Centre for Criminal Justice Studies
School of Law

UNIVERSITY OF LEEDS

The Cybercrime Ecosystem: The Challenges of New Pathways into Cybercrime

15th Biennial International Conference Criminal Justice and Security in Central and Eastern Europe, Ljubljana

Prof. David S. Wall,

d.s.wall@leeds.ac.uk

EPSRC (CRITiCal and EMPHASIS) Projects

Picture: https://www.pixelstalk.net/wp-content/uploads/2016/04/HACKER-hack-hacking-internet-computer-anarchy-sadic-virus-dark-anonymous-code-binary.jpg

Abstract

UNIVERSITY OF LEEDS

- New offender pathways into cybercrime are arising from the cybercrime ecosystem.
- The ecosystem facilitates cybercrime by supplying specialist skill sets that are rented by attackers to achieve their goals.
- The provision of these skillsets is creating new opportunities for potential offenders by luring them into cybercrime.
- Offenders either choose them as a career path or drift from less serious cybercrime offending.
- Cybercrime at a police and political level is no longer just about cybercrime, it also includes participation in the processes which enable to the cybercrime to take place.
- Each pathway needs to become a focus for Law enforcement

Outline of *The Cybercrime Ecosystem: The Challenges of New Pathways into Cybercrime*

UNIVERSITY OF LEEDS

1. Five new technological developments that have changed the cyberthreat landscape in the past 10 years.
2. New pathways into cybercrime and the uncertainties of anticipating offenders – using analysis of ransomware.
3. The implications for policing cybercrime in the second quarter of the 21st Century
4. Conclusions

1. Five new technological developments that have changed the cyberthreat landscape.

Five distinctive (new) technological developments have been popularised during the past decade or so which have increased the scalability and feasibility of cybercrime but also created new pathways into new types of cybercrime.

a) Cloud technologies - increased the overall functionality of the internet

b) Social Media - expanded the reach of offenders across new social networks

c) The Internet of things - proliferated the number of devices (and data)

d) Cryptocurrencies - have become a convenient method of value exchange

e) Artificial Intelligence is increasing i) criminal opportunity ii) quality of attacks iii) the scalability of cybercrime - Proof of concept AI driven Ransomware has been found but not thought to be active yet, but it is coming!

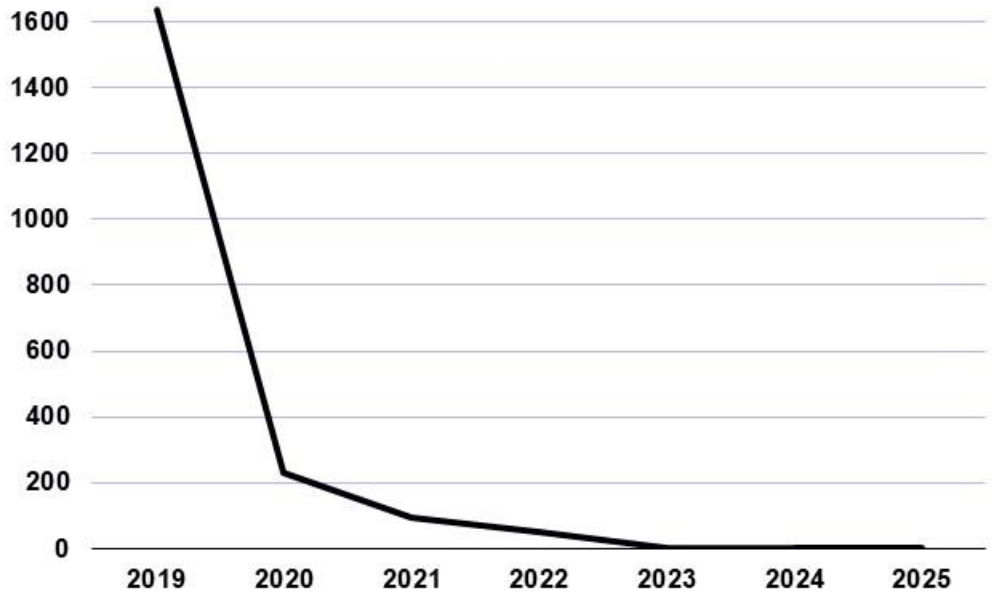
Has created drivers for crime i) More attack surfaces (services) ii) datafication (data has value) iii) new opportunities for theft and extortion (cryptocurrencies)

1a. A faster future

UNIVERSITY OF LEEDS

The ransomware infection (cybercrime) process is becoming faster and has reduced from months to minutes - from initial network access to encryption. *N.B. Quickest times*

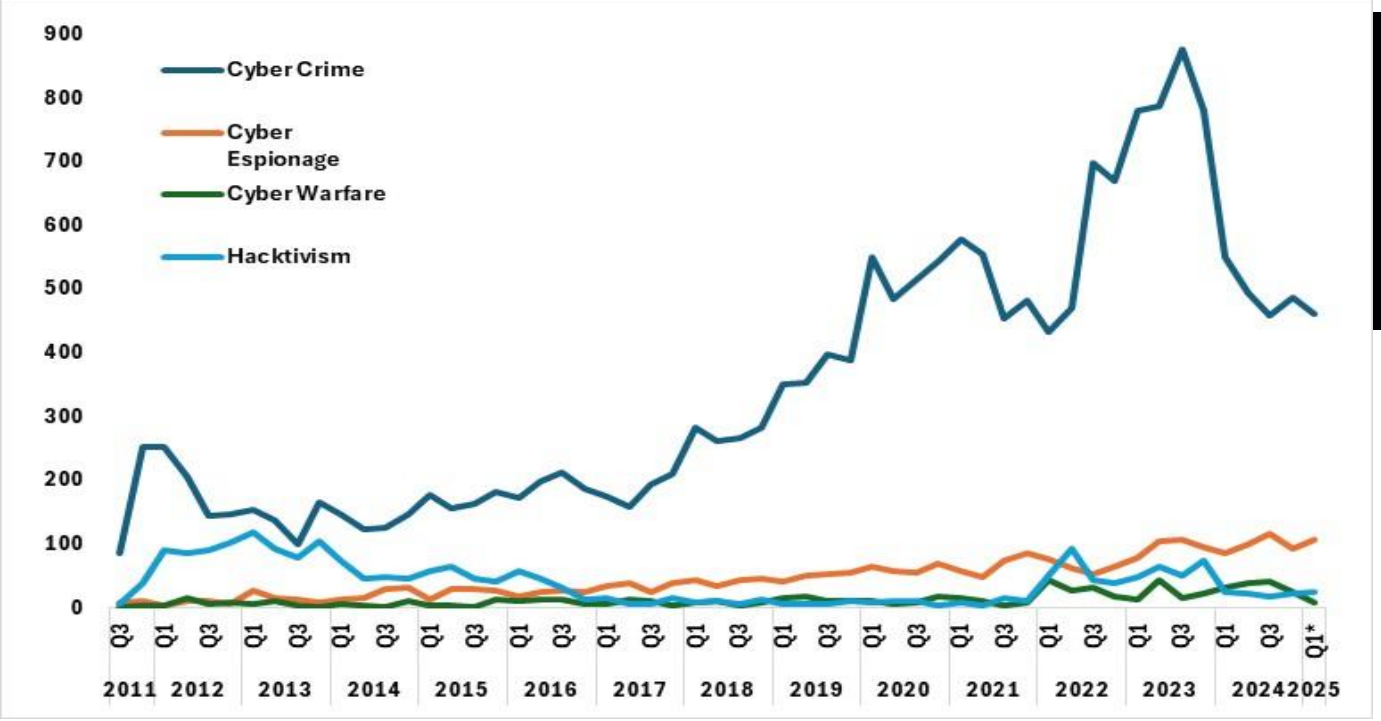
2019	**1637.6**	**(68 Days)**
2020	**230**	**(10 Days)**
2021	**92.5**	**(4 Days)**
2022	**48**	**(2 Days)**
2023	**4 hrs**	**(0.17 Day)**
2024	**45 min**	**(0.03 Day**
2025	**30 min**	



(adapting IBM's X-Force stats 2019-2021, my calculations for 2022-24 based upon events)

The cybersecurity response needs to be much quicker

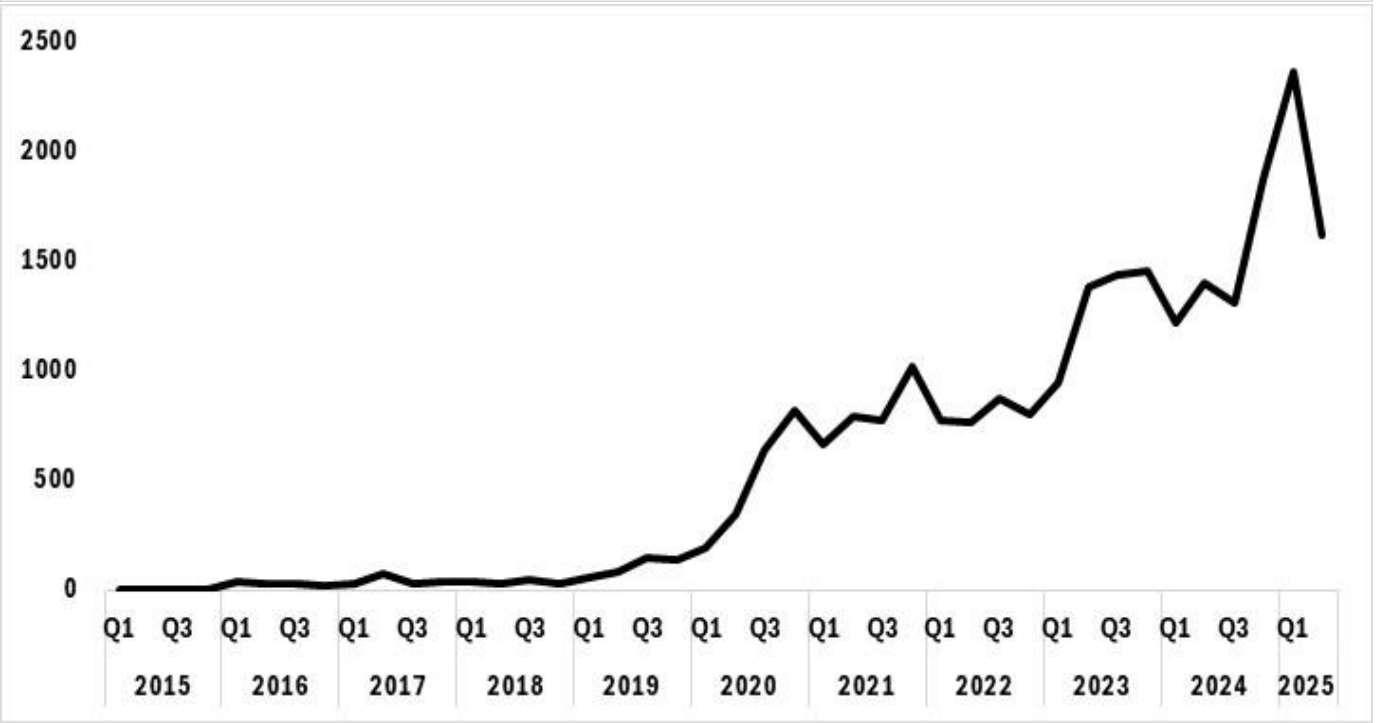
1b Evidence of change: Increase in cybercrime



Cybercrime ‘Events’ –

covered by the media

Source: CyberCrimeDb, 24,000 cases



Ransomware attacks – N.B. do not always become ‘events’

Source: RWDb, 26,000 cases

© David S. Wall 2025

1c. Changing cybercrime trends

UNIVERSITY OF LEEDS

Changes in cybercrime attack vectors have led to:

- In addition to existing bulk-low-impact cybercrimes there is a shift towards **keystone cybercrimes** such as Data Theft, DDoS attacks, Ransomware and CryptoCrimes.
- A rise in attacks on **organisations** in addition to attacks on individuals. Organisations are more lucrative victims.
- A shift to **using more blended cybercrime tactics**, e.g. social science with science – phishing, naming & shaming
- Shift **to using crime facilitators** – offenders buying in crime services (specialist skillsets) from the cybercrime ecosystem which has evolved in the past decade. These form new pathways into cybercrime for offenders.

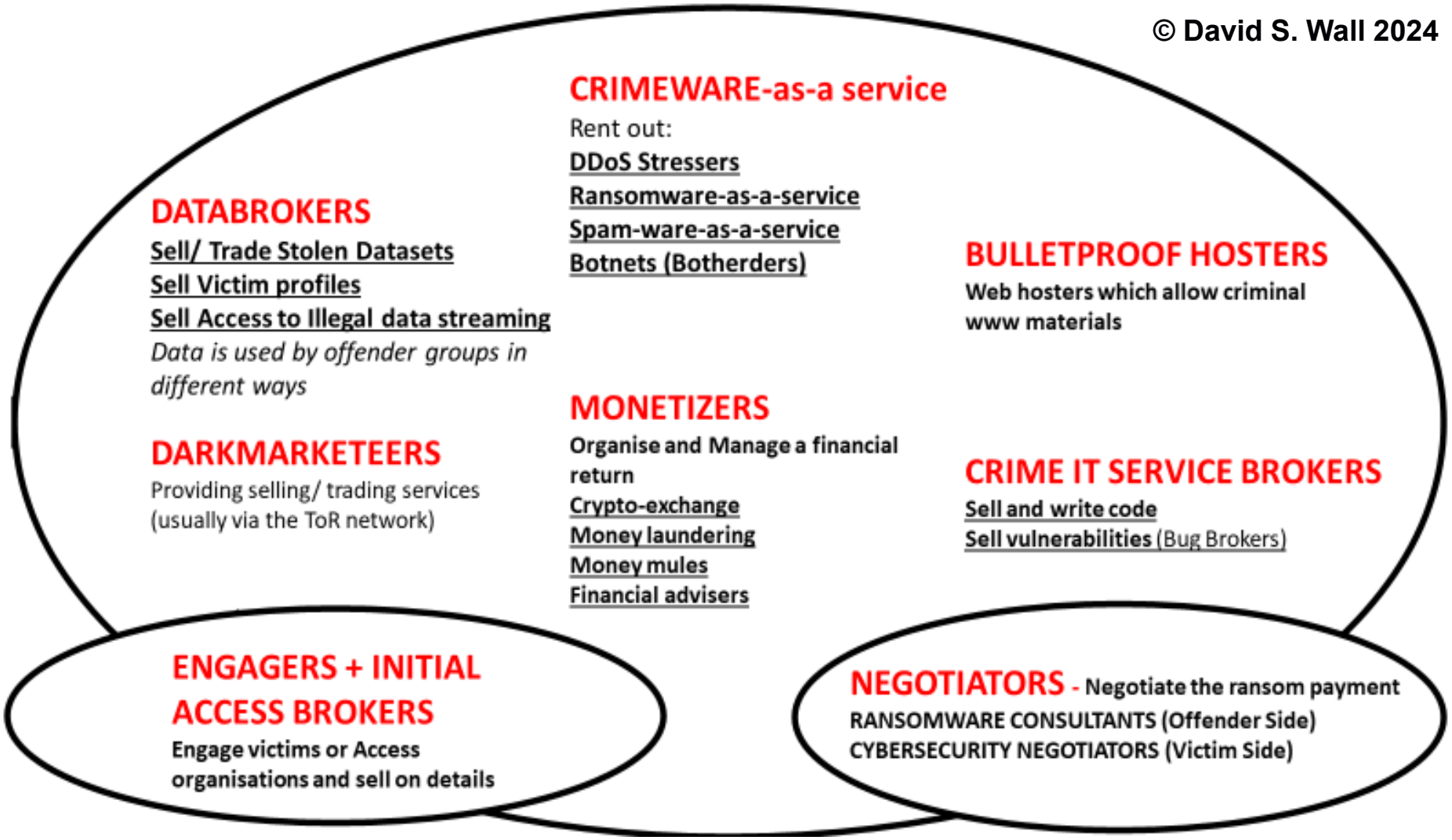
1d. Summarising change and introducing the new pathways into cybercrime

UNIVERSITY OF LEEDS

- **My research** shows that cybercrime has increased in scale, levels of harm, financial returns and physical disruption.
- **Repeated extortion attacks on economies and infrastructure** have pushed cybercrime up the political agenda, but not far enough. DDoS has fallen off.
- **There is an increasing criminal appetite for more cybercrime**, especially keystone cybercrimes which steal data
- **The various recent conflicts** - geo-politicised some offenders, i) activated hactivists ii) introduced new state-actors iii) developed a crime/conflict nexus
- **Adaptive offenders use business tactics** to outmanoeuvre attempts to prevent, mitigate and investigate attacks. *Business Studies vs organised crime playbook*.
- **To scale up**, cybercriminals have rationalised the criminal process. Component parts are deskilled from the individual and reskilled into groups. Following the industrial labour model. AI will take this further in the future.
- **A skill-set ecosystem has developed** to facilitate cybercrime - which provides new 'professionalised' pathways into cybercrime.
- **Cybercrime has become a plausible career choice for skilled young people**

2. The many new pathways into cybercrime to which policing have to respond to

© David S. Wall 2024



2a. What do you need to do to commit a ransomware attack?

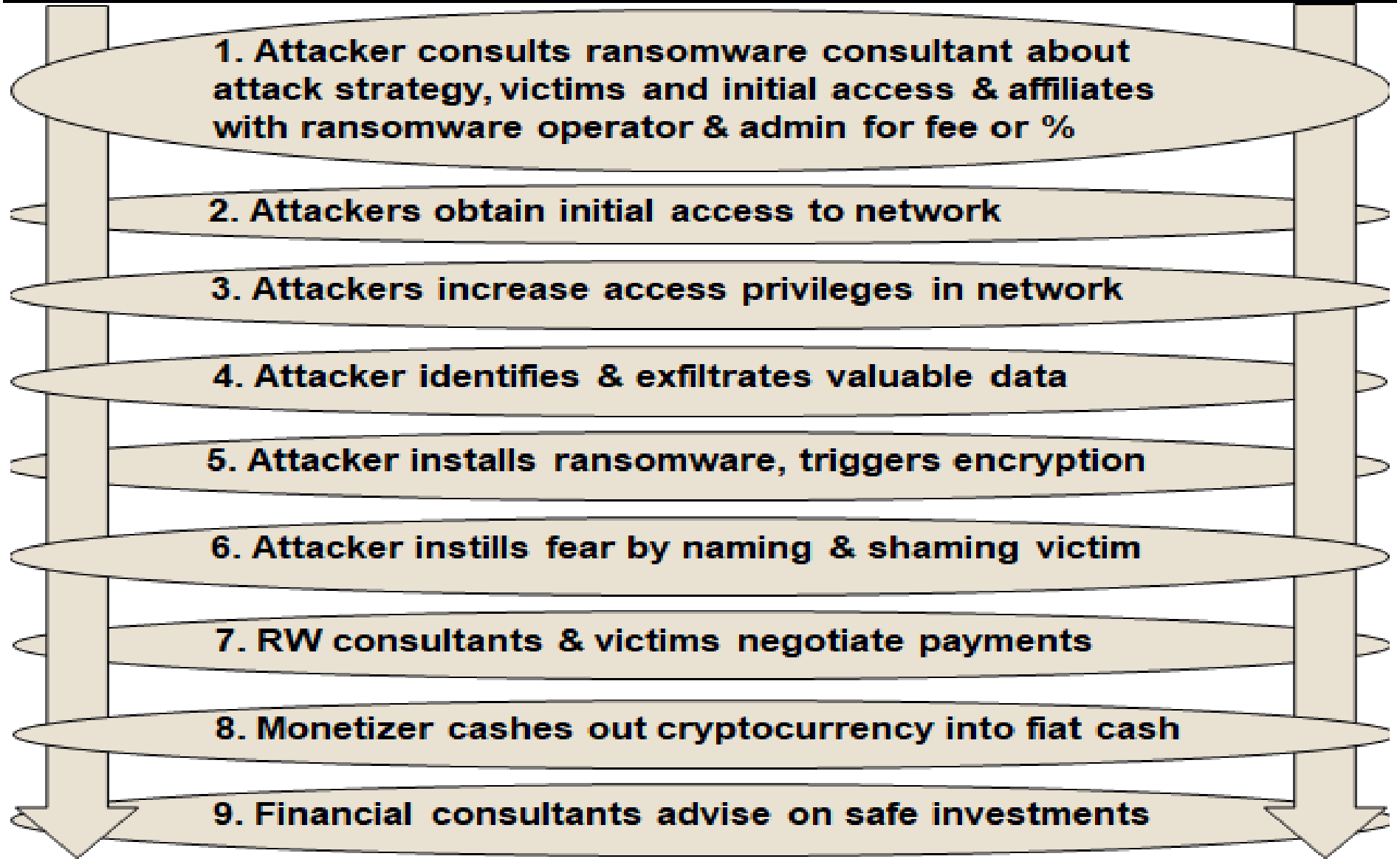
UNIVERSITY OF LEEDS

1. **Reconnaissance** - identify best victims to attack and methods
2. **Gain 'initial access'** to infiltrate the victim's network (e.g.Trickbot)
3. **Escalate computing access privileges** across the system (Emotet)
4. **Identify key organisational data** that will hurt most when lost
5. **Exfiltrate key data, install ransomware and choose time to infect**
6. **Levy the ransom demand and name & shame victims** on WWW
7. **Obtain payment of the ransom demand in cryptocurrency**
8. **Monetarise the crime** – turn cryptocurrency into fiat money
9. **Post-crime - Invest proceeds in legitimate economy**

Each stage requires specialised skills and at least four different groups of criminal actors provide services for a fee.

2b. Who are the actors involved?

UNIVERSITY OF LEEDS



2c. The structure of a Modern Ransomware (RAAS) Group (n.b. they are fluid)

N.B. % are based upon info about REvil (Cybernews, April, 2021)

UNIVERSITY OF LEEDS

1. **Ransomware Affiliates** (often Crime Group or gang of individuals) – employed /pay fee to operate RW - carry out crime – often use more than one RW type – carry most risk/ are paid the most (70%-80%)
2. **Ransomware Operators** – develop, operate & protect their RAAS brand and even approve the affiliates who use it (20-30% of ransom).
3. **Ransomware Consultants** – *information brokers* who advise affiliates on victims, initial access brokers, attack strategy, level of RW ransom, even negotiate the payment and even advise on the cash-out process and on crime proceeds investment (5%-10% or flat fee).
4. **Ransomware Monetisers** – the affiliates hire cryptocurrency exchanges and launderers approved by RW operators (get 4%-5%).

N.B. Each group group of services also employs a number of skilled individuals to enable them to provide their own services – the boundaries are blurred.

3. The implications of the challenges for policing - Enhancing the current capabilities of the police?

- **Develop better National collection points for strategic and tactical information & intelligence**
- **Give the public (victims) a greater stake in their victimisation!**
- **Connect local with national police & different police sectors** (transport, military etc)
- **Work out what works from past police 'operations'**
- **Connect different stakeholders** (police, cybersecurity, courts)
- **Do we need specialist cybercrime courts?**
- **Introduce new disruptive multi-sector 'operations' to disrupt the skill chain that is central to the cybercrime ecosystem and stop or divert offenders from the new pathways into cybercrime.**
- **Develop the role of the guardians of cyberspace (beyond police) to divert potential offenders from cybercrime.**

3a.The Guardians of Cyberspace - police play only a small part in the overall regulation of cyberspace!

1. **Internet users** (social censure)
2. **Online security managers** (threat of exclusion)
3. **Internet service providers** (contractual governance)
4. **Corporate security** (contractual/corporate governance)
5. **Non-government /non-police agencies** (IWF, TS) (recommendation for prosecution)
6. **Non-police /government agencies** such as Action Fraud, NCSC/ GCHQ (intel + prevention) Also BIS etc. Cabinet, Home Office, Foreign Office (policy) – also EU agencies – Enisa, Eurim, Europol (IC3), Interpol + VTF
7. **Police Forces** at local, regional and national levels

4. Conclusions

UNIVERSITY OF LEEDS

- Cybercrime will develop in scale as new opportunities arise from developments in the technologies of computing and networking.
- AI LLMs will continue to improve offender tactics
- Offenders (will) regard the 'Cybercrime Industry' as career choice.
- Cybercrime is not going to stop, there is no silver bullet, it is part of social, business and political life
- LE must work with CS to become more proficient at 'whack-a-mole'
- Need robust technical measures and appropriate legal and tech tools
- Be organised to anticipate crime trends and quickly apply those tools
- More proactive cybercrime prevention - LE and CS need to play a stronger and combined role - Cyber Choices (PREVENT)
- Policing agencies will need to be reviewed for a quicker response
- Criminal justice systems (one criminal per crime) need to deal with multiple offences, especially across borders
- At a political level, cybercrime does not 'bang, bleed or shout' does not rank so high in the policing, political, or research agendas
- Raising cybercrime on all agendas is the next big challenge

4a. More specifically – What to do for the future

UNIVERSITY OF LEEDS

1. **Offenders** - *how can they be disincentivised – can alternative pathways (e.g. PREVENT) draw offenders away from cybercrime?*

2. **Victims** – *what are the responsibilities of victims* - be forced by law not to pay ransom? and be 'responsibilised' into cooperating with LE?

3. **Government** – *speed up the policy response and funding process?*

4. **Police/ Law enforcement** – *Tactically* how can data about victimisation be shared, what should be shared, by whom and how? *Strategically*, should the current police-centric role be rethought? Is the 'LE' model too narrow for cybercrime? Would a peace keeping order and law policing focus be a better strategic approach?

5. **Internet guardians** – Could the responsibilities of the various guardians and bodies responsible for managing order in cyberspace be further invoked and even constitutionalised.

References

UNIVERSITY OF LEEDS

See (and check out the references in) CH7 - Wall, D.S. (2024) *Cybercrime: The transformation of crime in the information age, 2nd Edition*, Cambridge: Polity. (Hardback ISBN: 978-0-745-65352-5) (Paperback ISBN: 978-0-745-65353-2)

Wall, D.S. (2021) 'The Transnational Cybercrime Extortion Landscape and The Pandemic: Ransomware and changes in offender tactics, attack scalability and the organisation of offending', *European Law Enforcement Research Bulletin*, (SCE 5) Oct 5, 45-60 https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/475