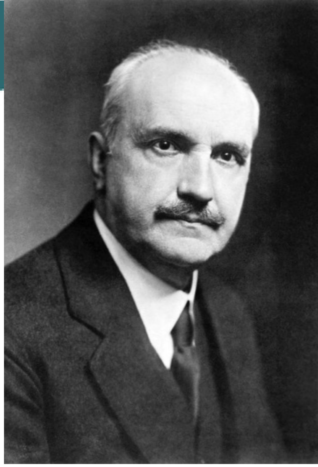
Australian Government
Australian Institute of Criminology

ECPR General Conference

The development of cybercrime: past, present and future

Dr Russell G Smith
Principal Criminologist



Outline

The argument

- ‘those who cannot remember the past are condemned to repeat it’ (George Santayana in *The Life of Reason* 1906)
- Could the opportunities for organised crime created by technology have been avoided or lessened in their impact had decision-makers been aware of developments in the past and been willing to act on them?

Understanding the trajectories of cybercrime

- How have information and communications technologies developed?
- What opportunities for organised crime have been created as a result?
- What lessons from the past have been unknown, forgotten or ignored?
- What lessons from the past have been successfully acted upon?
- How can future organised cybercrime risks be avoided through reliance on knowledge of prior successful and failed initiatives?

Theoretical background

Opportunity-based ‘social’ explanations for offending

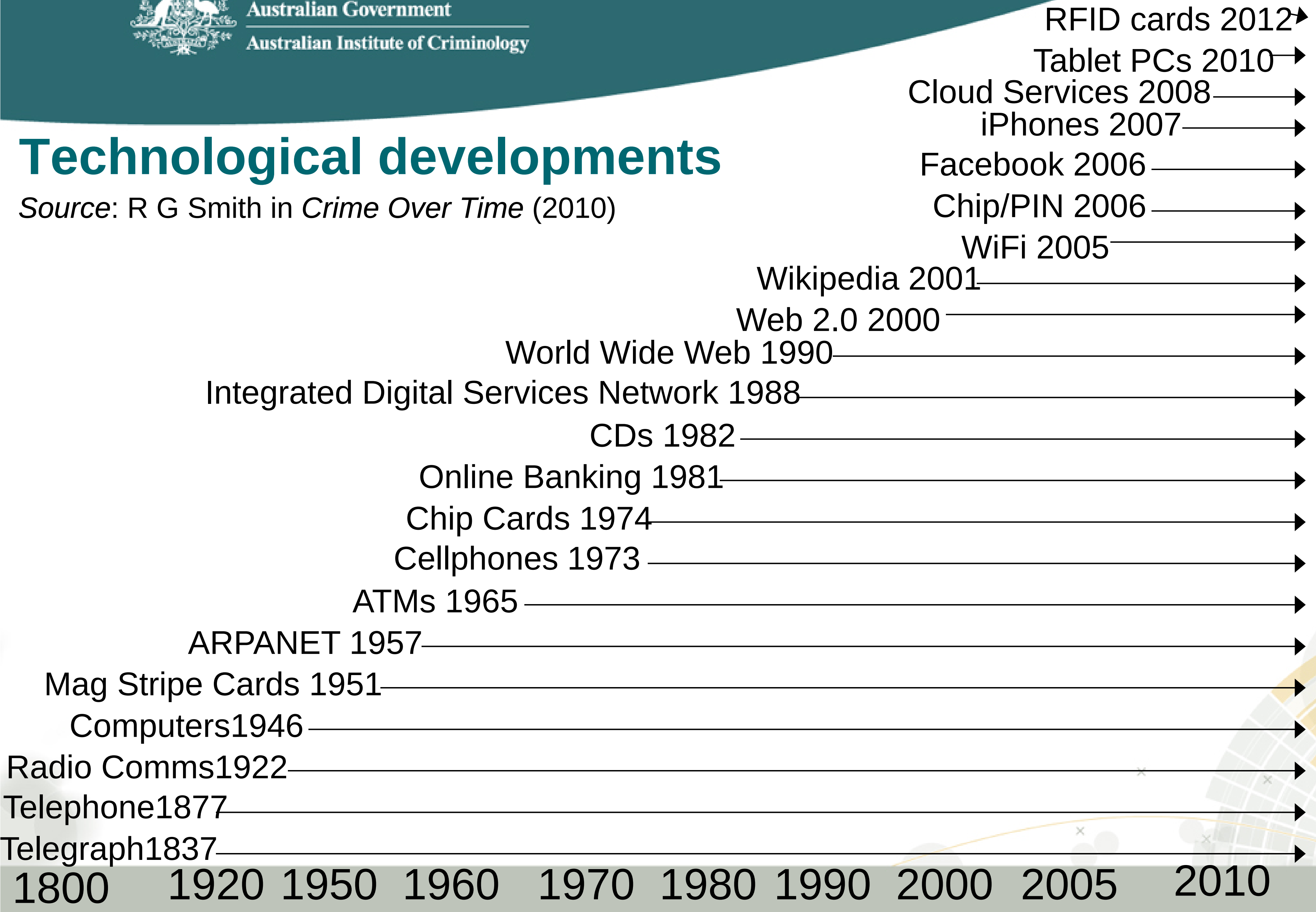
- Cloward & Ohlin (1960) *Delinquency & Opportunity* – location of individuals within legitimate and illegitimate opportunity structures
- Criminals simply make use of illegitimate opportunities that exist
- *Crime reduction* is achieved through enhancing legitimate opportunities and minimising illegitimate opportunities

Opportunity-based ‘situational’ explanations for offending

- Cohen & Felson (1979) *Routine Activity Theory* – predatory crime depends on the presence of motivated offenders, suitable targets, and the absence of capable guardians
- Emphasises criminal acts rather than individual factors
- *Crime reduction is achieved* by increasing the effort required to offend; increasing the chances of getting caught; reducing the rewards of offending (Clarke 1992), and neutralising offenders’ rationalisations.

Technological developments

Source: R G Smith in *Crime Over Time* (2010)



The generations of cybercrime

Telephony-based offending

- The use of telephony technologies to commit crime

Mainframe computer-assisted offending

- Low-level cybercrime involving the use of mainframe computers and their operating systems to assist traditional forms of offending such as theft of funds or information

Network-based offending

- Offending across computer networks, such as hacking and cracking activities

Automated global offending

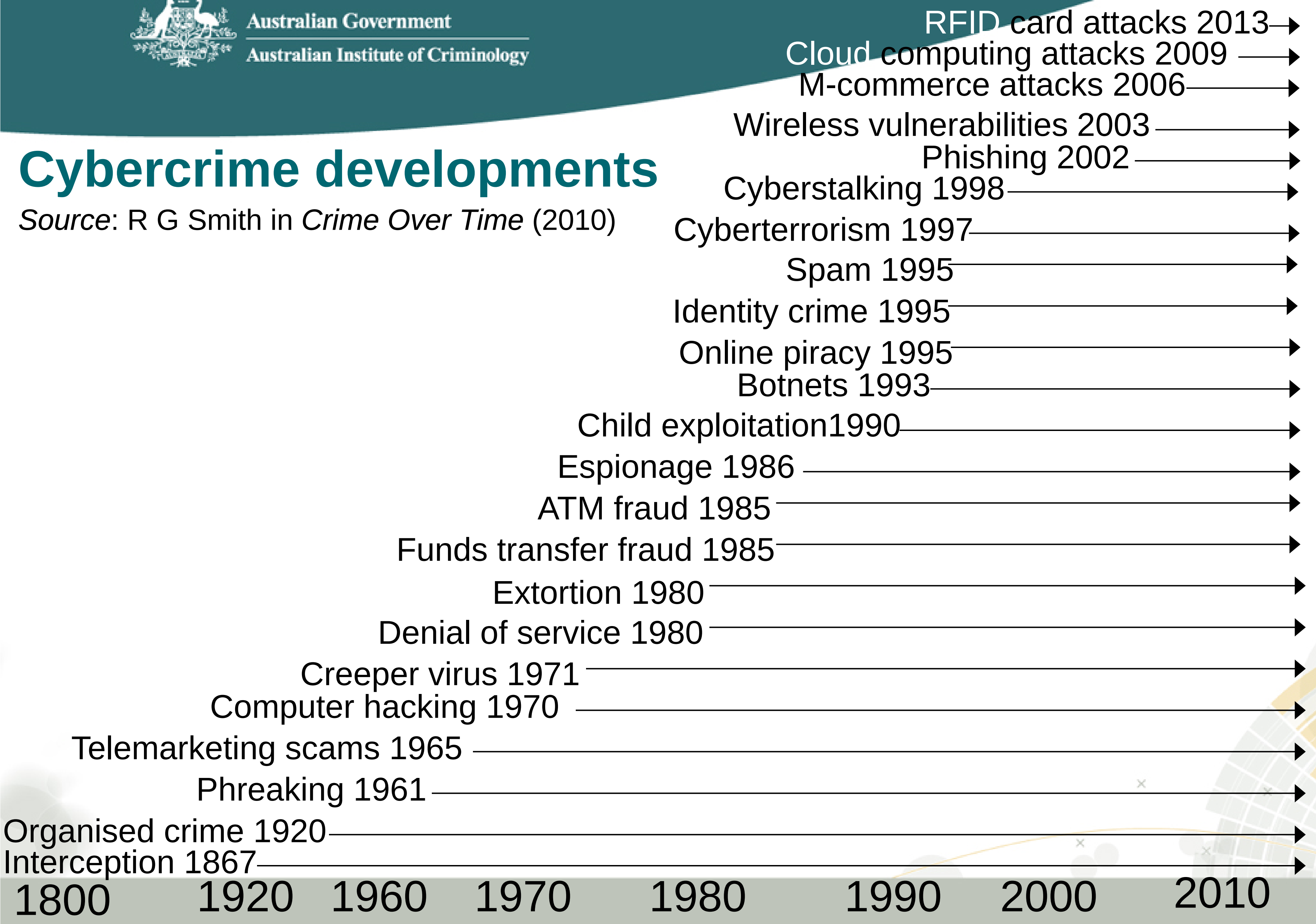
- Crimes wholly mediated by technology, being truly distributed and automated, such as occurs in the dissemination of spam using botnets
- Crimes enabled through mobile and wireless networks and the cloud

Derived from : David Wall “Criminalising Cyberspace” in *Handbook of Internet Crime* (2010)

Australian Government
Australian Institute of Criminology

Cybercrime developments

Source: R G Smith in *Crime Over Time* (2010)



RFID card attacks 2013
Cloud computing attacks 2009
M-commerce attacks 2006
Wireless vulnerabilities 2003
Phishing 2002
Cyberstalking 1998
Cyberterrorism 1997
Spam 1995
Identity crime 1995
Online piracy 1995
Botnets 1993
Child exploitation1990
Espionage 1986
ATM fraud 1985
Funds transfer fraud 1985
Extortion 1980
Denial of service 1980
Creeper virus 1971
Computer hacking 1970
Telemarketing scams 1965
Phreaking 1961
Organised crime 1920
Interception 1867

The limitations of routine activity theory

Creation of new opportunities

- Technologies introduced with undiscovered flaws
- Technologies with acknowledged flaws, too expensive to address

Changing motivations for offending

- Offenders exploiting vulnerabilities for curiosity and enhanced status
- Offenders with pathological, inter-personal motivations
- Offenders seeking financial reward
- Offenders with socio-political, religious and policy-driven motivations

Failures of guardianship

- *Individual* – Limited effect due to concern over invasion of privacy
- *Business* – Unwillingness to incur the costs of prevention
- *Government* – Under-resourced law enforcement and regulators

Continuing rationalisation of offending

- Awareness of rationalisations but inability or failure to address them

Based on: Cohen & Felson *Routine Activity Theory* (1979)

Phases in the adaptation of cybercrime attacks

Cybercrime type	Phase 1	Phase 2	Phase 3
Interception	Postal, landline	EMR scanning	RFID cards
Phreaking	Black box	PABX	VOIP, Skype
Consumer scams	Door-to-door	Telemarketing	Online, mobile
Funds transfer fraud	Bank transfers	Payroll, invoicing	Online banking
Malware	Experimental	Disruption/extortion	Terrorism
ATM attacks	Robbery	Contact skimming	Remote attacks
Phishing	Simple - trading	Government targets	Extortion DDoS
Identity crime	Personal crime	Banking and finance	Government
Cyber terrorism	Intelligence	Target investigation	Mobile detonation
Cloud computing	Illegal data access	Data manipulation	Extortion

Crime reduction employing knowledge of the past

Cybercrime type	Opportunities	Motivations	Guardianship
Interception	RFID screening	Open government	Early notification
Phreaking	Detection/blocking	Low cost / free calls	Identity checks
Consumer scams	Spam blocking	Full employment	EFT monitoring
Funds transfer fraud	Password control	Staff satisfaction	User verification
Malware	Firewalls, filters	Refusing ransoms	Data monitoring
ATM attacks	Target hardening	Early detection	ATM security
Phishing	Risk awareness	Early detection	Email scanning
Identity crime	ID security	Full employment	Online verification
Cyber terrorism	Precursor controls	Anti-radicalisation	Target surveillance
Cloud computing	Access controls	Early detection	Data monitoring

Cybercrime trajectories of the future

Technologies and typologies

- Smaller ICT devices, with increased data capacity
- Increasing bandwidth and data streaming capabilities
- Increasing demand for new ICT products and services
- Increased usage – globally including offender & victim locations

Offenders and targets

- Increasing financial motivations
- Increasing organised crime involvement
- Increasing business and government disruption
- Increasing cross-border activity and decreasing local focus
- Increasing numbers of victims and financial losses

Response capabilities

- Increasing user autonomy requiring self-regulation
- Decreasing government budgets and external regulation
- Decreasing private sector budgets for security and prevention

Conclusions

Lessons learned

- Hardware security to prevent theft; ubiquity of devices can reduce risk
- Malware controls from the cyber security industry
- Attempts to harmonise cybercrime policies and legislation

Lessons ignored

- User authentication risks – passwords, PINs, biometrics, multi-factor
- Data security – data loss and breaches; data storage in the cloud
- Marketing new ICT products in the knowledge of cybercrime risks
- Harm to victims and absence of victim support
- Failure to educate users concerning risks (computer driving licence)

A lesson for the future

The longer a technology is used, the more entrenched in life it becomes. When technologies are new, or are used in newer ways . . . their uses are easier to modify and their consequences easier to control. . . . If we wish to question the unintended consequences of these developments, now is the time to do so.

Source: *Ronnie Casella "The false allure of security technologies" in Social Justice (2003)*

Australian Government
Australian Institute of Criminology

Australian Government
Australian Institute of Criminology
CRC Criminology Research Council

Russell.Smith@aic.gov.au

Australia's national research and knowledge centre on crime and justice