Winter is Coming! Balancing expectations with delivery in AI and Cybercrime

David S. Wall
Cybercrime Group, CCJS, School of Law, University of Leeds, UK
d.s.wall@leeds.ac.uk

WebSci'20 Workshop: Socio-technical AI systems for defence, cybercrime and cybersecurity (STAIDCC20), Southampton, June 7, 2020

Outline: Framing the talk

- I will look at offensive & defensive AI cybercrime systems
- The debate meanders down different disciplinary paths
- Results in mismatch of expectations from AI claims & delivery - e.g. policy vs scientific or academic objectives
- The real issue is layered, much like an onion
- Most AI apps offline/street crime, cybercrime is different
- AI is now also part of the cyber-offender's playbook
- As the arms race develops, security to be more adaptive
- A 3rd AI Winter may come, but is springtime for offenders!

Structure of this talk

- Part 1 explores the use of AI systems to deal with crime and policing in a risk society
- Part 2 identifies the challenges presented by AI, cybercrime and cybersecurity – what is cybercrime
- Part 3 looks at how AI is part of the cybercriminal's playbook as offenders have begun to use it
- Pt 4 discusses the realities of using AI in investigating & preventing cybercrime & concludes

Winter is Coming!

AI Winters and Summers

- **The social capital of AI rises and falls over time as expectations fail to match delivery, causing interest to wax and then wane**
- **It creates a research funding cycle**
- **It is, arguably, a normal funding cycle**

[1st Summer 1950s/60s - 1st Winter 1970s
2nd Summer 1980s - 2nd Winter 1990s
3rd Summer 2000/10s – 3rd Winter 2020s?]

Are we about to enter a 3rd AI Winter?
The problem is that the Offender's summer is already Here !

1. Using AI systems to deal with crime and policing in a risk society

- Using AI to identify Crime hotspots & manage police resources (PREDPOL)
- Assessing individual prisoner risk
- Assessing offender risk (domestic violence) Durham
- Offender street surveillance schemes (Cardiff, Met)
- Automatic Number Plate recognition

- ALL may be good science & even if some fail their technical goals, we can know why
- AI may succeed technically and may not inform the policy problems they set out to
- AI applications are also fraught with unconsidered privacy concerns (Covid tracing app?)
- There is the fundamental data problem, which can lead to bias (inc. race)
- AI lives in a socio-political world where the social-political prevails

---

AI raises questions about who actually benefits & do we know the advance knock on effects?
But as we move through AI seasons it becomes more sophisticated, and effective.

1.1 A Vignette

A police force spent millions of pounds on an AI Crime Hotspots application that told them that a park nearby is dangerous at night times, particularly for women. The programme was sophisticated, but did not really tell police managers any more than an experienced analyst or police officer would know already.

- You'd think that spending the cost of the software on staffing could have secured the jobs of key staff to achieve the same, but …
- The actual issue was not scientific (the prediction), but replacing dwindling skillsets through a large turnover of staff
- And providing management with reliable and routine information across the social geography of the police force area
- Success meant getting reliable data that is fit for purpose

1.2 The ‘Fundamental Data problem’

- The ‘fundamental data problem’ underlies all AI systems and Big Data Analytics & is three fold

i) **how do we ensure the data is appropriate for the problem?** & address different interdisciplinary expectations of what data is the

ii) **how do we improve the quality of data?**

iii) **how do we get the data?**

iv) **why should owners share data with us?**

Appropriate data helps the AI and ML work – but how do we identify and get it? Why should owners give it?

N.B. This is a plug for further discussion

2. Challenge of AI, cybercrime and cybersecurity – what is cybercrime

- The cybercrime challenge is that they are different to street crimes in a number of ways
- Remember that Cybersecurity is the broader field - proof of concept, risks, threats, harms and crimes - security is 'felt'. Cybercrime is different and deals with the harms from crime.
- Cybercrime offenders use digital and networked technologies (internet) for criminal purposes – cybercrimes are asymmetric, global, informational and immediate
- Offenders use the internet to a) organise crimes (**cyber-assisted**), b) enable existing crimes (**cyber-enabled**) or c) commit entirely new crimes (**cyber-dependent**)
- There are three distinct crime types (by *modus operandi*). **Crimes against the machine** (hacking, DDoS etc.), **Crimes using the machine** (frauds, hate etc.) and **Crimes in the machine** (extreme hate, terror or sexual materials, illegal data).
- Different cyber-offender groups victimise individuals, organisations and nation states.
- The cyber difference is their asymmetry, globalised, informational and immediate nature
- Most cybercrimes are very small (significant in aggregate) - *why commit 1 X £50m robbery when you can commit 50m X £1 thefts from your room? Or DDoS, or Phishing, data breaches, cryptojacking, ransomware etc …* ***<u>These challenges can be addressed with AI</u>***

3. AI and the cybercriminal playbook

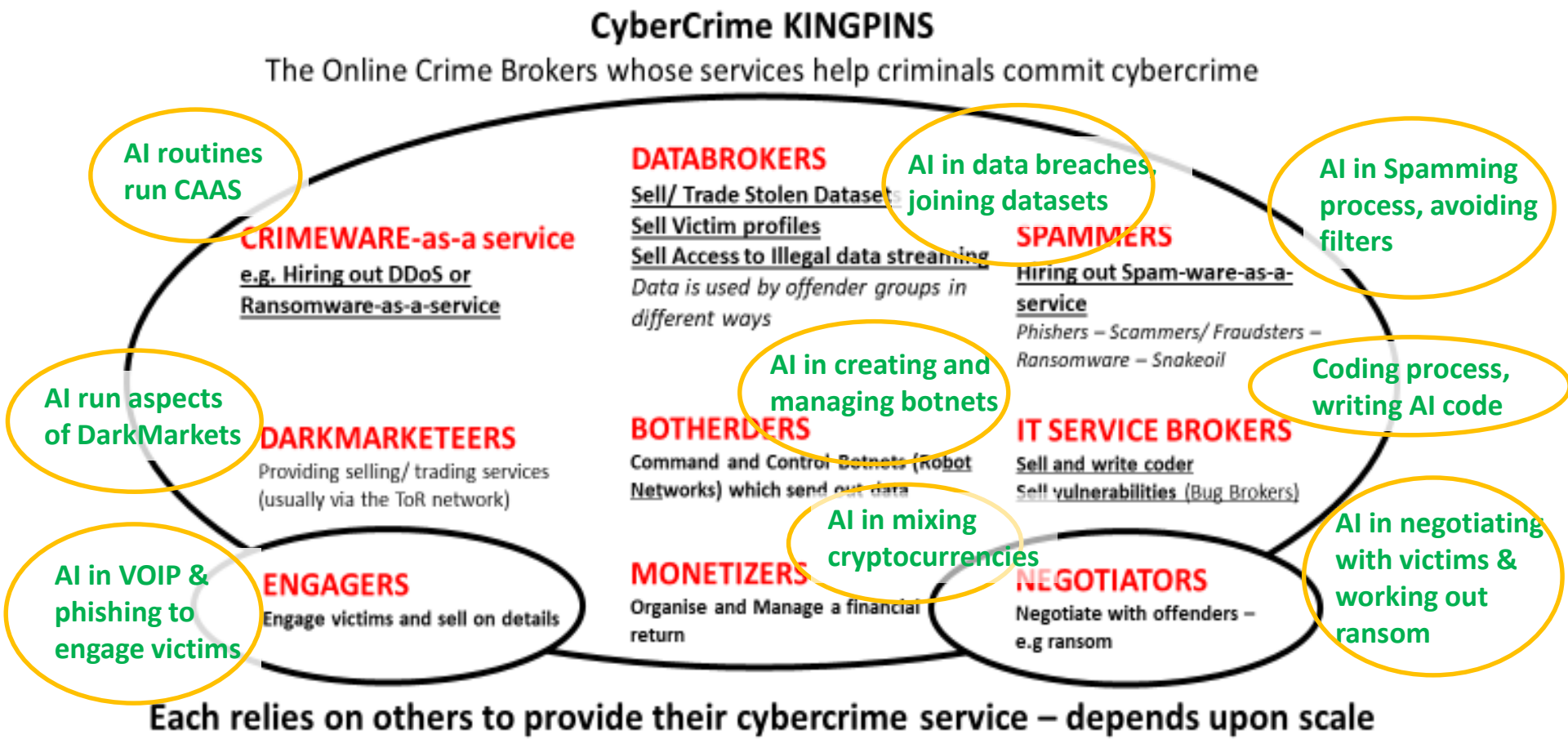
- But, AI is already firmly part of the cyber- criminal playbook
- AI routines are currently being used by offenders to help them commit cybercrimes and are an essential part of the cybercrime ecosystem
- By understanding these routines, we can, arguably, identify where to place interventions & effect the kill-chain to disrupt the ecosystem and stop cybercrime
- Not least, there is too much focus upon ‘amateurs’ and not skilled ‘professionals’. I feel, we may be missing a trick

3.1 The key functions in organising a cybercrime – adapting my existing work on identifying cybercrime kingpins and their cybercrime brokerships

- **Databrokers** provide data – e.g. to construct spam lists
- **Spammers** - sending out Spam emails
- **Botherders** – provide botnet services **-** command and control botnets (Robot Networks) which help spammers send out data
- **Crimeware-as-a-service (CAAS)** sellers – hire out service to do DDoS, Ransomware and other malware attacks (e.g. Zeus banking trojans)
- **Darkmarketeers** provide, sell or trade cybercrime services, usually via the ToR network.
- **IT Cyber Crime service brokers** write and sell code and vulnerabilities (to Bug Brokers)
- **Engagers** use social engineering to engage victims and sell contact deets (details)
- **Monetizers** organise and manage the financial returns from cybercrime, often via money mules.
- **Negotiators** negotiating ransom amount with offenders (is also sometimes automated – set by AI powered software)

EACH PROCESS USES AI ROUTINES TO RUN OR HELP RUN IT

3.2 AI Routines in the Cybercrime ecosystem



3.3 What do we know about ransomware offenders

Based upon 30 known ransomware hackers + 10 facilitators + 10 OCG/APT groups

- **Who are RW Offenders? –** they are older than amateur 'hackers'. They are 'professionals' (or proto) (as opposed to amateurs and non-professionals). They have graduated from being script kiddies.
- **What drives them?** Business or Robin Hood values? They see RW as victimless because of insurance - which drives them, and gives them esteem. Has been a shift from dilettantes to professionals.
- **Who helps them - facilitators** are much the same profile, though possibly a little younger. They have either found their niche, or are in a transitional stage.
- **How many are there?** not many as you would think as one person can have massive effect.
- **How adaptive are they?** they are incredibly adaptive and regularly change tactics to stay ahead of the security 'Wack a mole' response. They use psychology to get their way.
- **What keeps them motivated?** – retain the prankster humour of hackers, but seem to drift to RW because of large pay-outs – as said before insurance has a large role in driving the shift
- **How are they organised?** mainly distributed, but the gangs have potential for OCGs
- **What are cyber-security and Law enforcement doing?** adaptiveness is increasing, but is varied – this emphasises the value of the prevent programmes.

4. Using AI to investigate & prevent cybercrime

- Learn Lessons from IBM DeepLocker – AI Cybercrime Simulator
- WE HAVE (EMPHASIS Project) used AI to:
- a) identify ransomware types from the screen image (Atapour-Abarghouei et al. 2019)
- (b) developed AI to help identify data exfiltration (McGough et al. 2015)
- Learn from Cybercrime AI playbook – apply AI routines to key parts of the cybercrime ecosystem

5. Conclusions: Balancing expectations of AI

- We need solutions that are (like the problem) blended and more sophisticated the current ‘whack-a-mole’ approach
- E.g. AI skillsets are different from trad’n science thinking – e.g. replicability – running the same routine twice may produce different results is not in the Popperian mould
- Focus AI solutions on specific problems - Sci & SocSci led
- Identify good quality & appropriate data for the application
- Get rid of cultural obstacles to breakdown siloed thinking to get “Security through knowledge rather than obscurity”
- Develop partnerships that co-own the problem in order to co-produce the solution – and I hate the word ‘solution’

Thank You

- David S. Wall - email d.s.wall@leeds.ac.uk

ESPRC Projects EP/M020576/1 & EP/P011772/1

- Web Pages -

https://essl.leeds.ac.uk/law/staff/238/professor-david-s-wall-facss

- Academic Articles - https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=376504
- Short Articles https://theconversation.com/profiles/david-s-wall-98233
- https://www.firstlinepractitioners.com/?s=David+Wall