Humans and Hybrids

Repositioning the social threat to network security in the 21st century

M.R. McGuire: University of Surrey

The Cybersecurity Imagination

Social Threats to Networks =

“Human Factors”

“Social Engineering”

or

“The Socio-technical”

Etc. etc.

The Human Factor

Accepted - and known that (for example):

- Between 60 -90% of data breaches have a human basis
- 83% of organisations reported insider attacks in 2024
- Phishing attacks remain the most prevalent and disruptive type of breach or attack (experienced by 85% of businesses and 86% of charities)

The Human Factor

- 70%–79% of organizations targeted by business email compromise. Global losses surpassed $8 billion between 2021 and 2023, making it more frequent than ransomware
- 50% of firms say that family members permitted to use work issued devices
- Only 19% of businesses overall have specific cyber training (76% of large businesses)

(*UK cyber breaches survey 2025*)

Acceptance is one thing - But

– what more clearly IS a human factor?

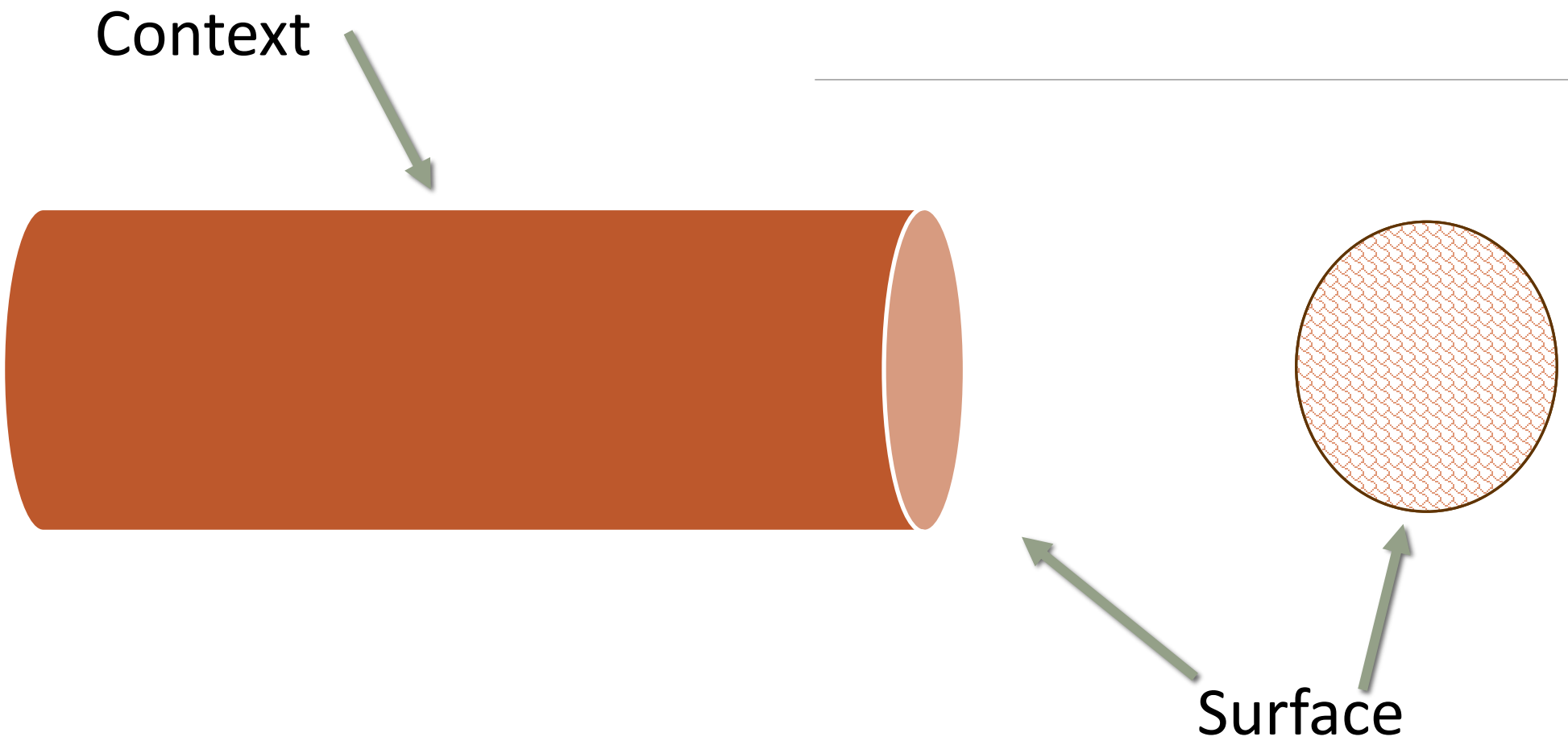
– If it is to do with ‘errors’ (as is commonly assumed) what is an ‘error’ in this context?

– is “human” equivalent to “social”?

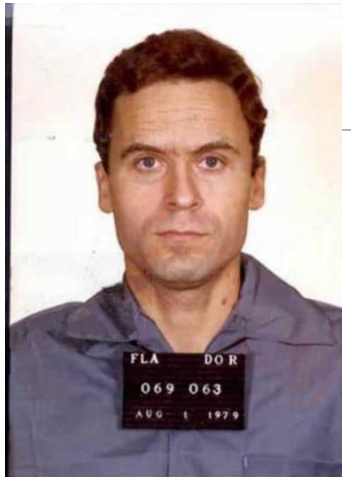
– where in the socio-technical does human agency end/begin and technical agency predominate?

– Where is the predominant requirement of any science – causality….. ?

Attack Surfaces and Explanatory Voids



Attack Surfaces - Analogy from a Murder Scene



Local Ridge Orientation = gradient of

$$\nabla\theta = \nabla(\arg p(z))$$
$$= \frac{1}{2}\sum_{i=1}^{k}\left\{\frac{(y_{ci}-y, x-x_{ci})}{(x-x_{ci})^2+(y-y_{ci})^2} - \frac{(y_{di}-y, x-x_{di})}{(x-x_{di})^2+(y-y_{di})^2}\right\}.$$

Three Varieties of Social Challenge

1: Challenges of Social Change

2: Challenges of Social Organisation

3: Challenges of Social Mutation/Hybridization

1: Social Change

Contemporary socio-political shifts e.g.:

- Electoral influences
- Economic shifts/upheavals
- Conflicts and tensions

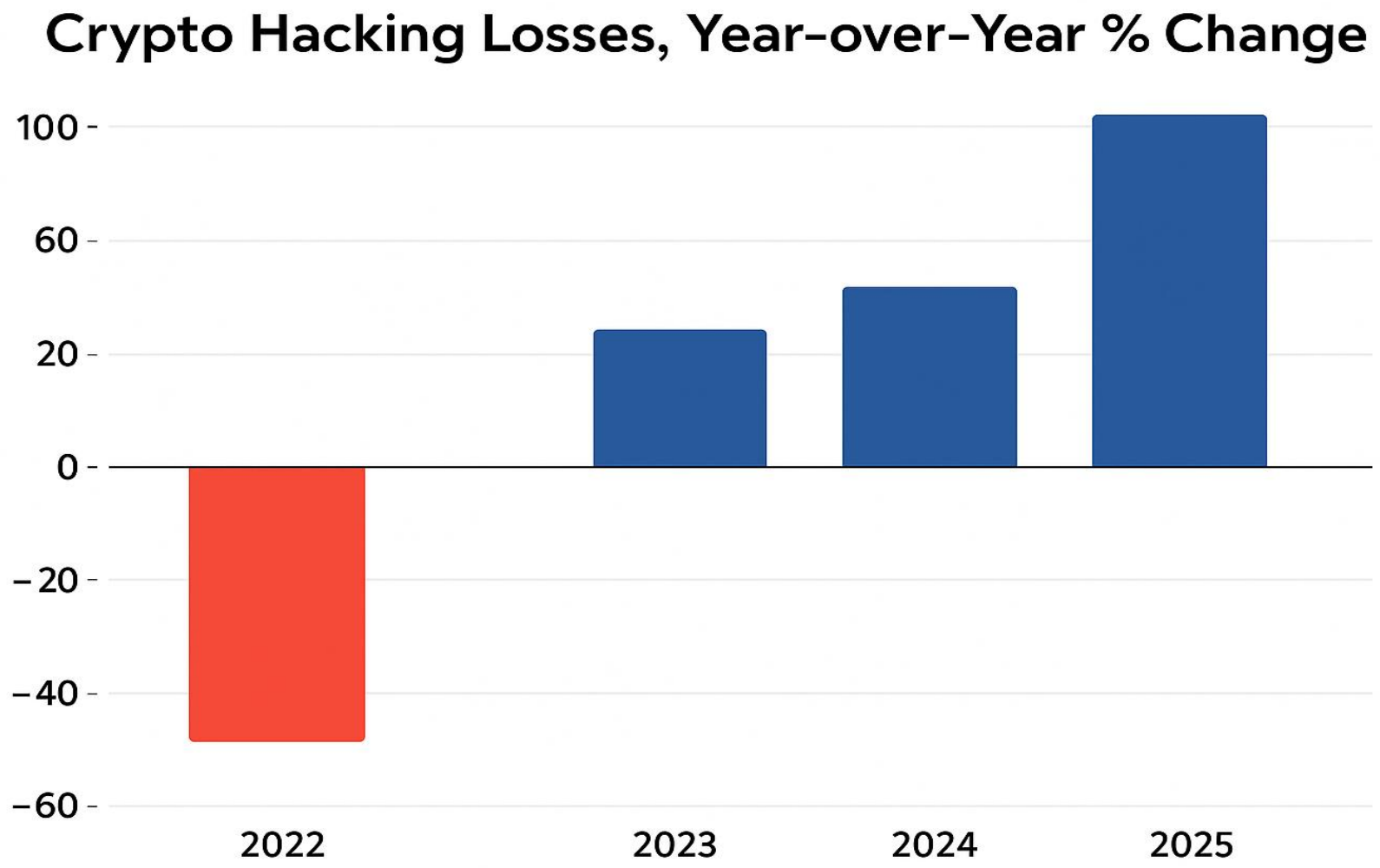
How is any of this a network security issue?

Social Change

Electoral influences

New attitudes, new policies e.g.

- Trump administration pivot towards crypto
- Coinbase crypto-mining malware enters top 3 threat list in 2025
- Use of illegal crypto-wallets increase by 145% between 2024-25. Valued at $158bn – highest ever



Deep Strike (2026)

1: Social Change

Electoral influences

September – October 2020

- Process of forced removal of Charles Krebs from his post as Director of Homeland Security Cybersecurity Agency
- Krebs had affirmed the 2020 US election was the safest (most cybersecure) in US history and denied any election fraud

November 2020

- Solar Winds Supply Chain attack (by Russian SVR?) – one of the most sophisticated to date
- 30,000 public and private organization had networks, systems and data compromised – including US Treasury, Department of Justice, Pentagon, Microsoft, Intel, Vmware, Visa, Mastercard, CBS, McDonalds, Volvo & Ford

Social Change

Economic upheaval

- Impacts of economic instability upon share value of cybersecurity firms
- Average falls of between 4-5% in 2026 with wider falls for software firms
- Reduced capacity to produce effective tools
- Impact of economic downturns/recessions on investment in cybersecurity and shifts toward other priorities

Social Change

Economic upheaval

- Booms in certain forms of network provisions can quickly turn into economic bubbles
- Subsequent financial crashes which then reorientate sector away from previous solutions.
- EG dotcom bubble of late 1990s. Over investment in IT start-up firms led to reductions in caution and protections
- Rise of wholly new varieties of attack vectors and cybercriminal organisations
- EG Melisa Virus (1999) I loveyou Virus (2000); My Doom Virus (2003) MafiaBoy Ddos attacks, Carding groups like ShadowCrew
- Many argue current obsession with AI based solutions are leading to similar risks – and probable outcomes....

Social Change

Global Conflicts and tensions

- Research suggests that rate of cyberattacks rise by up to 50% during stand-offs or conflicts
- And new conflicts can create entirely new kinds of cybersecurity risk
- Cf. 22-day attack on Estonia in 2007, the cementing of Ddos oriented strategies like ping flood, UDP flood & malformed web queries as nation state attack vectors
- Protecting networks against adversaries can have the opposite effect, providing cybercriminal groups with new options and opportunities
- 2016 NSA hack by the 'Shadow Brokers' – Eternal Blue exploit + 1 gigabyte of other exploits enter the criminal ecosystem. Up to 20m Eternal Blue attack attempts recorded every month….
- Russian cybercrime groups like Conti,TrickBot, Kraken, Noname 057and Killnet developed arrangements with Putin regime to undermine Ukraine under the 'Dark Covenant'
- 74% of all ransomware profits now goes to such groups

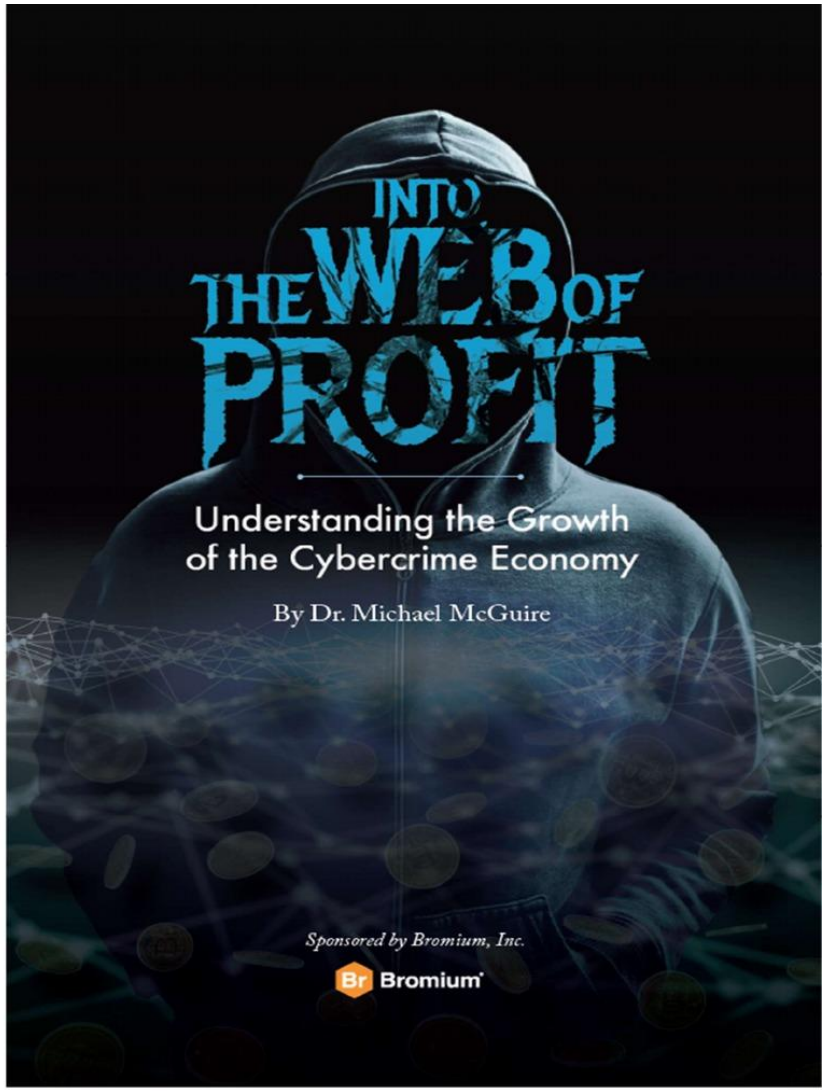
2: New Forms of Social Organisation

History of cybercrime shows movement from lone actors through to agile, integrated groups, nationalization and regionalization of production

Major impacts upon cybercriminal practices and network threat landscape.

Coming together of:

- Original carding groups
- Forums
- Communication channels
- Emerging online crime marketplaces like Silk Road



New Forms of Social Organisation

The Cybercrime economy

2 year study – initially to understand how cybercriminals spend profits. Field Research and Qualitative interviews with over 150 Dark net vendors, suppliers and customers

Identified emergence of a highly integrated cybercrime economy

Multiple modes of revenue generation

Estimated value in excess of $1.5tn annually

Larger than the GDP of many nation states

2: New Forms of Social Organisation
Platform Criminality

Resulting evolution of traditional cybercriminality into a new modality - Platform Criminality

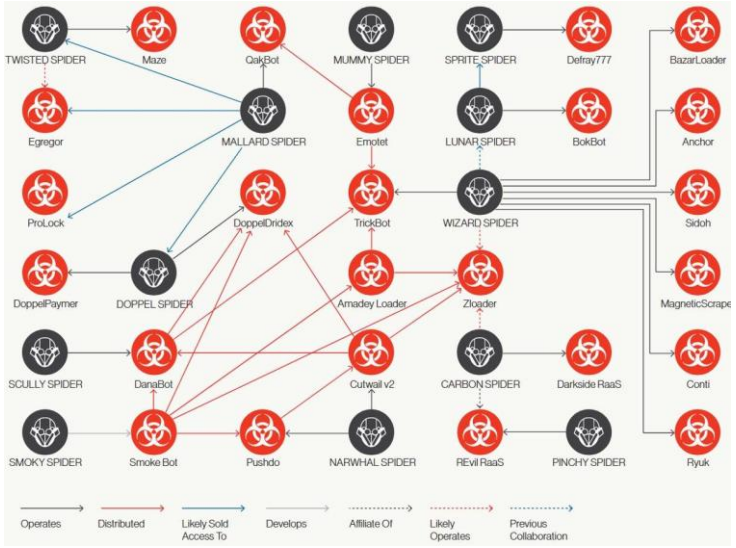
Integration of platform modes of organization into digital crime word

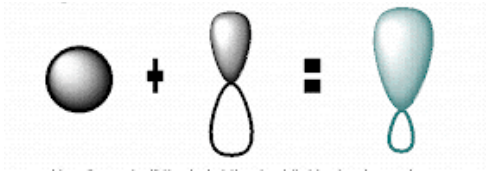
Blurring between operations of legal and illegal platforms. “Post-Crime”?

Easy availability of digital crime tools across crime platforms

Legal platforms increasingly targets and resources for digital crime

Widening need for new approaches to cybersecurity





3. Hybridisation

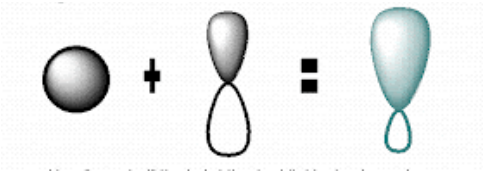
Digital Attack techniques

Increasingly merge with

Kinetic Attack techniques

For example:

Ukraine war demonstrating that jamming, or e-warfare responses not sufficient to block drone attacks



Hybridisation

Conversely: drones can now use **physical** means to compromise network security.

EG: Flying in close to:

- Conduct local de-authentication attacks.
- Detect and spoof wi-fi networks
- Carry devices to infiltrate or shut-down systems

Emergence of micro drones which conduct simple intelligence and surveillance of cybersecurity at work.

Password sniffing and filming network protection tools

Social Hybridisation

Human bodies and social life integrated ever more closely with digital technologies

Technological extension

Wearables

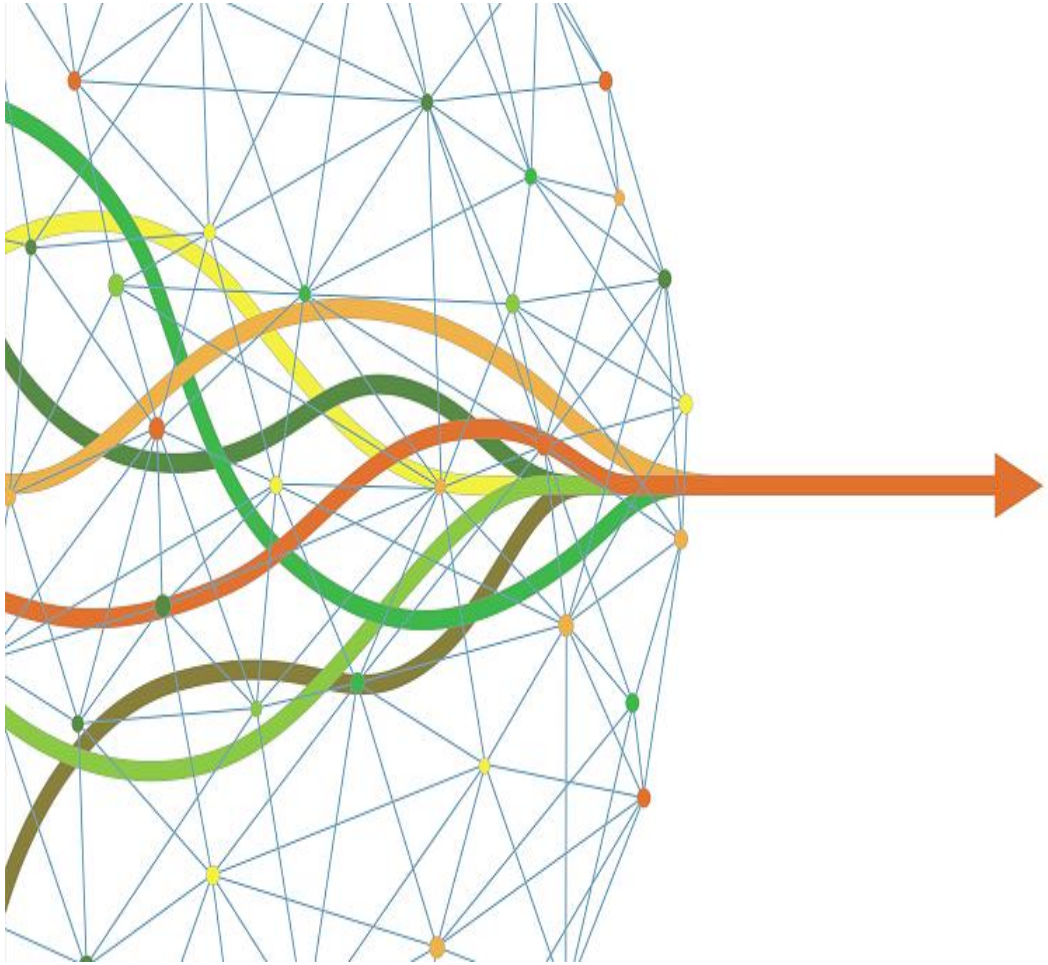
Wholly new threats –

Enhanced Personal/Corporate/State Espionage

Pacemaker hacks

Incorporation in Botnets

Privacy risks



Putting things back together

Increasing evidence that cybersecurity has not only failed to meet any of these challenges

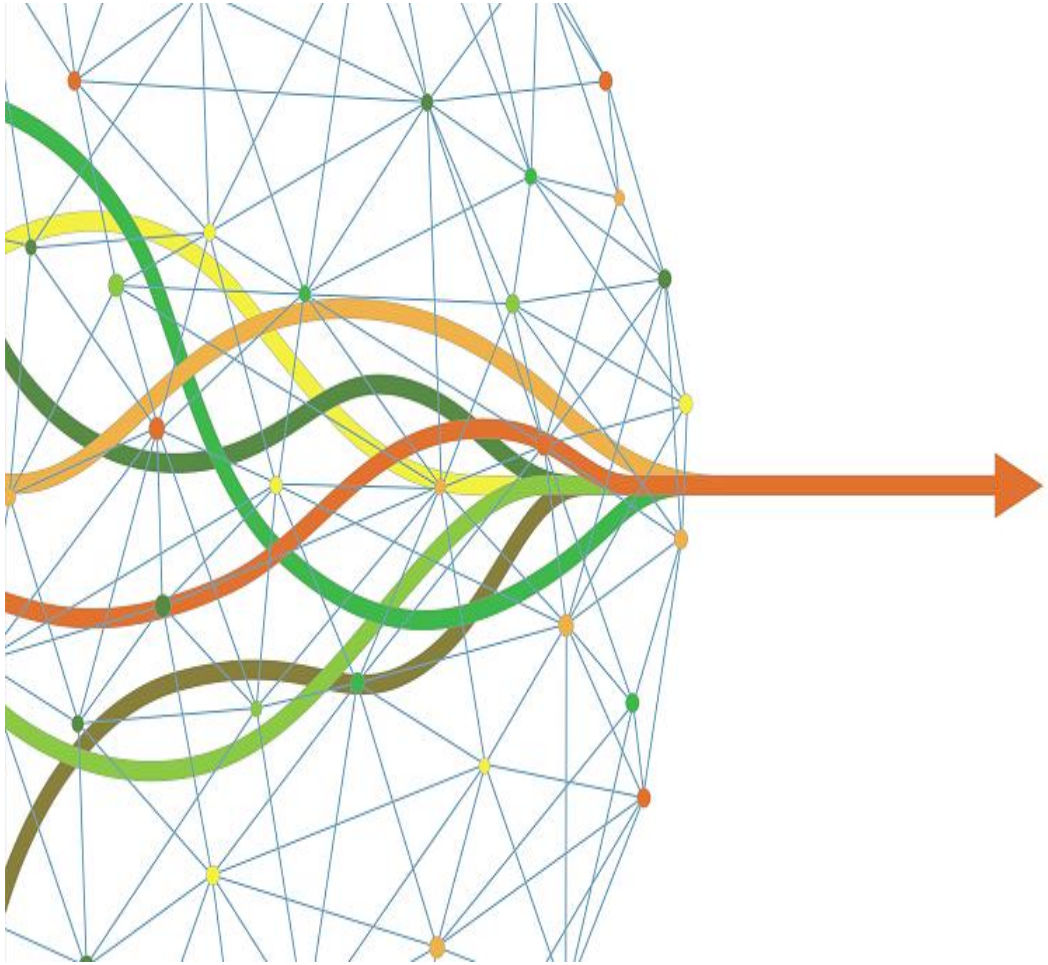
But also, as it stands, may not be fit for purpose

In spite of industry value estimated at $500bn+

Ongoing rises in malware

Continuing success of new (and old) attack vectors

And so on



Putting things back together

Could there even be a sense in which cybersecurity can be held to be **responsible** for cybercrime?

Time to take stock and rethink again?

Embedded Cybersecurity?

A model which no longer treats network security as an afterthought

Not just the old chestnut of ‘better education’

Something embedded at every stage of policy and institutional adaption

Embedded Cybersecurity?

In higher education – bridging computer science/social science type divides

In the professional domain - breaking down the glass wall between fields of expertise (cf. professional conferences....)

In everyday life – “naturalising” how social actors use and respond to security

Or – do we need something yet more radical?

Co-evolutionary Cybersecurity?

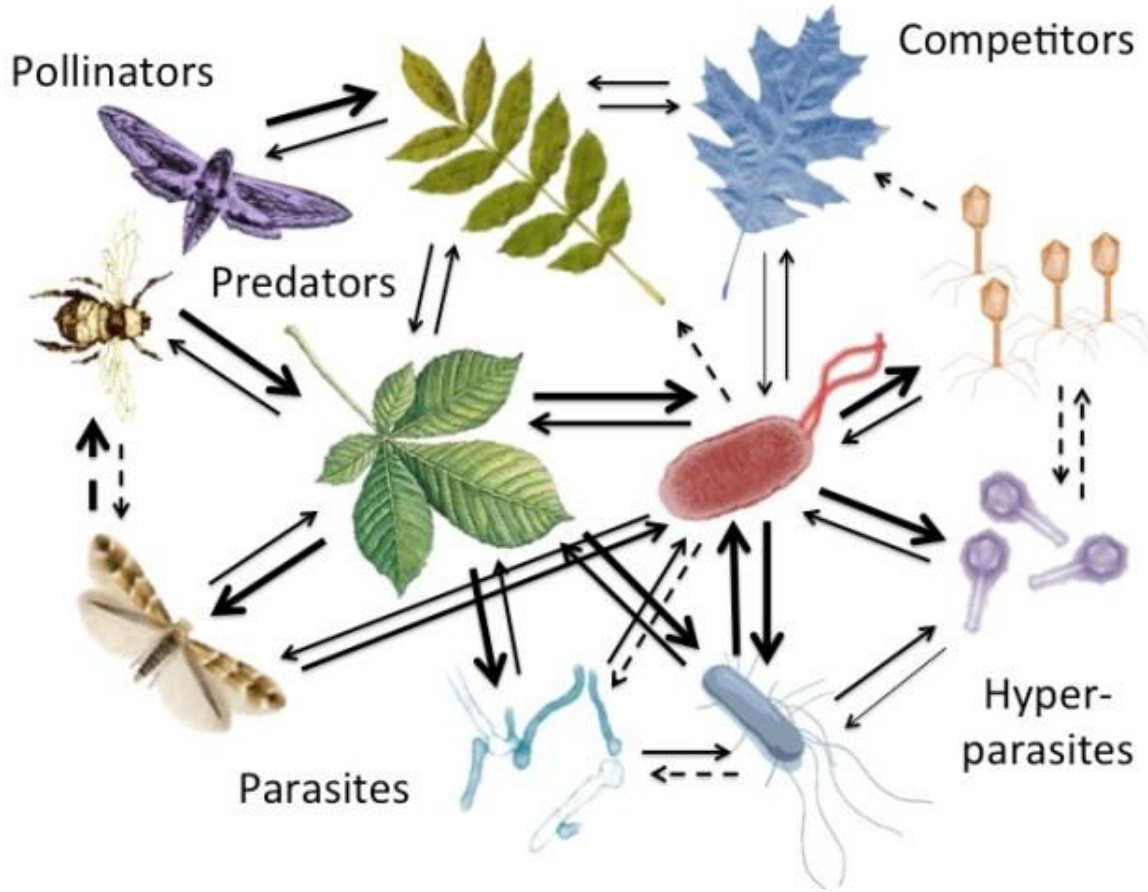
A new paradigm?

Responding to cyberthreats in a dynamic evolutionary way

Across all levels of social interaction

But in line with co-evolutionary, NOT individual evolutionary processes

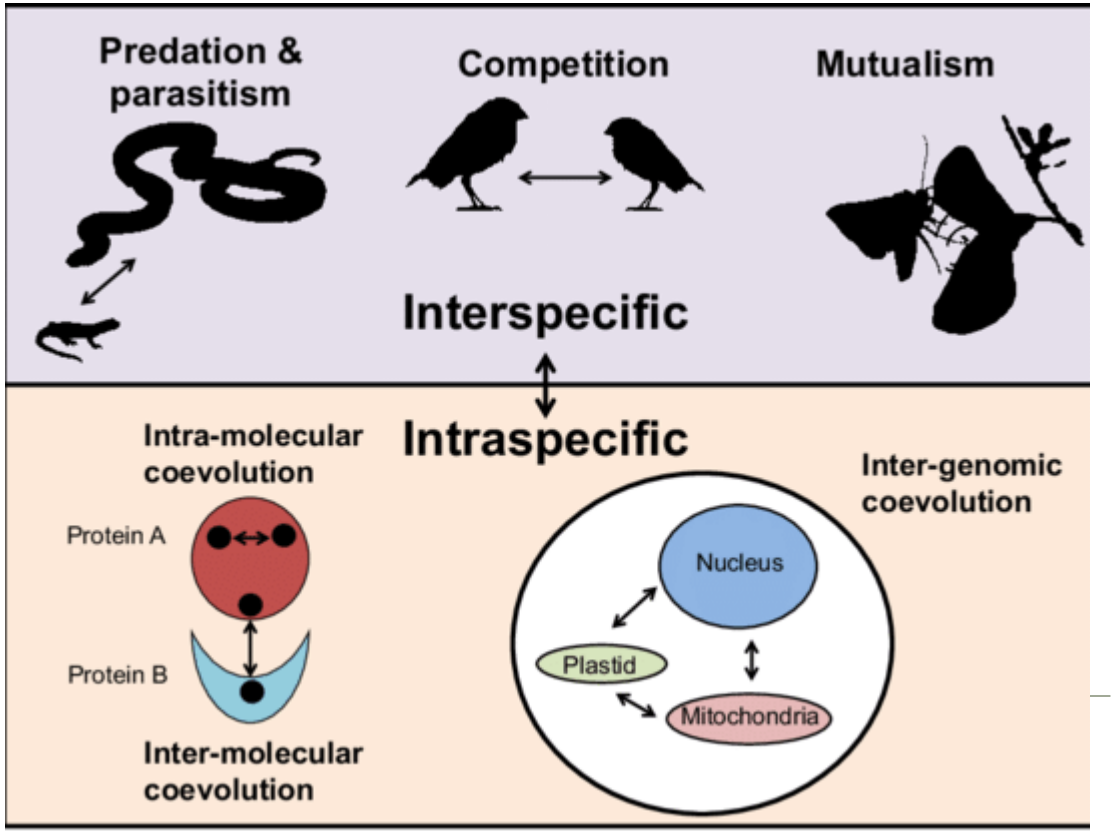
Eg ensuring that evolutions in network protection co-evolve with evolutions in attack tools

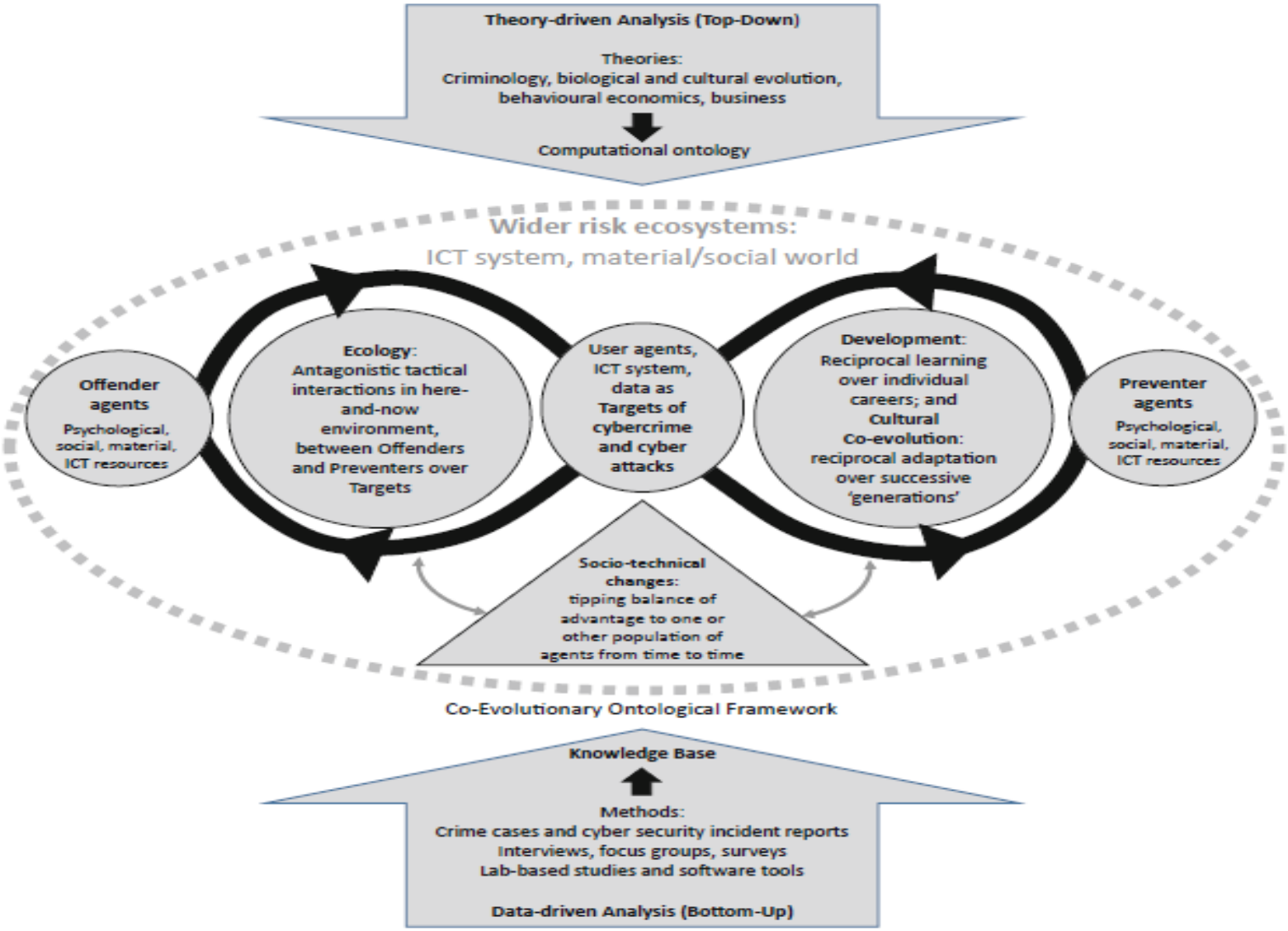


Level Complications

But:

Multiple complexities in mapping co-evolutionary relations between agents at different levels ...





A Socio-technical Framework for Reducing Human Related Risks in Cybersecurity (McGuire et al. 2019)

Conclusions

A more extended engagement with the social now essential.

Needs to move beyond poorly grounded assumptions about ‘human factors’

Towards a full spectrum, technologically extended merging of the social and the cyber…

Far greater co-operation and more considered integration between social scientists and cybersecurity practitioners will be crucial for this to happen