

THE CYBER ATTACKER: PUTTING THE ATTACKER BACK INTO THE HUMAN EQUATION

PROF. DR. WIM HARDYNS

ERC CONSOLIDATOR GRANTEE

Cyber Renaissance

Wavre – 22 September 2026

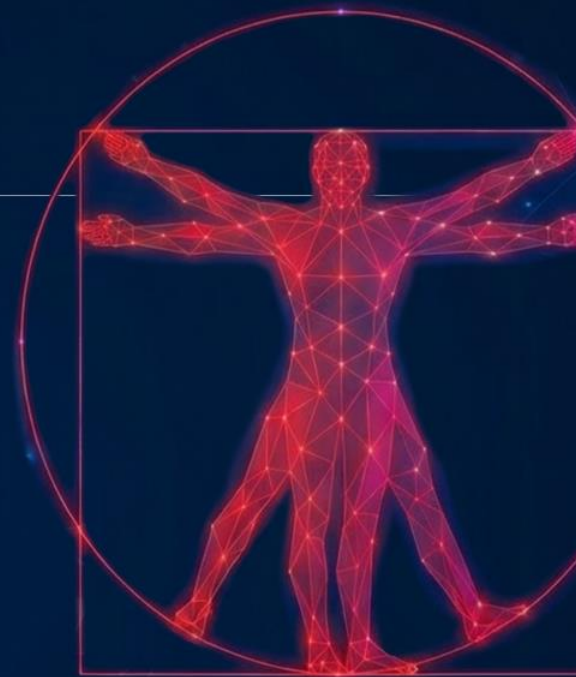


Cyber Humanism

The Cyber Attacker Putting the Attacker Back into the Human Equation



Wim Hardyns
Professor of
Criminology & Security
Ghent University
University of Antwerp

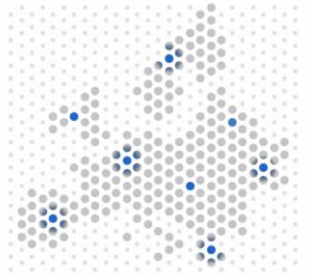


BE-CYBER
Cyber Security Coalition



Cyber Renaissance

22/09/2026 La Sucrierie, Wavre



BIGDATPOL

Towards an evidence-based
model for big data policing



LET ME INTRODUCE MYSELF

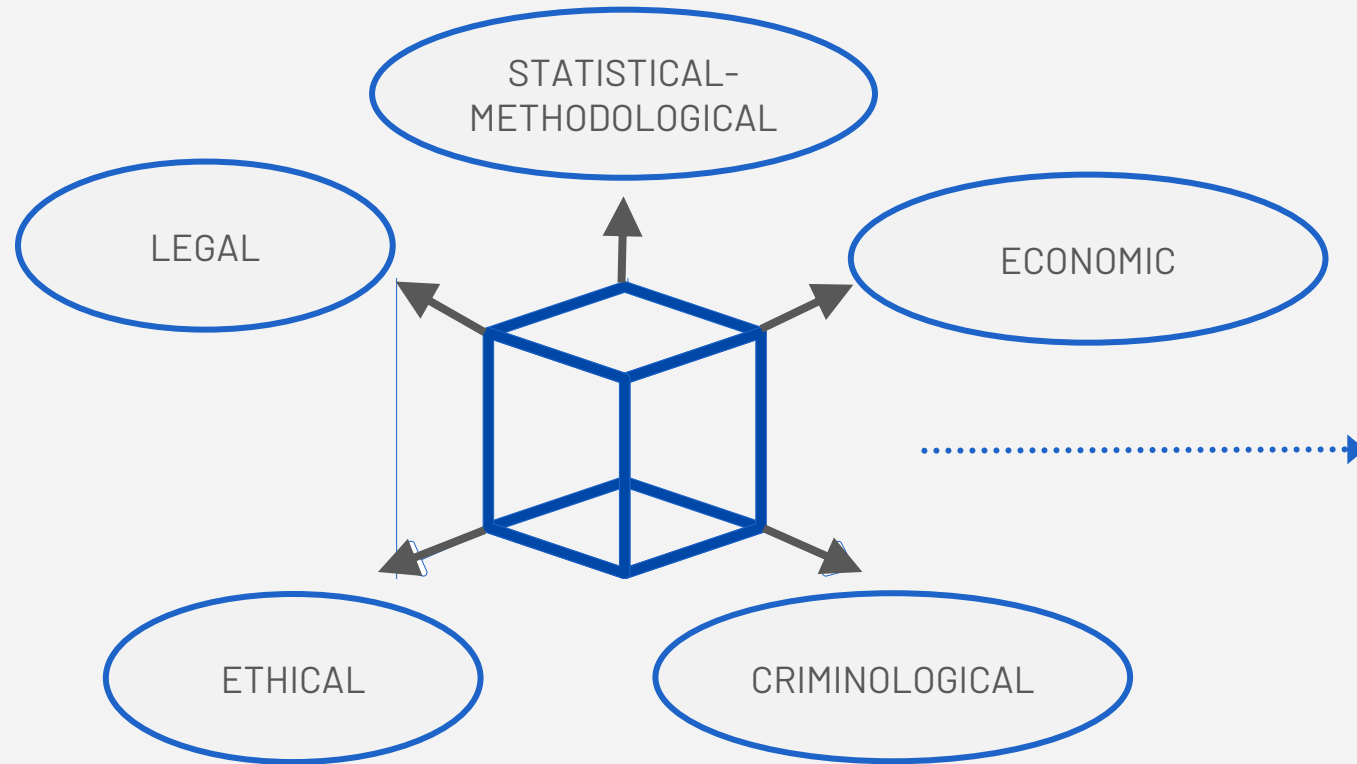
Prof Dr Wim Hardyns

- Professor Criminology (Ghent University) and Security Sciences (University of Antwerp)
- ERC Consolidator Grant holder
- Principal Investigator BIGDATPOL research programme
- [LinkedIn](#)
- Wim.Hardyns@UGent.be

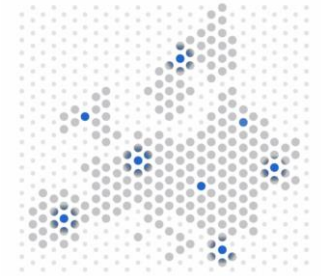


Research programme objective

Develop evidence-based 5D models for big data policing



Field tests



BIGDATPOL

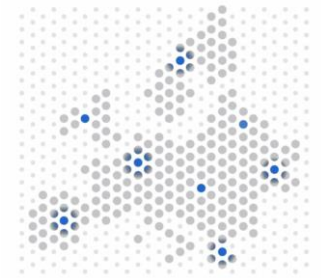
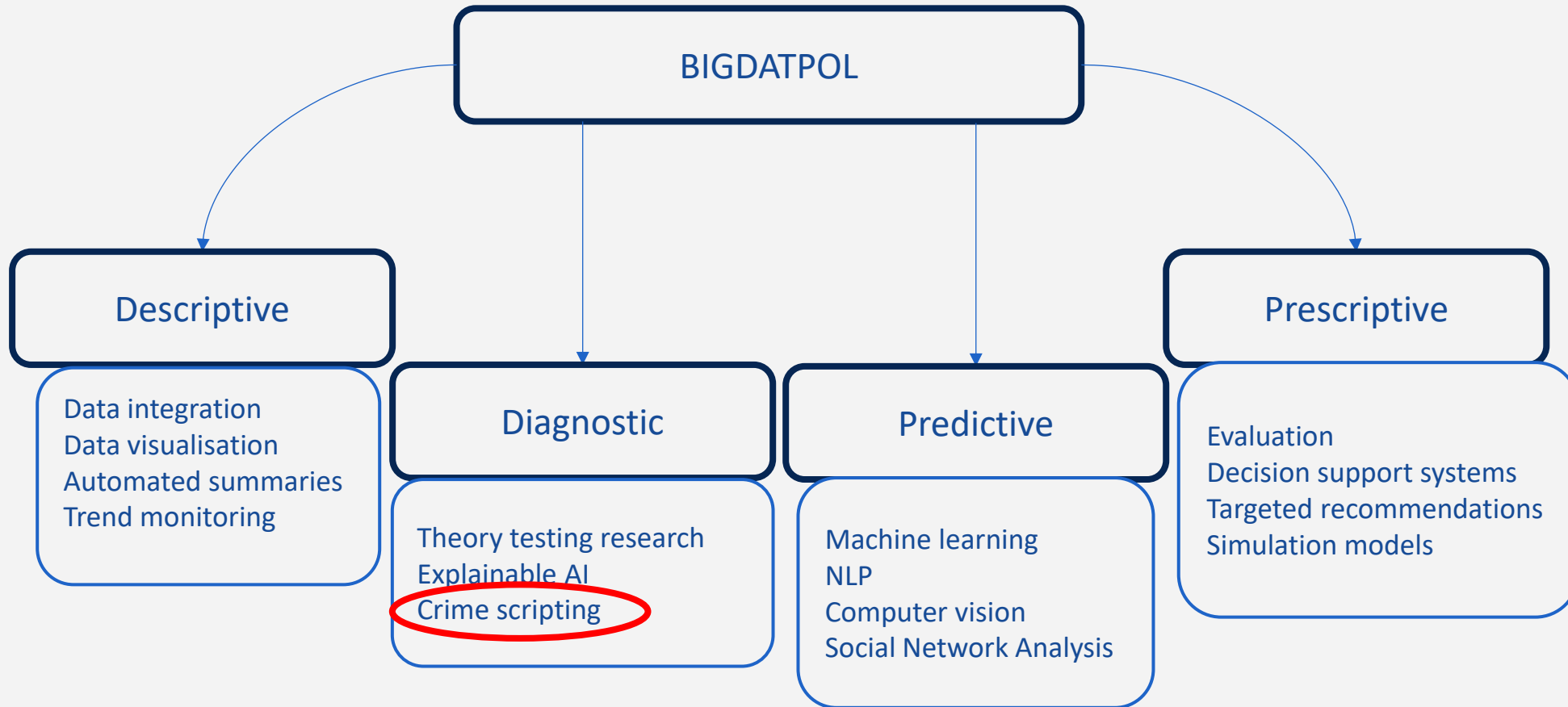
Towards an evidence-based
model for big data policing



Funded by
the European Union



BIGDATPOL FRAMEWORK



BIGDATPOL

Towards an evidence-based
model for big data policing



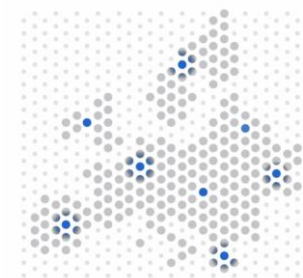
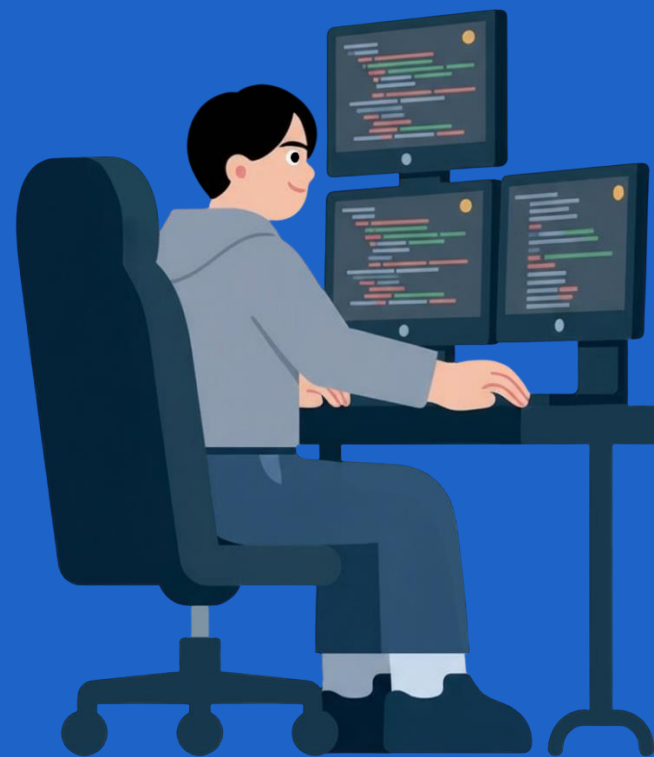
Funded by
the European Union



European Research Council
Established by the European Commission

“

If cyberattacks are carried out by people, why do we still design our defences as if they were purely technical events?



BIGDATPOL

Towards an evidence-based
model for big data policing



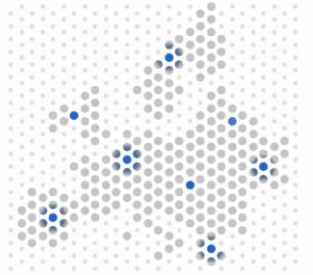
Funded by
the European Union



European Research Council
Established by the European Commission

PRESENTATION OVERVIEW

- 01 Rethinking cyberattacks**
From technical events to human choices
- 02 Understanding attackers and their choices**
Actors, pathways, ecosystems, opportunity and AI
- 03 Crime scripting as a method**
From individual decisions to an intervention-ready script
- 04 Lessons from three cases**
Scattered Spider, LockBit and scam compounds
- 05 Implications for defence and research**
Prevention, organisational design and BIGDATPOL



BIGDATPOL

Towards an evidence-based
model for big data policing



Funded by
the European Union



European Research Council
Established by the European Commission

A cyberattack is a socio-technical process

CONTEXT

Markets • geopolitics • regulation • inequality

ECOSYSTEM

Communities • service providers • brokers • money mules

ORGANISATION

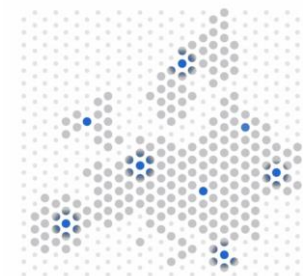
Routines • incentives • trust • access governance

DECISION

Goal • target • timing • method • exit

TECHNICAL ACT

Credential abuse • malware • exploitation • transfer



BIGDATPOL

Towards an evidence-based
model for big data policing

- 01 Rethinking cyberattacks**
From technical events to human choices
- 02 Understanding attackers and their choices**
Actors, pathways, ecosystems, opportunity and AI
- 03 Crime scripting as a method**
From individual decisions to an intervention-ready script
- 04 Lessons from three cases**
Scattered Spider, LockBit and scam compounds
- 05 Implications for defence and research**
Prevention, organisational design and BIGDATPOL



Funded by
the European Union



erc
European Research Council
Established by the European Commission

From telemetry to explanation

TECHNICAL EVIDENCE

What happened?

Which technique?

Which system failed?

Which indicator remains?

HUMAN & CRIMINOLOGICAL EVIDENCE

+

Why this target and this moment?

+

Who enabled or collaborated?

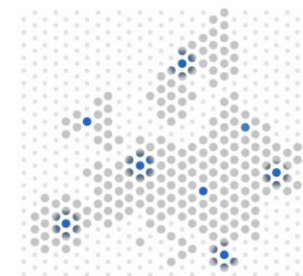
+

Which choice or routine was exploited?

+

Where can the process be disrupted?

Better defence requires both columns.



BIGDATPOL

Towards an evidence-based
model for big data policing



Funded by
the European Union

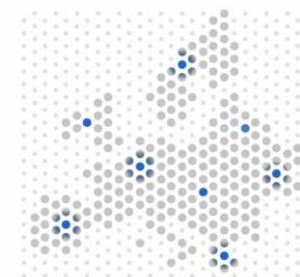


European Research Council
Established by the European Commission

Different actors, different decision logics

ACTOR LOGIC	PRIMARY GOAL	WHAT SHAPES TARGET CHOICE
PROFIT-DRIVEN	Revenue and repeatability	Access, payment capacity, low friction
STATE-LINKED	Strategic advantage	Intelligence value, persistence, deniability
IDEOLOGICAL	Attention and symbolic impact	Visibility, timing, narrative value
INSIDER / GRIEVANCE	Personal gain or retaliation	Privileged access, perceived injustice

- These are analytical logics, not fixed profiles. Actors and motives can overlap or change.
- Pathways are cumulative, not linear



BIGDATPOL

Towards an evidence-based
model for big data policing

- 01 **Rethinking cyberattacks**
From technical events to human choices
- 02 **Understanding attackers and their choices**
Actors, pathways, ecosystems, opportunity and AI
- 03 **Crime scripting as a method**
From individual decisions to an intervention-ready script
- 04 **Lessons from three cases**
Scattered Spider, LockBit and scam compounds
- 05 **Implications for defence and research**
Prevention, organisational design and BIGDATPOL



Funded by
the European Union



European Research Council
Established by the European Commission

Cybercrime markets turn capability into a service

IDENTITY & DATA

stolen credentials
session cookies
target lists

ACCESS

initial access
phishing kits
botnet capacity

EXECUTION

malware
ransomware
negotiation

MONETISATION

money mules
laundering
crypto conversion

80M+

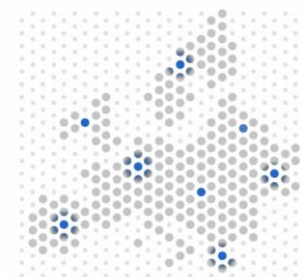
account-access credentials
advertised by Genesis Market

2,000+

victims attributed to LockBit
before Operation Cronos

MODULAR

skills can be bought, rented or
brokered



BIGDATPOL

Towards an evidence-based
model for big data policing



Funded by
the European Union



European Research Council
Established by the European Commission

Attackers decide under bounded rationality

PERCEIVED REWARD

Expected value
Status • profit • strategic impact

EFFORT

Skills, time, access,
coordination and tool
costs

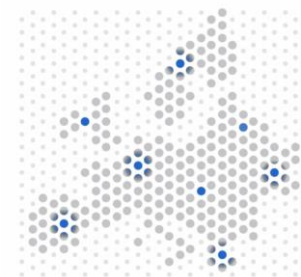
RISK

Detection, attribution,
sanctions and betrayal

UNCERTAINTY

Incomplete information,
bias, urgency and learning

A choice can be rational to the offender without being objectively optimal.



BIGDATPOL

Towards an evidence-based
model for big data policing



Funded by
the European Union



European Research Council
Established by the European Commission

Which target would you choose?

A

High value
Strong controls
High visibility

B

Moderate value
Weak process
Low friction

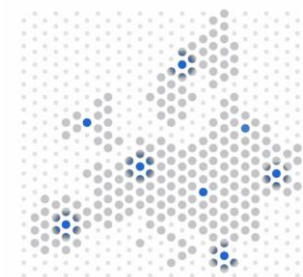
C

Low value
Many similar targets
Easy to scale

ATTACKER VIEW Perceived attractiveness, accessibility and guardianship

BIGDATPOL VIEW Empirical concentrations of risk across time, place, networks and organisations

The strongest prevention targets are where perceived opportunity and measured risk converge.



BIGDATPOL

Towards an evidence-based
model for big data policing



Funded by
the European Union

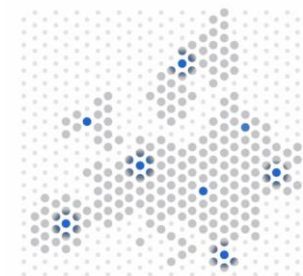


European Research Council
Established by the European Commission

AI changes the cost structure, not criminal intent

MECHANISM	WHAT MAY CHANGE	DEFENSIVE CONSEQUENCE
ACCESSIBILITY	Language and technical assistance can lower entry costs	More actors can attempt competent-looking attacks
SPEED	Research, drafting and variation can be accelerated	More iterations in less time
SCALE	Content and targeting can be generated in volume	Cheap expansion across targets
PERSONALISATION	Messages can be adapted to roles and contexts	Potentially more credible persuasion

Human actors still define goals, select targets, deploy tools and decide how outputs are used.



BIGDATPOL

Towards an evidence-based
model for big data policing

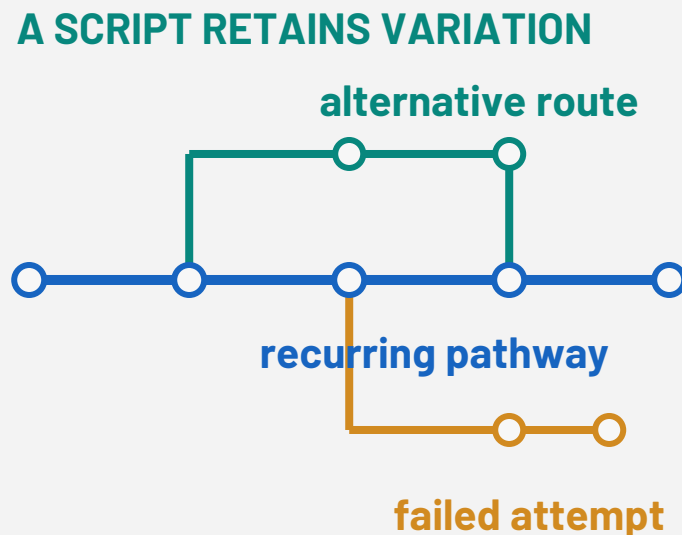


Funded by
the European Union



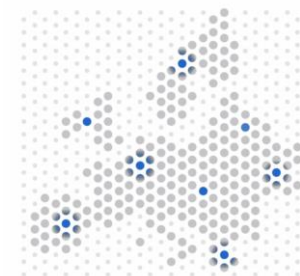
European Research Council
Established by the European Commission

Crime scripting as an analytical method



Cases are compared to model recurring pathways without forcing every offence into a single sequence.

A credible script records variation and uncertainty; it does not force every case into one sequence.



BIGDATPOL

Towards an evidence-based model for big data policing

- 01 **Rethinking cyberattacks**
From technical events to human choices
- 02 **Understanding attackers and their choices**
Actors, pathways, ecosystems, opportunity and AI
- 03 **Crime scripting as a method**
From individual decisions to an intervention-ready script
- 04 **Lessons from three cases**
Scattered Spider, LockBit and scam compounds
- 05 **Implications for defence and research**
Prevention, organisational design and BIGDATPOL

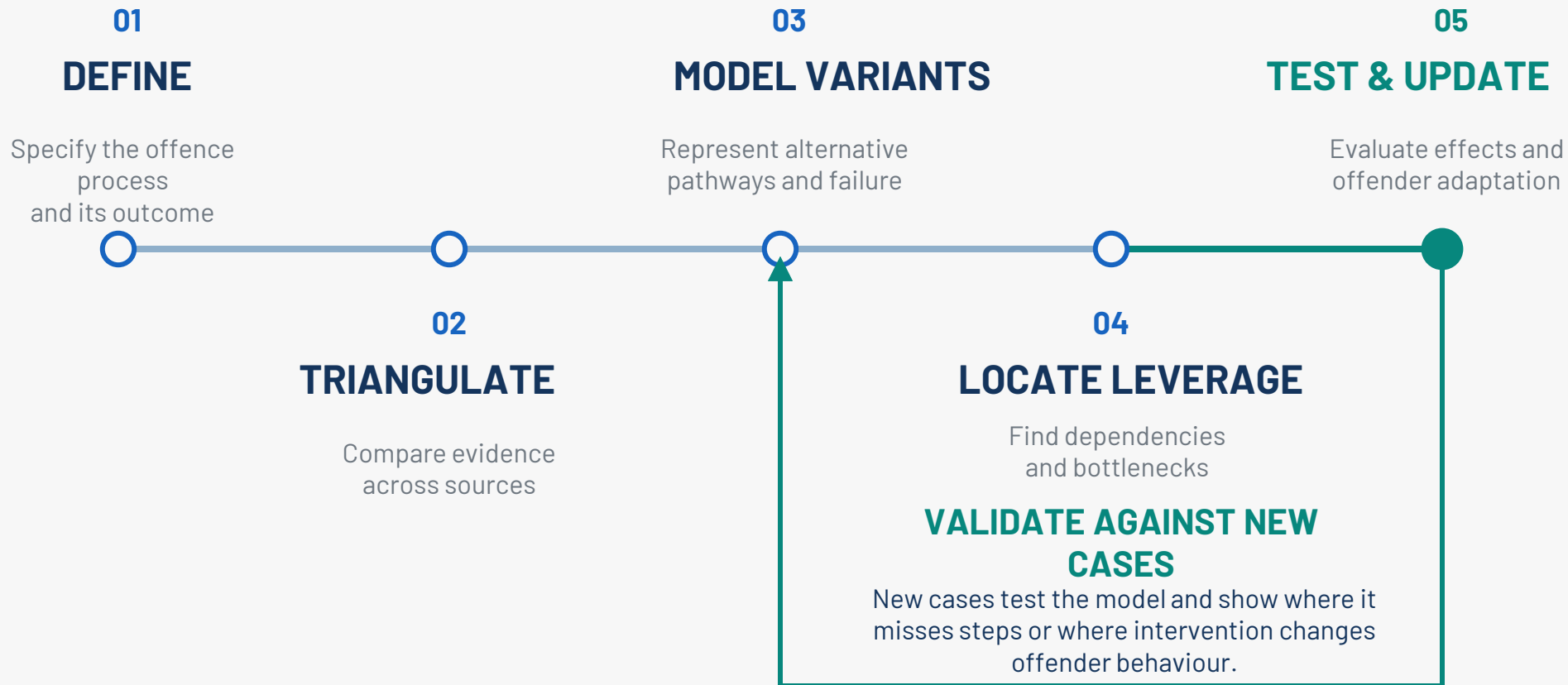


Funded by
the European Union



European Research Council
Established by the European Commission

From cases to an intervention-ready script



The script is revised when new evidence or changes in offending challenge the model.

Business email compromise as a decision process

1 SELECT

valuable & reachable

2 PREPARE

learn routines

3 CRAFT

credible request

4 DELIVER

right channel & time

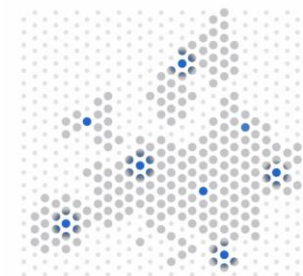
5 CONVERT

bypass checks

6 MOVE

retain proceeds

Each stage contains actors, choices, tools, evidence and intervention points.



BIGDATPOL

Towards an evidence-based
model for big data policing



Funded by
the European Union

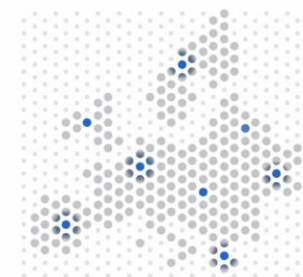


European Research Council
Established by the European Commission

Crime script part I – constructing credibility

LENS	SELECT	PREPARE	CRAFT
ACTORS	Scout / broker	Researcher / account user	Impersonator / writer
CHOICE	Which target is worth pursuing?	Which routine can be imitated?	Which request will feel legitimate?
TOOLS & AI	Public data, breach data	Inbox search, language analysis	Drafting, translation, variants
INTERVENE	Reduce exposed role data	Detect anomalous access; limit mailbox history	Trusted domains; pre-agreed payment rules

AI can support specific tasks; it does not replace target selection or criminal intent.



BIGDATPOL

Towards an evidence-based model for big data policing



Funded by
the European Union

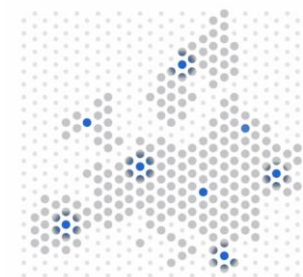


European Research Council
Established by the European Commission

Crime script part II – converting trust into proceeds

LENS	DELIVER	CONVERT	MOVE
ACTORS	Sender / compromised account	Victim + approver	Mule recruiter / launderer
CHOICE	When and through which channel?	How can verification be bypassed?	How quickly can funds be dispersed?
TOOLS & AI	Look-alike domains, messaging	Adaptive replies, invoice changes	Accounts, transfers, crypto services
INTERVENE	Authentication and domain controls	Independent callback; dual approval	Rapid reporting; transaction holds; mule disruption

The offence is not complete at payment: retaining and laundering proceeds is part of the script.



BIGDATPOL

Towards an evidence-based
model for big data policing



Funded by
the European Union



European Research Council
Established by the European Commission

Case 1 - Scattered Spider: identity is infrastructure

PUBLIC INFORMATION

HELP DESK

IDENTITY RESET

CLOUD ACCESS

HUMAN CHOICE

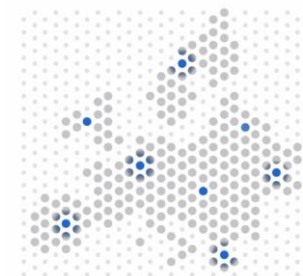
Impersonate staff and exploit pressure on support personnel

ORGANISATIONAL CONDITION INTERVENTION

Identity recovery relied on information the attacker could reproduce

High-assurance recovery, phishing-resistant MFA, anomaly checks and escalation

Lesson: the help desk is not outside the security perimeter. It is part of the identity control system.



BIGDATPOL

Towards an evidence-based model for big data policing

- 01 **Rethinking cyberattacks**
From technical events to human choices
- 02 **Understanding attackers and their choices**
Actors, pathways, ecosystems, opportunity and AI
- 03 **Crime scripting as a method**
From individual decisions to an intervention-ready script
- 04 **Lessons from three cases**
Scattered Spider, LockBit and scam compounds
- 05 **Implications for defence and research**
Prevention, organisational design and BIGDATPOL

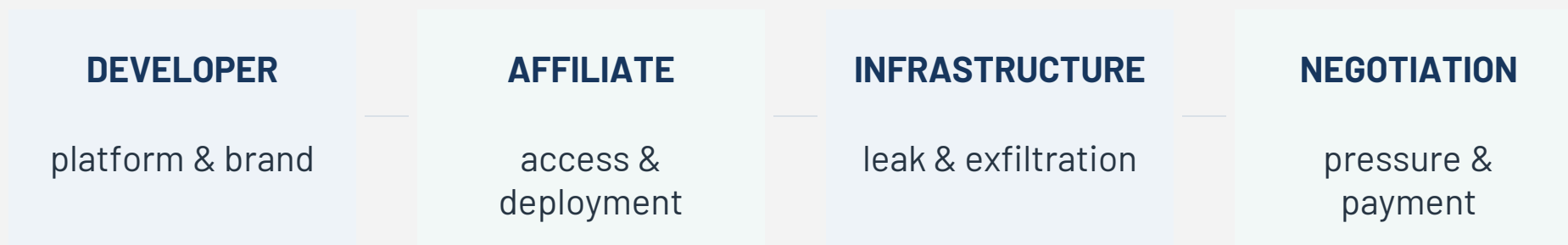


Funded by
the European Union



European Research Council
Established by the European Commission

Case 2 - LockBit: disrupt the business system



2,000+

victims attributed to LockBit

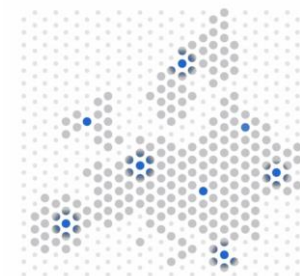
28

affiliate servers taken down

3

countries hosting seized core infrastructure

Operation Cronos targeted shared infrastructure and trust. Leverage points used by many affiliates.



BIGDATPOL

Towards an evidence-based
model for big data policing



Funded by
the European Union



erc
European Research Council
Established by the European Commission

Case 3 - scam compounds as coercive enterprises

RECRUIT

Workers are recruited – and some are trafficked or coerced

TRAIN

Scripts, personas, language and platform routines

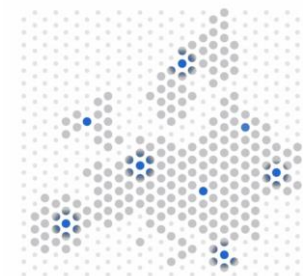
OPERATE

Target lists, shifts, supervision and performance pressure

MONETISE

Payments, crypto, laundering and cross-border networks

One operation can contain offenders, facilitators and victims of trafficking at the same time.



BIGDATPOL

Towards an evidence-based
model for big data policing



Funded by
the European Union



European Research Council
Established by the European Commission

Design defence around the offender's process

BEFORE ACCESS

Reduce exposed data
Harden identity recovery
Disrupt illicit access
markets

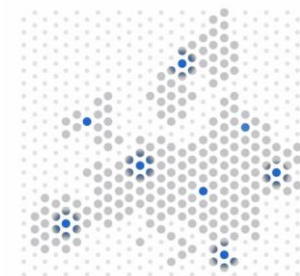
DURING ATTACK

Detect behavioural
anomalies
Add friction at high-risk
decisions
Create trusted escalation
paths

AFTER ACTION

Report rapidly
Freeze and recover funds
Share evidence across
sectors

Portfolio principle: combine controls that raise effort, increase risk, reduce reward and support recovery.



BIGDATPOL

Towards an evidence-based
model for big data policing

- 01 **Rethinking cyberattacks**
From technical events to human choices
- 02 **Understanding attackers and their choices**
Actors, pathways, ecosystems, opportunity and AI
- 03 **Crime scripting as a method**
From individual decisions to an intervention-ready script
- 04 **Lessons from three cases**
Scattered Spider, LockBit and scam compounds
- 05 **Implications for defence and research**
Prevention, organisational design and BIGDATPOL



Funded by
the European Union



European Research Council
Established by the European Commission

Human-centred security is not human blame

FRAGILE DESIGN

One click can authorise loss

Recovery relies on trivia

Speed is rewarded over verification

Reporting feels punitive

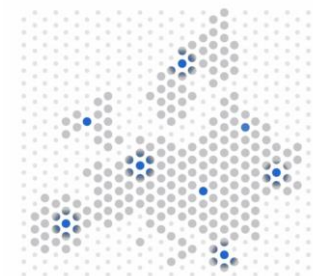
RESILIENT DESIGN

Consequential actions need confirmation

Recovery uses high-assurance evidence

Pausing is legitimate and easy

Early reporting is safe and useful



BIGDATPOL

Towards an evidence-based
model for big data policing



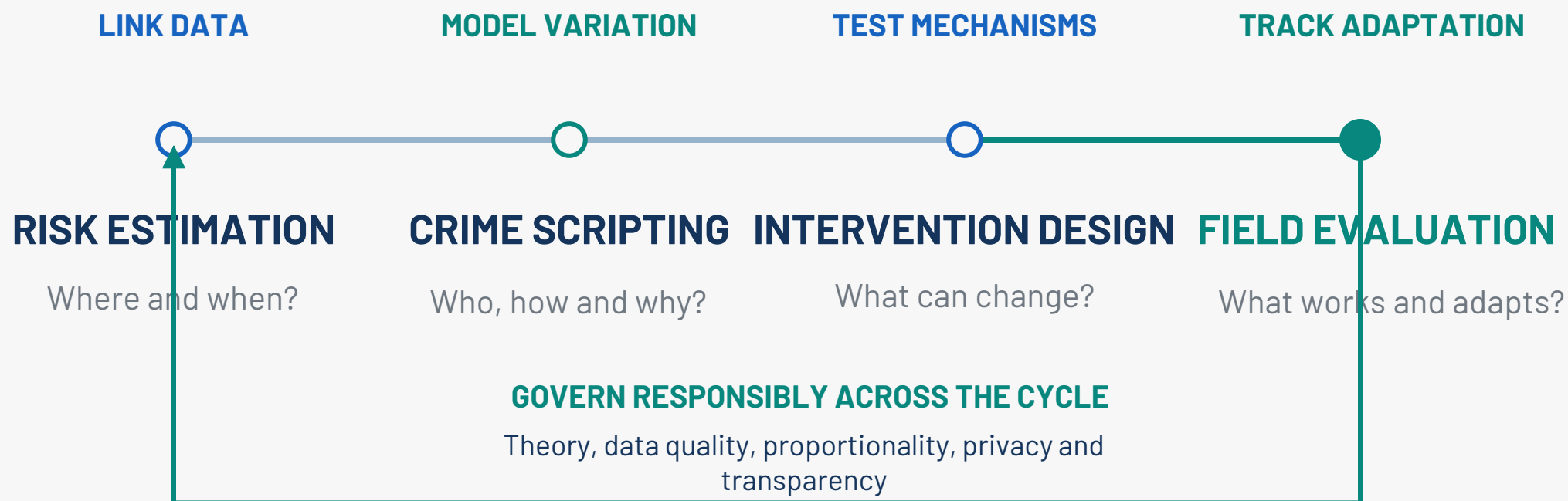
Funded by
the European Union



European Research Council
Established by the European Commission

Design systems and routines that absorb predictable error, pressure and manipulation.

BIGDATPOL: from evidence to evaluated intervention



Measure prevented harm, recovery, adaptation and unintended effects, not detections alone.



BIGDATPOL

Towards an evidence-based
model for big data policing



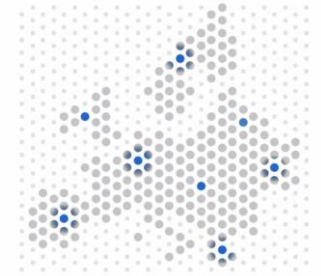
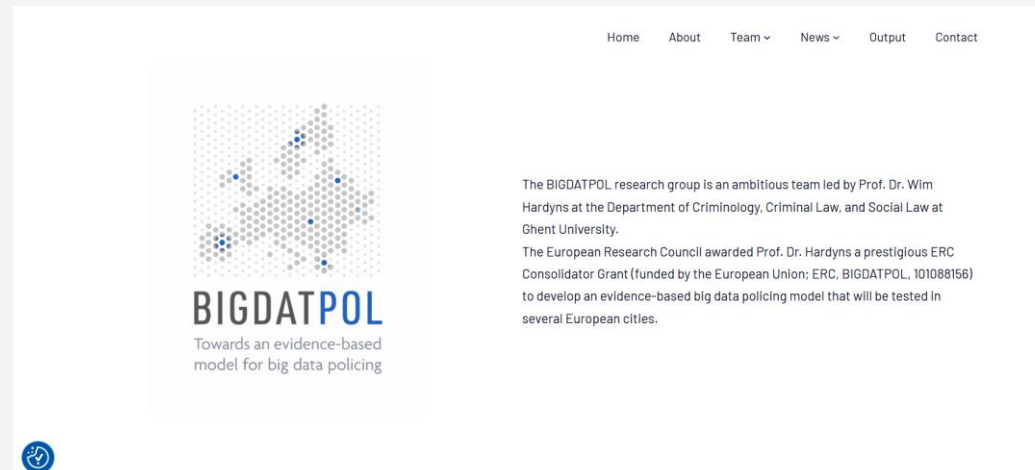
JOIN OUR NETWORK

- LinkedIn page BIGDATPOL



- Wim.Hardyns@UGent.be

- WWW.BIGDATPOL.COM



BIGDATPOL

Towards an evidence-based
model for big data policing





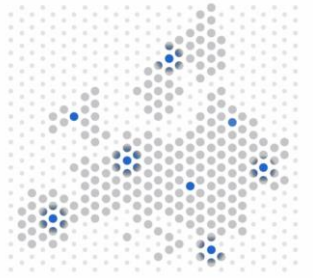
Q&A

The background features a blue-tinted city skyline with various skyscrapers. Overlaid on this is a white network diagram consisting of lines, circles, and arrows, suggesting a digital or technological theme.

Acknowledgements



Funded by the European Union (ERC, BIGDATPOL, 101088156). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them.



BIGDATPOL

Towards an evidence-based
model for big data policing



Funded by
the European Union



European Research Council
Established by the European Commission

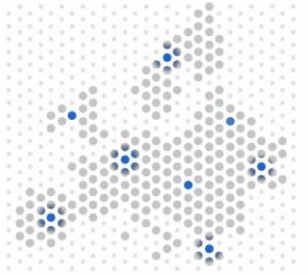
THANK YOU FOR LISTENING!

PROF. DR. WIM HARDYNS



REFERENCES

- Clarke, R. V. (1995). Situational crime prevention. *Crime and justice*, 19, 91-150.
- Clarke, R. V. G. (1992). Situational crime prevention: Successful case studies.
- Cohen, L. E., & Felson, M. (2010). Social change and crime rate trends: A routine activity approach (1979). In *Classics in environmental criminology* (pp. 203-232). Routledge.
- Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime prevention studies*, 3(1), 151-196.
- Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime prevention studies*, 16, 41-96.
- CyPro. (n.d.). *Crime script analysis in cyber attacks: BEC case study*. [CyPro BEC Case Study](#)
- Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime*, 14(2-3), 175-196.
- Dehghanniri, H., & Borrion, H. (2021). Crime scripting: A systematic review. *European Journal of Criminology*, 18(4), 504-525.
- Emerging Technology Lab. (2023). *Briefing on MGM cyberattack and Scattered Spider*.
- European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. Publications Office of the European Union. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. Publications Office of the European Union. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- Europol. (2026). *Internet organised crime threat assessment (IOCTA) 2026: The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime*. Publications Office of the European Union.



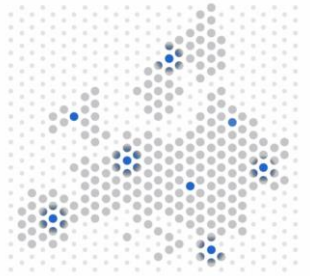
BIGDATPOL

Towards an evidence-based
model for big data policing



REFERENCES

- Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.
- Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, 31(2), 165–177.
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensics: An introduction* (2nd ed.). Routledge.
- Ho, H., Ko, R., Mazerolle, L., Gilmour, J., & Miao, C. (2024). Using Situational Crime Prevention (SCP)-C3 cycle and common inventory of cybersecurity controls from ISO/IEC 27002: 2022 to prevent cybercrimes. *Journal of Cybersecurity*, 10(1), tyae020.
- INTERPOL. (2025). *Cybercrime*. International Criminal Police Organization.
- Leukfeldt, E. R. (2014). *Cybercrime and social ties*. Eleven International Publishing.
- Leukfeldt, E. R., & Holt, T. J. (2020). Examining the social organization practices of cybercriminals in the Netherlands online and offline. *International Journal of Offender Therapy and Comparative Criminology*, 64(5), 522–538.
- Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, 67(1), 21–37.
- Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*, 67(1), 39–53.
- National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce. <https://www.nist.gov/cyberframework>
- O'Kane, Philip, Sakir Sezer, and Domhnall Carlin. "Evolution of ransomware." *IET networks* 7, no. 5 (2018): 321–327.



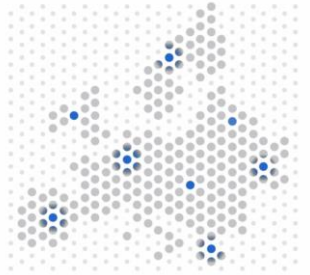
BIGDATPOL

Towards an evidence-based
model for big data policing



REFERENCES

- Specops Software. (2023). *MGM Resorts service desk hack*.
- United Nations Office on Drugs and Crime. (n.d.). *Cybercrime module 9: Situational crime prevention*. United Nations Office on Drugs and Crime.
- Verizon. (2024). *2024 data breach investigations report (DBIR)*. Verizon.
- Yar, M. (2006). *Cybercrime and society*. SAGE Publications Ltd.



BIGDATPOL

Towards an evidence-based
model for big data policing

