Counting Cybercrimes Reduction: Deterrence, Diversion, & Desistance

MIKE LEVI, PROFESSOR OF CRIMINOLOGY, CARDIFF UNIVERSITY

LEVI@CARDIFF.AC.UK

STRASBOURG VIRTUAL 2020 COUNCIL OF EUROPE CONFERENCE

Goals for Today

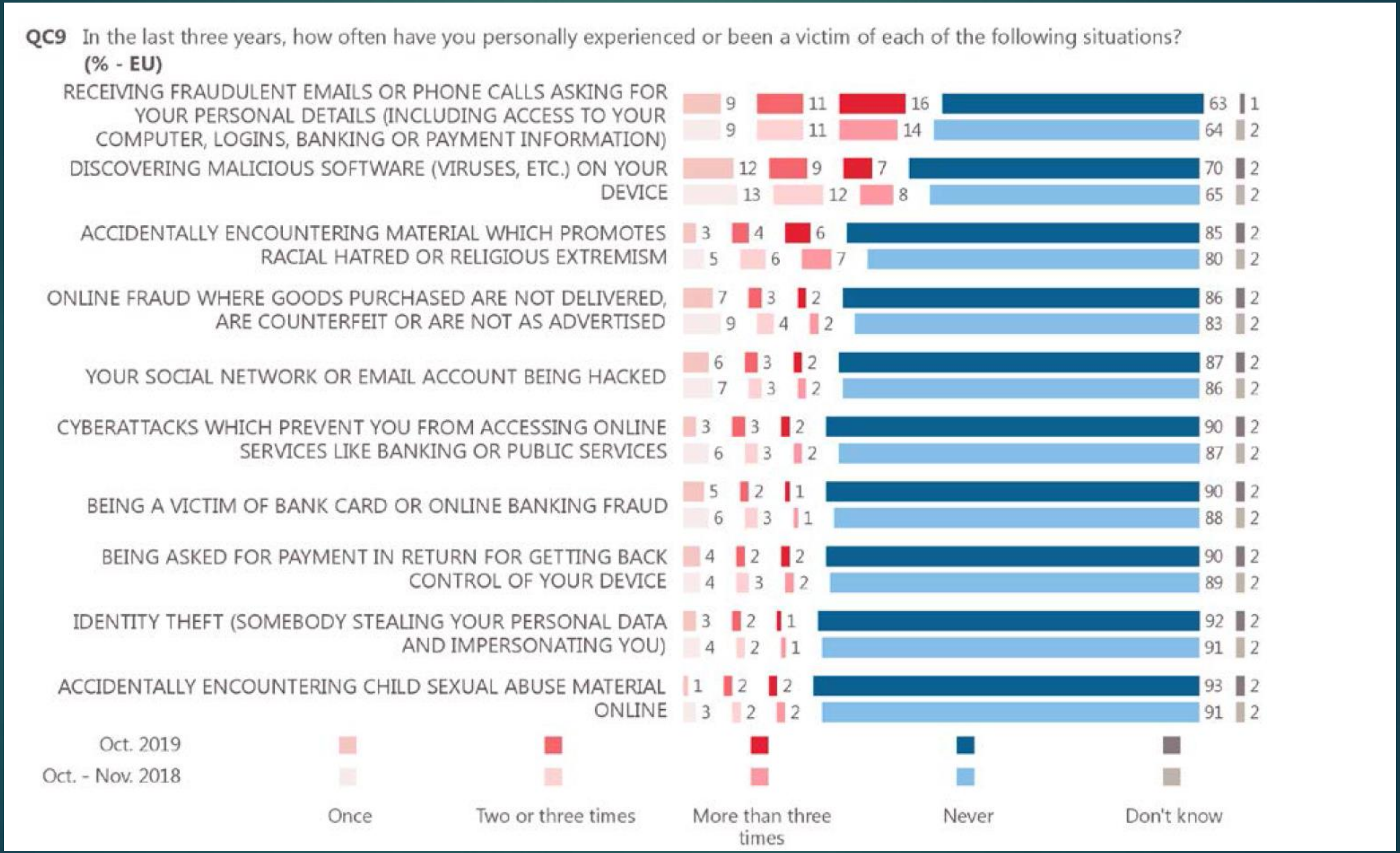
- Government strategies have involved adapting counter-terrorism control models to all serious and organised crime, including cyber-enabled crimes
- The aim is to re-examine public policing and public-private partnership policing to consider what may be required to 'satisfice' cyber crimes reduction and harm: victimisation, repeat victimisation, & fear of cyber scams
  - Nobody in authority believes we can prosecute our way out of *any* online crimes – but public wants 'justice'?
- And to summarise key features of deterrence, diversion and desistance from cybercrime in the light of poor criminal careers data
  - the dark figure of unreported crimes & unprosecuted offending, plus the cross-border dimensions of both
  - Need to take account of civil and administrative sanctions

The Four Ps CT Model

- Prevent – leading people away from path of vice
  - Ill-understood terminology outside Counter-Terrorism
- Pursue – traditional police and criminal justice
- Prepare – primary prevention
- Protect - resilience after first strike

- Rolled out to all 'Serious and Organised Crime' & Cyber
- This is just a typology – tell us nothing about what to prioritise, given scarce resources. CT and some 'organised' and 'cyber' crimes are high drama – but the rest are usually not pursued. Even in legality principle countries.

Prevalence Personal Cybercrimes EU 2020



QC9 In the last three years, how often have you personally experienced or been a victim of each of the following situations? **(% - EU)**

Current non-Police Initiatives in the UK (adapted by EU 2013)

- National Cyber Security Centre
- WARP (Warning, Advice and Reporting Points)
- Cyber Security Information Sharing Partnership (CiSP)
  - ‘Fusion Cell’ analyse cyber threats and inform partners
- Get Safe Online and other general public prevention
- Private sector selling prevention and post-strike investigation and protect services (market failure in which services are better or worse?)

Current Police Initiatives in the UK

National Crime Agency

- **CEOP Command**
  - Coordinates child protection online and offline
- **Economic Crime Command**
  - Money laundering; International corruption; Fraud; Counterfeit Currency
- **National Cybercrime Unit – cyber-dependent crime**
  - Investigate; Target hardening; Intelligence; Partnership

Action Fraud & National Fraud Intelligence Bureau (City of London Police) – for online and offline **fraud** reports

NCSC – phishing reporting nationally (report@phishing.gov.uk)

Met Police Cybercrime Unit (Falcon)

- Malware; Phishing; Hacking; DoS; IP theft; Fraud

Regional Organised Crime Units (ROCUs)

Force level Economic Crime and Cybercrime units

Public/private partnerships

Explanations for poor cooperation (and consequently poor offender data):

-over-crowded cybersecurity space

-criminal justice system's poor record in apprehension and prosecution

-inhibiting legislation and historically poor engagement with SMEs

-difficult to justify a business case for spending in austere times

-low levels of network capital

-Low police valuation of fraud and digital crime

- (see HMICFRS reports 2016-2019)

Some ambitions and key questions

- ‘Effective, proportionate and dissuasive’ sanctions – does this mean anything when data are so poor across Europe?
- What role for Prevent in reducing willingness to participate and increasing whistle-blowing? Money mules & hackers
- Incapacitation – ‘putting funds beyond use’!
- Deterrence – deterring whom from what?
    - Front-line offenders & their networks (some or all planned offenders need jail?) What if they are in Russia or China?
    - Criminal commercial enterprises (fronts & mixed) – no jail
    - Commercial enterprises/professionals that facilitate crimes of others: but who wants to prosecute or injunct Google or Facebook for selling adverts paid for by crime proceeds?
    - Differentiate organisational from individual impacts

Deterrence

- Risks of detection and intervention more important than sentences per se
  - But for highly profitable crimes, need to consider other 'rational choice' factors
  - Low prosecution rates for all online offences – need to take account of attrition rates
- Confidence fraud
- Possessing, making or supplying articles for use in fraud.
  - 'Articles' include any electronic programmes or data stored electronically
- Online hate and other cyber offences/National security threats
- In Sentencing Council England & Wales research (2013), perceived aggravating factors broadly agreed on by stakeholders included circumstances where the fraud:
  - had a considerable financial impact on the victim
  - was premeditated and showed careful planning
  - had involved an apparent abuse of trust/authority
  - involved repeated contact between the perpetrator and victim, and included complex or insidious perpetration strategies
  - involved considerable harm to the victims (both intended and actual)
  - affected a high number of victims
  - targeted vulnerable victims
  - involved a perpetrator who was a repeat offender & showed high level of intent

Mentoring

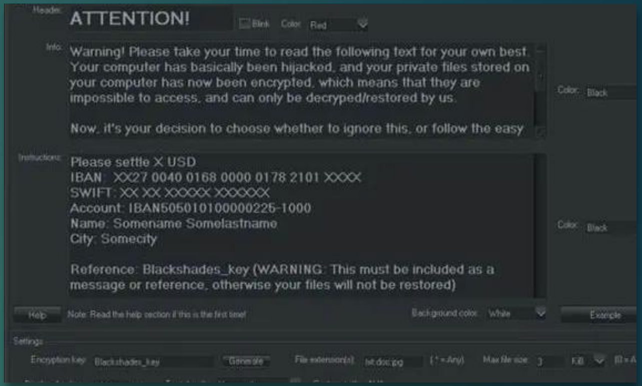
- No evidence directly on effects on cybercrimes
- While only little is known about the offender profiles of cyber-offenders, different from other forms of delinquency.
- Some malicious cyber-offenders do have histories of familial or adjustment problems, but less linked to routine exposure to violence, abuse, drug and alcohol use, or having parents in jail.
- Cyber-offenders more likely to show narcissism, anxiety, and depression, as well as lack of empathy and ethical flexibility – maybe like some politicians?

Targeted warnings/cautions

- The intention of targeted warnings is to deter recipients from beginning or continuing offending, by communicating the cost to their activities, and a consequence if they continue down a criminal pathway. Two key theoretical perspectives underpin intervention: deterrence and labelling
- Avoiding stigma and economic consequences of criminal record (and saving prosecution and court time!)
- Sanctions that focus on the wrongfulness of (and harm caused by) the act, rather than the characteristics of the offender, are more likely to reduce crime.
- Targeted warnings can prevent crime if the recipient perceives: (a) the warning is fair; (b) the cop or civilian who delivers the intervention is acting rightfully; and (c) the intervention is focused on the act rather than the actor
- Although cease-and-desist visits and targeted prevention messaging have been used in the context of cybercrime, there is little known about how effective they are

Some UK examples

- In 2014, UK-wide police investigation into *Blackshades*, a remote access tool designed to take over, control, and steal information from personal computers. 17 people arrested and 80 received a visit from a police officer. Approx 500 others received a warning letter advising that it was believed they had purchased the software and that using it could be illegal
- In 2015, the database for the *LizardStresser* booter service, which provided DoS attacks for a fee, was compromised and leaked, containing customer details for those who had purchased attacks. Six purchasers arrested. 50 others who had registered with the site, but were not believed to have carried out an attack, received a home visit from the NCA, and were told that denial of service attacks are 'illegal, can prevent individuals from accessing vital online services, and can cause significant financial and reputational damage to businesses'. They were also informed that 'committing cybercrime can result in severe restrictions on their freedom, access to the Internet, digital devices and future career prospects'



Header: ATTENTION!

Color: Red

Info: Warning! Please take your time to read the following text for your own best. Your computer has basically been hijacked, and your private files stored on your computer has now been encrypted, which means that they are impossible to access, and can only be decryped/restored by us.

Now, it's your decision to choose whether to ignore this, or follow the easy

Color: Black

Instructions: Please settle X USD
IBAN: XX27 0040 0168 0000 0178 2101 XXXX
SWIFT: XX XX XXXXX XXXXXX
Account: IBAN505010100000225-1000
Name: Somename Somelastname
City: Somecity

Reference: Blackshades_key (WARNING: This must be included as a message or reference, otherwise your files will not be restored)

Color: Black

Note: Read the help section if this is the first time!

Background color: White

Encryption key: Blackshades_key

File extension(s): txt doc jpg

Max file size: 3

Warning letters (cont)

- In 2016, Europol's EC3 coordinated Australia, Belgium, France, Hungary, Lithuania, the Netherlands, Norway, Portugal, Romania, Spain, Sweden, the UK, and the USA. Overall, 34 arrests, 101 suspects interviewed and cautioned
- many types of cybercrime are committed for money or peer recognition, so well-targeted cautions that increase offenders' perceived risk of detection could work
- likelihood of detection, not the severity of punishment, matters to many cybercriminals, so warnings highlight that low-level offenders are not necessarily anonymous online, increasing the perceived likelihood of detection.
- Other offline research shows positive effects of warning letters on general populations, both randomly allocated and without. So no evidence of follow up or impact, but this is promising
- But care needs to be given, since personally administered warnings about behaviour that is seen to be legitimate may generate defiance and more delinquency in future

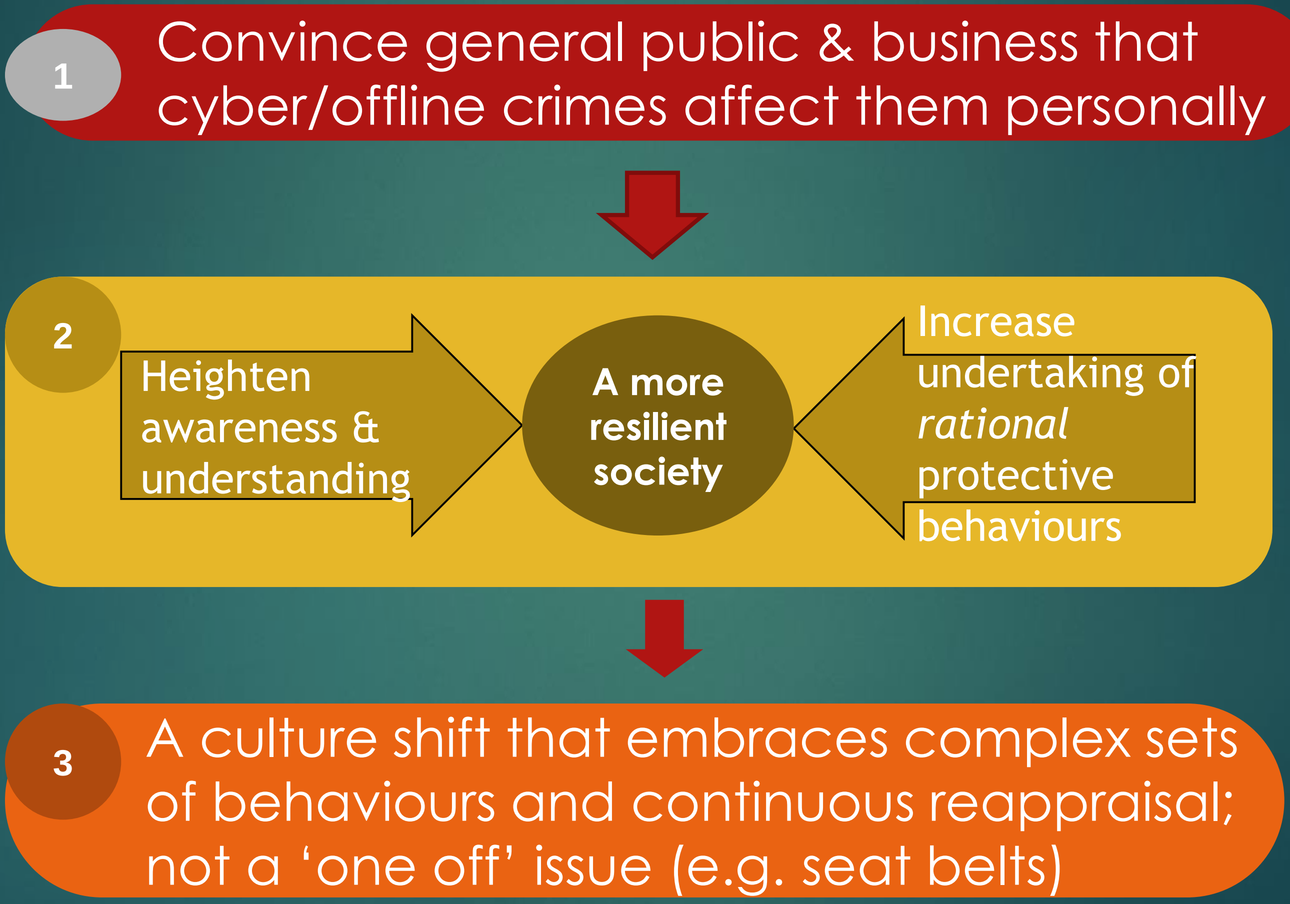
Positive interventions

- Diversion evidence is weak for cybercrimes
- Positive diversion programmes attempt to redirect or transform criminal behaviour into noncriminal behaviour, not suppress it entirely. Youth who engage in illegal graffiti may be diverted into a programme that encourages legal 'urban art': accepts and leverages the motivation for committing crime and provides a legitimate (even profitable - Banksy) means to express it
- But some experiments e.g. with car thieves/speeding have ***not*** worked well & need to divide high and low risk (re)offenders
- No empirical evidence conclusively proving the effectiveness of such positive diversions in cybersecurity (except Mitnick etc in consulting), but may be worth trialling and evaluating. However, security risks may make it difficult to obtain support from industry or police for such schemes
- Challenge to keep offenders away from negative online influences
- Challenge the justifications used by cyber-offenders through moral reasoning and cognitive restructuring might help: But no-one knows how this works/does not work in China, Romania or Russia (Nigerian evidence)
- Desistance evidence depends on good data about cyber careers

Efficiency, Effectiveness and Legitimacy

- What are our goals and are they prioritised?
  - **Crime or serious harm reduction: how tight a focus?**
    - The *Jihad* against 'crime enablers': an inconsistent effort
  - **Satisfying the public we are punishing very bad people**
    - Local/global offenders, and the crisis in cross-border justice
  - **Getting value for money**
    - What are the costs and benefits, and who should/will pay?
    - Is there an optimal mix of prevention & prosecution efforts applicable to cyber/organised crimes across the board?
  - **Confusing effectiveness with efficiency**

The challenge for Government, police and ‘nudgers’



1

Convince general public & business that cyber/offline crimes affect them personally

2

Heighten awareness & understanding

A more resilient society

Increase undertaking of *rational* protective behaviours

3

A culture shift that embraces complex sets of behaviours and continuous reappraisal; not a ‘one off’ issue (e.g. seat belts)

Some models for action

- The targets for cyber-fraud/extortion are very widespread
- Need more understanding of teachable moments to divert offending
  - But can we do that credibly overseas?
- Prevention (i.e. Prepare and Protect) should be built-in with minimal effort or administered in a more bottom-up way through peer groups, community level bodies and charities, to help individuals and SMEs adopt easy security processes – to expect regular efforts from them is unrealistic

Some Thoughts for the Future

- Offline and online strategies differentiated
- Disruption strategies – including take-downs of websites, botnets and dark markets – reduce harm, especially if websites are taken down early
  - but they rapidly re-emerge, though we know little yet about the longer-term signalling and market reduction effects of these ‘whack-a-mole’ measures
- Scope for experiments, e.g. warning ‘pop ups’ on screen for those who fall victim to offers that could have been fraudulent or fake, though need careful management of media concerns.
- More focused Internet Governance could deal with these Global Bads, but the politics of international opportunity reduction are very hard to achieve.