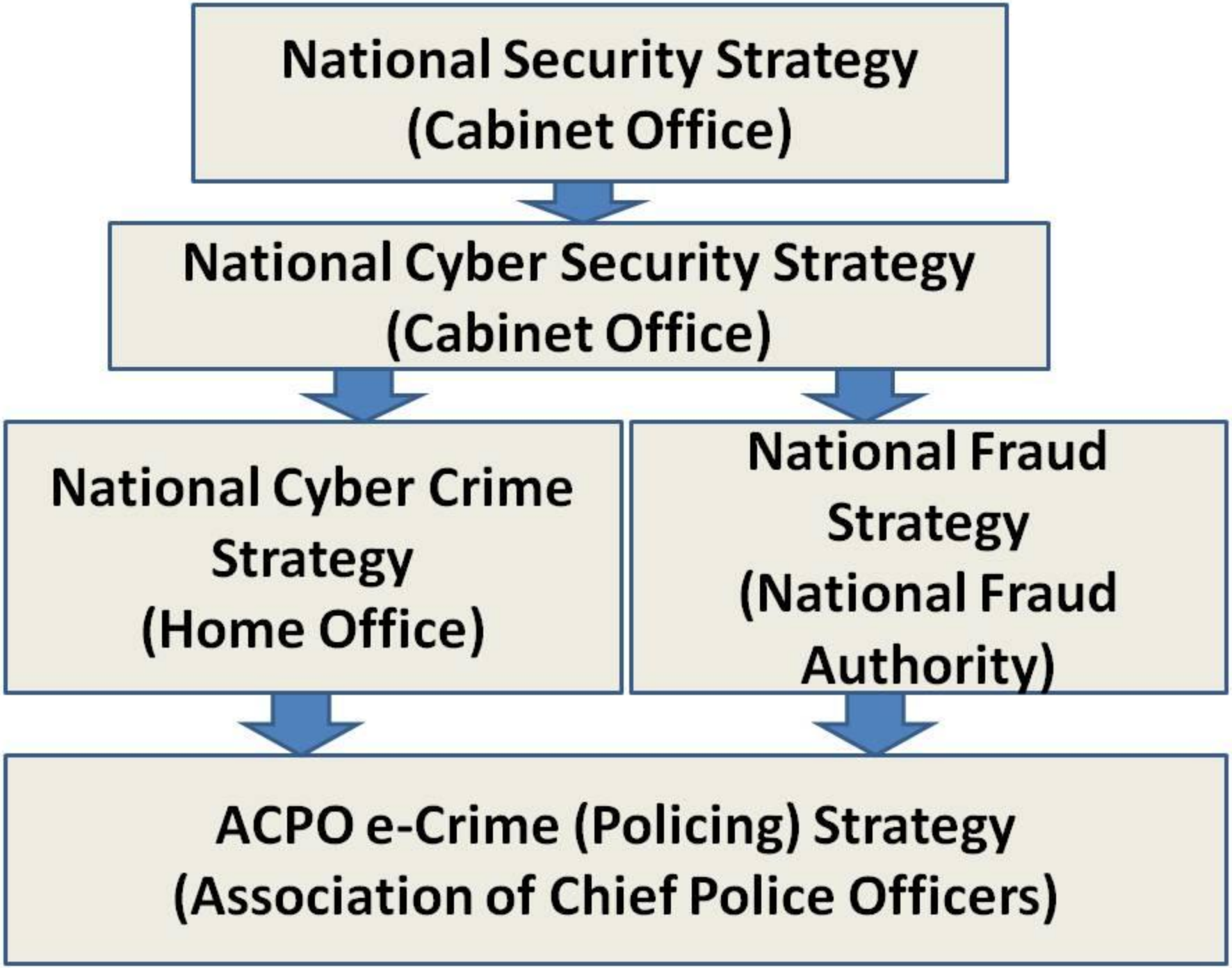
http://www.acpo.police.uk/asp/policies/data/Ecrime%20Strategy%20Website%20Version.pdf

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)

4.3 UK CyberSecurity Strategy emphasises need for Government, organisations across all sectors, international partners and the public to work together.

Purpose of Strategy - The Government will… Secure the UK's advantage in cyber space …by reducing risk from the UK's use of cyber space…

- **Reduce the threat of cyber operations by reducing an adversary's motivation and capability;**
- **Reduce the vulnerability of UK interests to cyber operations;**
- **Reduce the impact of cyber operations on UK interests;**

…and exploiting opportunities in cyber space…

- **Gather intelligence on threat actors;**
- **Promote support for UK policies; and**
- **Intervene against adversaries;**

…through improving knowledge, capabilities and decision-making.

- **Improve knowledge and awareness;**
- **Develop doctrine and policy;**
- **Develop governance and decision making;**
- **Enhance technical and human capabilities.**

4.4 The UK's cyber security strategy – Cabinet Office

To address the UK's cyber security challenges, the Government will:

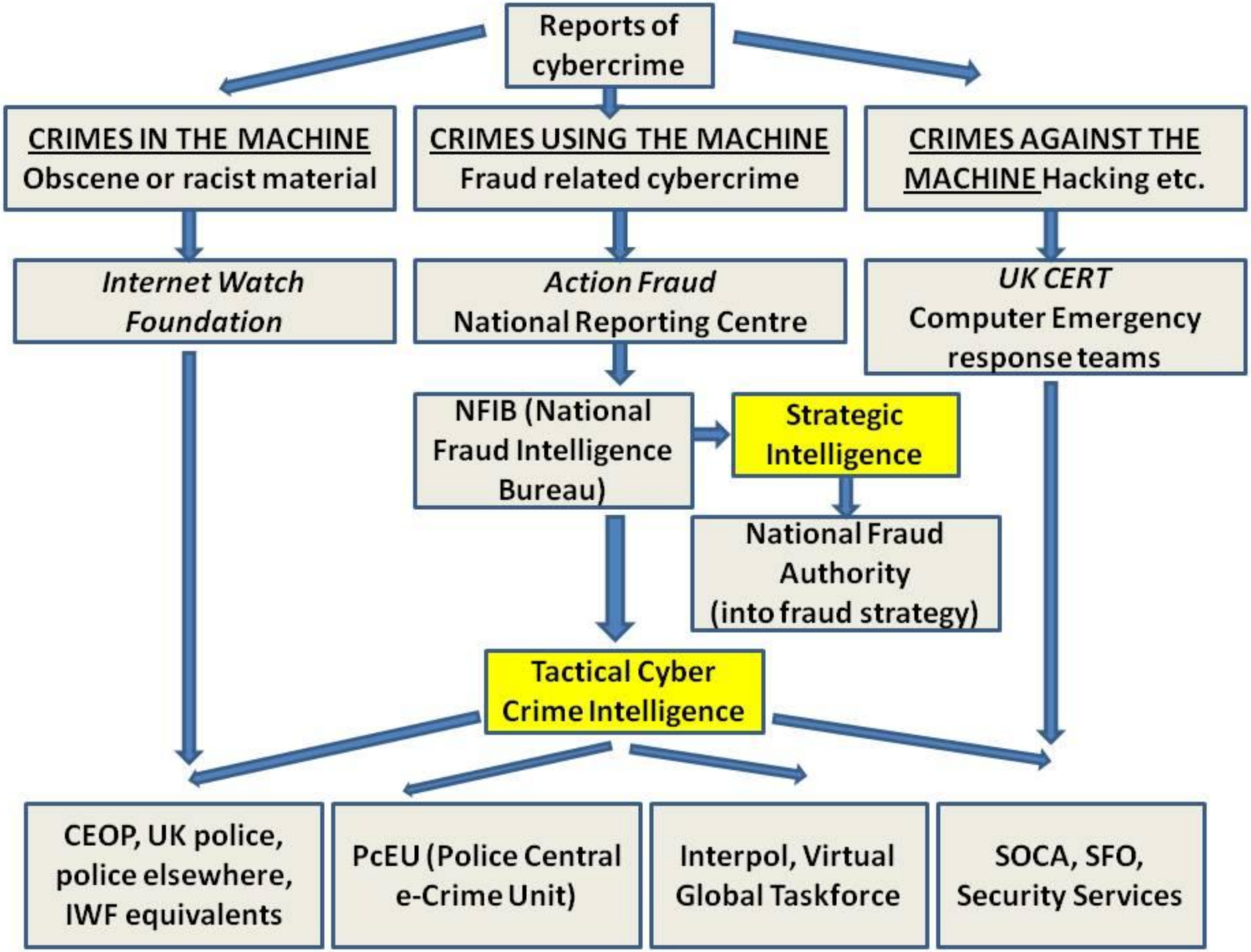
- ***Establish a cross-government programme to address priority areas in* pursuit of the UK's strategic cyber security objectives, including:**
  - **− Providing additional funding for the development of innovative future technologies to protect UK networks;**
  - **− Developing and promoting the growth 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.**

Durham University

4.5 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


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

5. WHAT PROBLEMS WILL WE FACE IN THE FUTURE?

1. New forms of crime

- **Are all of the (proof of concept) predictions and fears over the past 10-15 years now starting to be realised?**
  - **Crimes against the machine – new hacks**
  - **Crimes using the machine – new frauds**
  - **Crimes in the machine – social networking as a means of offenders engaging with victims**
- **Convergence of cybercrimes** – e.g. scareware (fake antivirus software) can combine all three, uses hacking techniques to get into the machine, mimics operating system IP to get trust, but then defrauds. It is primarily a fraud, but also combines aspects of the others.
- **Convergence of technologies** – new devices converging technologies to create new functionality — different operating systems (and weakness in operability) both technologically and also socially. **Killer toaster reality?**

STUXNET??

Durham University

A Quick Note on Stuxnet

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.

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.

5.1 WHAT MORE PROBLEMS WILL WE FACE IN THE FUTURE?

2. Viral Information Flows

- **as a possible platform for cyber-terrorism? Misinformation creating social action – malicious flash mobbing creating disasters**
- **as a possible danger to reputation of one's own organisation or one's self – misinformation gets out of control – SEE NEXT SLIDE ON VIRALS**

Note on Technical solutions

- **ethics and law about information held and shared**
- **should we allow updates only from every www source (like we allow 999 calls from all phones)**
- **should we allow updates to illegally copied operating systems (because everyone suffers?)**

A Quick note on viral information flows and the significance of the signal event

- **Viral information flows across the blogosphere and news medias to create <u>panics</u> – REMEMBER Y2K!!**

– those countries that didn't prepare were no less affected than those that did.

  - **Estonian Cyberwars!! Russia or ??**
  - **Madeleine McCann**
  - **Internet Suicide Sites**
  - **UK Muslim education policy**
  - **Cyber stalking**
  - **Sub-prime panic - Northern Rock – 2008 World Credit Crunch**

- **'Signal events' distort perceptions of reality**
- **They increase the culture of fear of cybercrime**

Durham University

"PANIC ON THE STREETS OF LONDON"
2008 Sub-prime panic and Credit Crunch – wakeup call

Conclusion

- **Distorted perceptions of cybercrime arising from tensions in the production of knowledge about cybercrime and the cultural construction of the hacker have contributed to a culture of fear about cybercrime**
- **Raised public demands for police and government action on cybercrime cannot be fully met because the policing of cyberspace is conducted by a range of actors and organisations. The public police play only a small part in policing cyberspace despite the high level of demand.**
- **The reassurance gap is closed by creating specialist national police units and also engaging all of the participating networks of security.**
- **The problem with such measures is sustaining them within the police organisation and managing micro-politics and also using prevention technology wisely and ethically.**

References

Chapters 2&3&8 - Wall, D.S. (2007) *Cybercrime: The transformation of crime in the information age*, Cambridge: Polity

Wall, D.S. (2008) '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

Wall, D.S. (2007/10) 'Policing Cybercrime: Situating the public police in networks of security in cyberspace', *Police Practice and Research: An International Journal*, 8(2): 183-205 (Revised May 2010) Available at SSRN: http://ssrn.com/abstract=853225