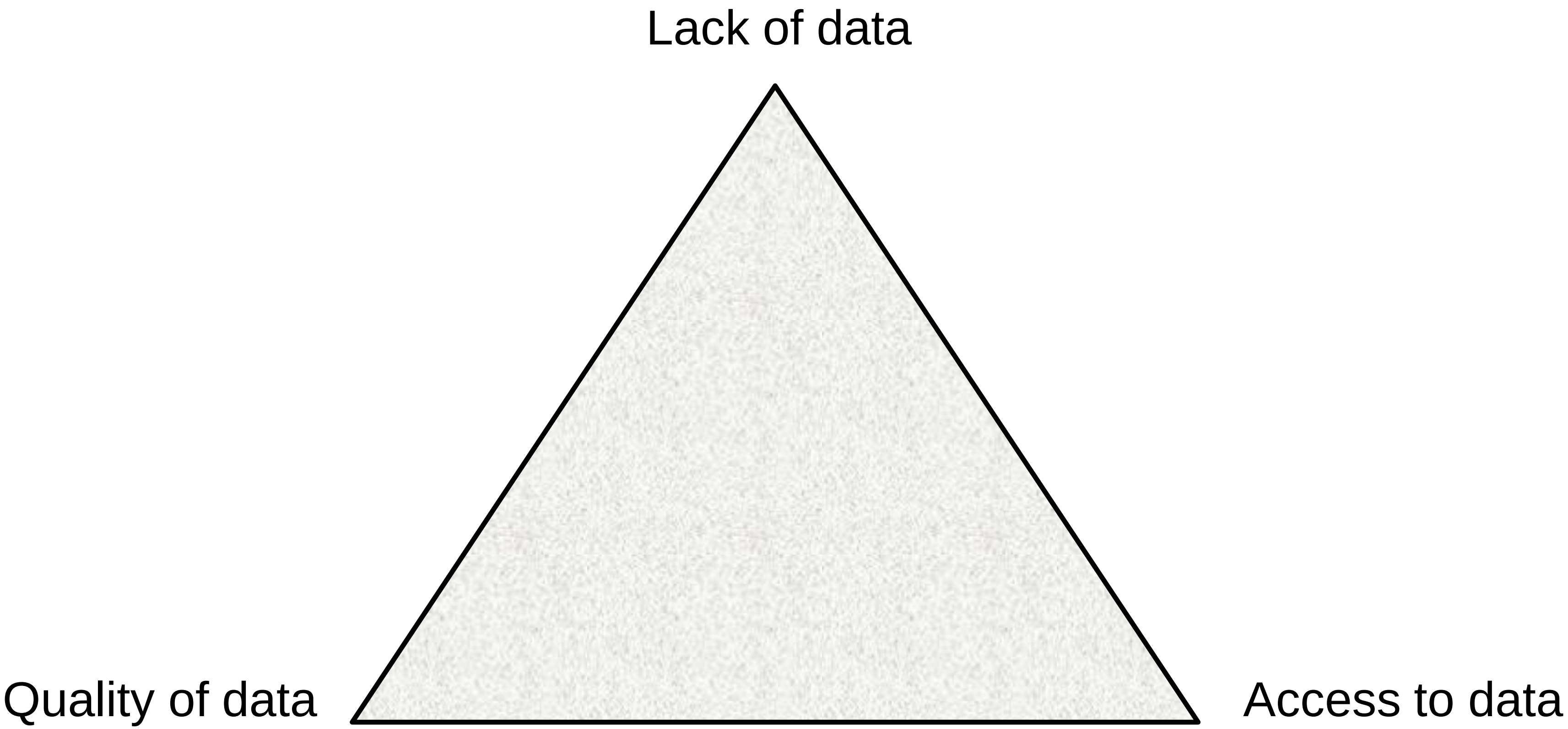
Evidence for cybercrime: reporting and evaluation

M.R. MCGUIRE

UNIVERSITY OF
SURREY

Backgrounds

Acquiring and evaluating the threat of cybercrime faces 3 familiar problems around data reliability



Data organisation and modelling

Evaluating cybercrime threat challenged by at least two conceptual problems

1. What is ‘threat’ – and for whom?
2. Whether to frame threat in technical/technological or in social terms

The UK Review of Cybercrime (2013)

Acknowledging that current cybercrime knowledge very weak & fragmented UK Home Office decided in 2012 to conduct a ‘stocktake’ of what we know about cyber-offending and the cyberthreat

The Review of Cybercrime (I) : Brief & methods

Methodology: Evidence review

Criterion for inclusion: only data acquired by robust methods – ie data acquired through scientifically conducted survey; representative sample, etc

Problem: - Automatically ruled out large areas of cybercrime literature - especially from security software sector because of inadequate methods

(II): Model and Conceptual Framework

- **Second question** – how to accommodate data gathering within some kind of useful framework/model
- Radical suggestion : apply aspects of model developed in my (2008) *Hypercrime: the New Geometry of Harm*
- Don’t view cybercrime as a ‘technology crime’, view technology as a ‘secondary’ fact to the key relation. That is:
- The function of technology in ‘extending’ social interaction & ‘hyperconnectedness’
- Result in key medium for digital offending - a “hyperspace’ - not a cyberspace
- And therefore a different KIND of threat - ‘hypercrime’, not cybercrime?

Refinement of Model: Stage 1

- Less radical approach preferred
- Develop model based upon victims & harms
- **But**: attempt to retain why online/offline schism unhelpful by using the distinction between *Digital tools and Digital targets* to organise analysis

- **Key requirements**:
- Include only actions which were ‘criminal’ - not harmful
- Indicate relevant legislation
- Provide a ‘fit’ with SOCA conceptualisations

					Victims				
					Private		Public		
Digital Tool		SOCA defined Risk			Individual	Business	Government	Other	Legislation
Software		Malware operations		Offences	frauds theft		Fiscal Frauds		Fraud Act 2006
social network		none defined			stalking grooming bullying				Sexual Offences Act 2003 Protection of Children Act 1978
online markets		cyber enabled risks			marketing illicit commodities auction frauds				
Tor/anonymous services					criminal conspiracy intelligence sharing exchange of obscene images				
hardware - eg mobiles, pads		none defined					Public disorder criminal conspiracy		
Digital Target									
Data		data markets			IP/data theft & distribution				Computer Misuse Act
Networks		Technical Infrastructure threats			Hacking & unauthorised intrusions				
					Ddos Attacks				
Electronic Currencies		cyber-finances				money laundering			Fraud Act 2006

Refinement of Model: Stage 2

Decision taken to play down permeability between on & offline offending

Use a more common distinction used as central basis of the model:

Computer ***dependent*** crime v Computer ***enabled*** crime

Potential problem: -

confuses nature of technological contribution to criminal agency?

All forms of technological agency involve ‘enablement’ (ie extension)

	Digital tools & non-digital targets		Victims			Key Legislation
			Private (individual)	Private (business)	Public (govt/other)	
Computer Enabled Offending	Crimes against the Person - Violence	Cyberbullying	x	-	-	Protection from Harassment Act 1997, Communications Act 2003, Criminal Justice Act 1994
		Stalking	x	-	-	
		Hate Speech/Trolling	x	x	x	
		Defamation	x	x	x	Defamation Bill 2012
		Terrorism	x	x	x	
	Crimes against the Person: Sexual Offending	grooming	x	-	-	Sexual Offences Act 2003, Protection of Children Act 1978
		obscene materials	x	-	x	
		trafficking	x	-	-	
	Financial & Property Crime	Fraud	x	x	x	Fraud Act 2006
		IP Theft	x	x	x	Digital Economy Act 2010, Data Protection Act 1998
	Digital tools & Digital targets					
Computer Dependent Offending		Data-Theft	x	x	x	Data Protection Act 1998
		Malware distribution	x	x	x	Computer Misuse Act 1993, Privacy and Electronic Communications Regulations 2003, Data Protection Act 1998
		spam	x	x	x	
		Ddos & disruption	x	x	x	

Measurement, Data & Threat

- Having organized data into a workable typology further questions about how organise data in terms of threat
- That is - best metric to use as basis of threat evaluation

(i) Cost ?

(ii) Prevalence?

- Problems with the former - for example questions about (2011) Cabinet Office/Detica measure of £27bn
- Attempts to fix this remain problematic (though figure still circulates)
- CF Anderson et als (2013) suggestion – avoid overall ‘single cost’ measure, for category oriented measures. Scaled down global measures relativised to UKs c5% of global GDP
- **BUT** relies on accuracy of the global estimates used and assumption that the relative proportion of an offending category in the UK is always equal in cost to its proportionate GDP
- Is there any ‘point’ to cost measures - what would they help us do?
- Report largely concentrated on prevalence measures

Key Sources Used

I. Prosecution & Conviction Data

II. Police data

III. Academic Research & Survey Data

IV. Industry Data

V. Victim Reports

Note - very little from reported sources - will come back to reasons for this later

Structure

Methodological requirement for best quality data only and large amount of data to cover meant final report included only:

Summary/Overview chapter

Chapter on Computer Dependent Crime

Chapter on Enabled Crime (I) – Fraud

Chapter on Enabled Crime (II) – Sex offending

Chapter on Methods, Measurement and how to improve evidence base

Missing Themes

This resulted in several areas where data was less good that were omitted.

IP theft…. (property crime)

Stalking…. (sex offending)

Political activism & terrorism

Online hate crime

State & Corporate Cybercrime

Data breaches and compromises

Offence hybridisation - blurring between on-offline offending – increasing use of digital technologies to facilitate ‘standard’ crime - eg quasi-legal/illegal online markets drugs, sex, gambling ; pin code violence;

Computer Dependent Crime – Findings

Regular warnings of serious threat posed by CDC

“..Cyberattacks are increasingly representing the most serious threats to homeland security and in the next decade will likely eclipse the risk posed by traditional international terror organizations.”

James Comey, Director FBI November 2013

Expectations were this would translate into significance prevalence measures of CDC

And, given this is the ‘easiest’ cybercrime to measure, expectation was that sources on CDC would converge…

Prosecution Data

Computer Misuse Act 1990	2007	2008 (note 2)	2009	2010	2011	2012	Total
Proceeded against	19	17	19	10	11	25	101
Found guilty	10	12	10	18	11	27	88
Sentenced	9	13	10	18	11	27	88

Hacking & Misuse of Computers

Counterintuitive? Why were levels so low?

(1) Recording issues: -

Hacking and other stuff recorded as criminal under other offences such as Fraud

- 45,687 individual sentenced under Fraud Act between March 2011- 2012
- But this data does not record cyber component
- Sending a phishing email does not necessarily involve a hack (phishing rising, most common type of fraud.

(2) Poor Policing?

(3) Under-reporting - in 2006/7 according to CSEW only 1% of hacking victims reported this to police

(4) Not as major a problem as usually thought?

Computer Dependent Crime – Victim Data (I)

	A computer virus (%)	Unauthorised access to/ use of personal data (%)	Upsetting/ illegal images (%)	Loss of money (%)	Abusive/ threatening behaviour (%)	One or more negative incidents online (%)
All internet users 2010/11 (unweighted base = 8,383)	33	6	4	3	2	39
All internet users 2011/12 (unweighted base = 8,373)	31	7	4	3	2	37

Victim data: Experience of Viruses 2002-2012

2002/3	2003/4	2004/5	2005/6	2006/7	2007/8	2008/9	2009/10	2010/11	2011/12
18%	28%	-	41%	36%	-	-	-	33%	31%

Source: Crime Survey for England and Wales

In 2002/03 the question asked: "Has your HOME computer been affected by a computer virus?" In 2003/04–2006/07 the question asked: "Has your home computer been damaged by a virus, [or] been infected by a virus but not actually damaged?" In 2010/11–2011/12 the question asked: "Have you personally experienced a computer virus?"

- Peak in 2005?
- Gradual downward trend?

Industry Data (I)

- These ostensibly declining rates of infection different to picture presented in industry data
- EG
- Symantec (2012) for example, reported blocking 5.5 billion ‘attacks’ in 2012, an increase of over 81 per cent from 3 billion reported blocks in 2010
- Detected 403 million unique variants of malware globally in 2011, compared with 286 million in 2010.
- BUT Variations repeat when we compare scientifically conducted surveys with industry data....

Computer Dependent Crime – Non Industry Data

	Manufacturing (%)	Wholesale and retail (%)	Transportation and storage (%)	Accommodation and food (%)	All four sectors
Hacking	4	1	1	1	2
Phishing	0	0	0	0	0
Theft of money (online)	1	1	1	0	1
Theft of information (online)	0	1	0	0	0
Website vandalism	0	0	1	1	0
Computer virus	11	6	9	4	7
All online 'crime'	12	7	10	6	8

Proportion of business premises that experienced online 'crime' in the last 12 months, by industry sector, 2012

Source: Commercial Victimisation Survey

Computer Dependent Crime – Observations

- This more positive view corroborated by other measures indicating UK fares well compared to other countries? EG
- Sophos (2013) “Threat Exposure Rate” (% of PCs experiencing a malware attack over 3 months) showed UK ‘4th safest country at 4%. (Norway 1st at 1.8%; Indonesia 23.5%)
- Pandalab (2012) ‘Average infection ratio’ (average number of infected PCs) located UK at 37 out of 44 countries sampled. Ratio of 23% compared to average of 30%
- Kaspersky (2011) reported that the UK was subject to less than four per cent of total DDoS attacks globally.
- Symantec (2013) reported that globally, spam fell from 75 per cent of all email in 2011 to 69 per cent in 2012
- Is is a threat which is stabilizing/declining?
- individuals more at risk than businesses?
- Does the mismatch imply significant gaps in the findings & knowledge base between types of data (victim, prosecution private sector etc)

Computer Dependent Crime – Analysis & problems

- In official data rises and falls may be affected by different wording of survey questions
- Misunderstandings and lack of technical understanding amongst policing agencies
- Heavy dependence upon security industry for knowledge but:

  - often unclear methodology

  - different providers often use different terminology, (eg malware family names) inhibiting comparison

  - different metrics: *infection*; *average infection rate; threat exposure rate; amount of malware in circulation;*

  - Many measures global – not national

  - Vested commercial interests of security
- Access to key datasources around CDC very difficult. Commercial/Private sources cite reputation and commercial sensitivity issues (cf BRC)
- States cite national security concerns
- Numbers of virus infection or Ddos attacks is not a measure of crime, or of harm. Number of virus infections not a measute of offender prevalence

Indicators and their Reliability

Confusions between ‘measures’ and ‘data’ - measurement styles appear to profoundly distort findings

Measures NOT = Threat

Threat NOT = Crime

Crime NOT= Threat

Very limited data on ‘better’ potential measures such as victim, perpetrator, complexity and mode of tool use, etc

HO decision not to use ‘cost’ meant key indicators were based on prevalence measures

But do prevalence measures function as the best way of providing knowledge of cybercrime?

Is Prevalence a useful Measure of Cybercrime threat?

(1) Problems with obtaining accurate prevalence measures

(2) Prevalence a ‘thick’ rather than a thin measure (cf epidemiology where distinctions are made between ‘point prevalence’; ‘period prevalence’ etc)

(2) Dependence upon recorded crime - or on methodologically suspect private sector measures

(3) Double counting an issue - might be included under other offences, or counted twice (eg images from 1 URL, or virus infection)

(4) Prevalence might not reflect harm

(5) Prevalence does not reflect key aspects of cybercrime - eg comparative sophistication of computer misuse

Other measures?

If cost & prevalence flawed measures - what else could there be?

Ideally want measures that - at the very least - combines levels of harm (which may include financial cost) with other indicators offender type; victims; novelty; tool and means

Report recognised value of some of these, but indicated that any data scarce if not non-existent

Recording mechanisms to be partly improved - eg police definitions

Cybercrime indices?

Improving Data & its Evaluation (I) Reporting

- Clearly important to improve both quantity and quality of data and basis upon which it is evaluated if responses are to improve.
- Several ways of doing this

- More robust scientific/academic studies
- Better collection and retention of cybercrime data by police, security agencies, government and other parties
- Better reporting

- Will conclude discussion by considering some issues around the last option

Reporting Mechanisms - Options

- Can think of reporting mechanism in terms of several templates. In the UK these translate as follows:
- *Offence Based* : EG - Action Fraud Hotline, CEOP safety centre (for kids - up to 17), parents or carers
- *Agency Based* - Police - NCA hotline
- *Education/Information based* - Get Safe Online
- *Victim Based* – National Stalking hotline, Stop Hate UK
- These categories can crossover

Using Reporting Mechanisms - advantages

1. Data acquired from wider range of victim types
2. Data acquired about wider range of cybercrime offences
3. Data can be more nuanced and less compressed by offending categories
4. Data up to date and relevant
5. Data can indicate new or as yet undetected trends

Using Reporting Mechanisms - problems

Lack of confidence by public

Failure to report

Lack of awareness of victimhood

Business and other sensitivities

Issues around security

Quality of data highly variable (open to misreporting; omission, misinterpretation)

Inconsistencies across different reporting media

Reports can be affected by the media which is used

Many reporting facilities (esp victim based) are poorly funded

Reporting Mechanisms – Measures of success

- Urgent comparative research needed
- Better integration and data sharing across mechanisms

Conclusions (I) : Evaluation & Data Access

(i) *Major difficulties in evaluating threat*

- Questions about how much the ‘cyber’ component the real threat
- vague conceptualisations of threat and poor evaluation of comparative threat

(ii) *testing difficulties in obtaining good data*

- Few established conventions as yet about recording crimes as ‘cyber’
- Inconsistent metrics and indicators as a result
- Many police indicators that do exist have been inconsistent with industry based, prosecution based or victim based metrics
- Data loss resulting from changes in specialised agencies and personnel (from NHTCU to SOCA to NCA)
- Commercial sensitivity and unwillingness to share a common problem
- Fear of legislation – eg DP Act
- Difficulties in use of reporting mechanisms

Conclusions (II) New Cybercrimes?

The Review - and similar evaluations not only face difficulty of good data around many ‘standard’ categories' of online crime – eg stalking

Problems around attempt to keep up with emerging categories - EG

Online drugs markets

Hate Crime

Human Trafficking

But also major gaps in evaluation of more complex, more ‘cyberspecific’ offences

E.g. virtual currencies like BitCoin

Use of gaming & online environments to further criminal activity

Misuse of surveillance powers within virtual environments

Conclusions (III) ; General reflections

Overall the Review a worthwhile exercise, - at least to set an epistemic baseline for future work

BUT

Inherent flaws in Governmental measures of Ccycrime revealed

Tiny number of offences looked at

predictable set of offenders

No recognition of wider range of perpetrators involvement in cybercrime

No real sense of wider public concerns raised by offences

Failure to understand criminological continuities between human and technical causation

Failure to incorporate new social valorisations like information & privacy

Thank you

Dr Michael McGuire

m.mcguire@surrey.ac.uk