Measuring online financial and economic crimes within the context of other statistical reforms

PROFESSOR MIKE LEVI

CARDIFF UNIVERSITY

LEVI@CARDIFF.AC.UK

VIRTUAL STRASBOURG 2020

Why measure and *What* to measure?

- The challenge of newly criminalised acts
  - Online stalking, malware/ransomware, money laundering, transnational bribery, eco/wildlife crimes
- The challenge of changing forms of criminality
  - From local to global victim-offender relationships
  - Crimes without specific individual or business victims
  - Crimes with victims in multiple countries
- The politics of (non)measurement
- Measures of frequency
- Measures of multiple victimisation
- Measures of cost and harm
  - Does harm include fear (e.g. fear of cyber?)
- Deconstructing and dismantling hype

Reform Efforts (USA)

- US *Modernizing Crime Statistics* mainly fights classical wars against the narrowness of Uniform Crime Reports
  - Neglects cybercrimes & offline fraud, money laundering
  - The proposed classification includes a list of behavioral definitions (and code/reference numbers) that is meant to evoke "familiar" classification schema, but it includes as a coequal part of the overall classification a set of detailed attributes of the incident itself, and of the victims, the known perpetrators, and the relationship between the victim and the offender
  - Very little follow up/implementation under the Trump administration so still just personal identity fraud covered by the NCVS and separate from the general victimization survey. No corporate or government cyber victimization survey efforts or reforms to official data.
  - the FBI has committed to moving entirely to National Incident reporting at the end of January 2021 even though many police departments are unable (or unwilling) to make the switch. BJS estimates that nearly a quarter of US police agencies could end up trading the ability to report solid, local data for inclusion in the Uniform Crime Report for “national estimates” for offenses that occur after January 1, 2021 (2019.2 NIBRS User Manual)

Reform Efforts (non-US)

- "Fraud: Almost all countries provided data on fraud, although only a few of them could adopt the standard definition. Due to different definitions the rate per 100 000 being reported varied greatly (mean rate 179, ranging between 4 and 1219)" *European Sourcebook*, 2014
- Eurostat crime data – largely absent
- UK – cybercrime and fraud v individuals and business (but not government), data breach surveys, UK Finance (card fraud)
- Australia - Identity crime & misuse in Australia, ACSC, ACCC scams
- ICCS - the *Cybercrime-related* (Cy) tag serves to identify various forms of crime committed with the use of a computer (e.g. internet fraud, cyber-stalking or violation of copyright through electronic dissemination)
- the *Geographical location* (Geo) tag enables the regional location of the crime within the country and identifies crimes recorded as "extraterritorial" crimes
- Private sector surveys (e.g. antivirus firms, Deloitte, PwC)

EVENT DISAGGREGATIONS	VICTIM DISAGGREGATIONS	PERPETRATOR DISAGGREGATIONS	DATA DESCRIPTIONS/INCLUSIONS
At – Attempted/Completed	**SV** – Sex of victim	**SP** – Sex of perpetrator	**Th** – Threats included
We – Type of weapon used	**AV –** Age of victim	**AP** – Age of perpetrator	**AA** – Aiding/abetting included
SiC – Situational context	**STV** – Age status victim (minor/adult)	**STP** – Age status of perpetrator (minor/adult)	**Ac** – Accessory/accomplice included
Geo – Geographic location	**ViP** – Victim-perpetrator relationship	**ViP** – Victim-perpetrator relationship	**CP** – Conspiracy/planning/ preparation included
DaT – Date and time	**Cit** – Citizenship	**Cit** – Citizenship	**In –** Incitement to commit crime included
Lo – Type of location	**LS** – Legal status of victim (natural/legal person)	**LS** – Legal status of perpetrator (natural/legal person)	
Mot – Motive	**Int** – Intoxication status of victim	**Int** – Intoxication status of perpetrator	
Cy – Cybercrime related	**ES** – Economic sector of business victim	**EASt** – Economic activity status of perpetrator	
Rep – Reported by		**Rec** – Recidivist status of perpetrator	

Disaggregation data ICCS

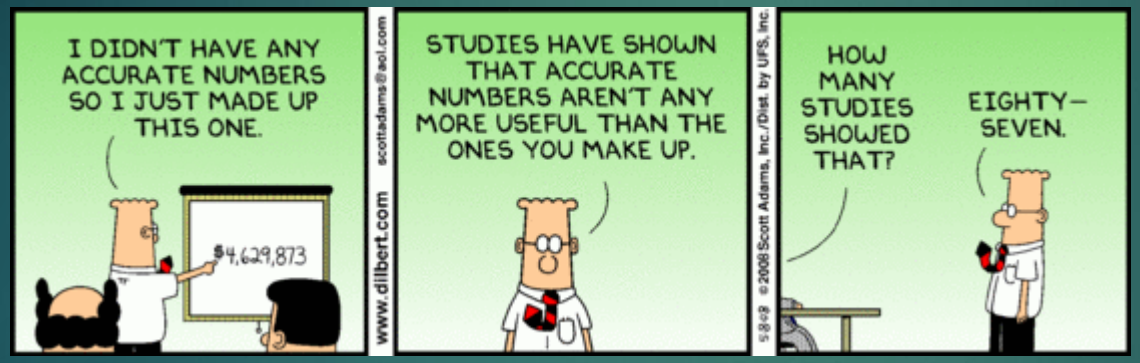
SECTION 07	ACTS INVOLVING FRAUD, DECEPTION OR CORRUPTION		
0701 Fraud Obtaining money or other benefit, or evading a liability through deceit or dishonest conduct.		+	**Inclusions:** Mortgage fraud, financial fraud, quackery, impersonation, identity theft; possession, creation or use of false weights for measure; apply all inclusions listed in 07011 - 07019
		-	**Exclusions:** Obtaining money without dishonest conduct but with intent to withhold it from the owner (0502); fraudulent insolvency, insider trading and other acts against commercial financial regulations (08042); electoral fraud (08079); illicit enrichment (07035)
07011	**Financial fraud** Fraud involving financial transactions for the purpose of personal gain. This includes using financial consumer products such as bank accounts, credit cards, cheques, store cards or online banking systems. - Fraud as defined in 0701.	+	**Inclusions:** Bank fraud; investment fraud; cheque/credit card fraud; store card fraud; online banking fraud; writing bad cheques; apply all inclusions listed in 070111 - 070112
		-	**Exclusions:** Financial transactions to conceal, transfer or disguise the proceeds of crime (07041); embezzlement (07032); apply all exclusions listed in 0701
070111	**Financial fraud against the State** Financial fraud against the State. - Financial fraud as defined in 07011.	+	**Inclusions:** Procurement and contractor fraud; false claims fraud not amounting to medical fraud
		-	**Exclusions:** Social welfare and tax fraud (08041); apply all exclusions listed in 07011
070112	**Financial fraud against natural or legal persons** Financial fraud against natural or legal persons.[99] - Financial fraud as defined in 07011.	+	**Inclusions:** Mortgage fraud; securities fraud; investment fraud; bank fraud
		-	**Exclusions:** Apply all exclusions listed in 07011
07019	**Other acts of fraud** Fraud not described or classified in 07011. - Fraud as defined in 0701.	+	**Inclusions:** Possession, creation or use of false weights for measure; medical fraud or quackery not amounting to malpractice or medical negligence; fraudulent failure to supply consumer goods or obtaining goods by fraud; false accounting; hiding or destroying money; wire fraud; insurance fraud; unlicensed/unregistered practice in a trade or profession; identity theft; false representation of identity or professional status; impersonation; fraudulent pretence of marriage; setting up or operating a pyramid scheme; swindling
		-	**Exclusions:** Financial transactions to conceal, transfer or disguise the proceeds of crime (07041); embezzlement (07032); illicit enrichment (07035); tax fraud (08041); apply all exclusions listed in 0701

Some threats and responses

- **The variegated threat landscape from cyber/cryptocurrencies**
  - **Threats of what to whom by whom? *Harms* of what to/by whom?**
- **Cyber security 'the new frontier of warfare, espionage'**
  - **From NATO responses to Internet of Things connected threats**
- **The growing elision between national and human security**
- **Incidence, damage, fear, concern, and how firms & individuals carry out cost-benefit judgments in practice**
  - Easier to design in relevant data at reporting stage than afterwards
  - Who and how many use Uber/Facebook/Equifax/Marriott/BA etc. less now than before *revelation* of data breaches?

How much e-crime & what kinds?

- **Guesstimates of the cost of cybercrimes (controversial)**
- **Why is knowing how much money/harm or what proportion of a population – or sub-groups – are victims important?**
  - The problem of 'facts by repetition



- Are past trends much guide to the future?
- Data breaches and collateral damage/corruption opportunities
- What can the Council of Europe do to assist data collection