CC-DRIVER

Researching cybercriminality to design new methods to prevent, investigate and mitigate cybercriminal behaviour.

Policy Brief No. 7

November 2022

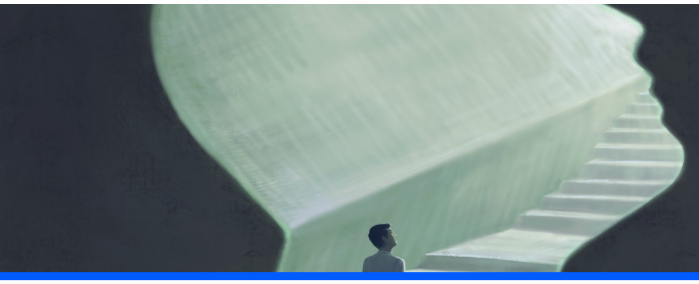
Who is this for?

This policy brief gives an outline of cybercrime definitions, typologies and taxonomies and provides recommendations for future work. Included is a new classification framework to understand cybercrime and cyberdeviance. This policy brief, therefore, is designed for all professionals working within the area of cybercrime and key stakeholders, including LEAs, Academics, Criminal Justice, Policy Makers, Educators and others who work with young people, children and young people.

Highlights

1. The lack of clarity surrounding the term cybercrime has significant impact on society, cybercrime policy, legal intervention and academic research.
2. No single classification system fully encapsulated cybercrime concepts or accurately reflected the nebulous nature of cybercrime acts.
3. There is remaining ambiguity as to what exactly constitutes a cybercrime and it is likely that a clear conceptualisation of cybercrime will continue to be challenge.
4. This review presents key cybercrime definitions, categorisations of cybercrime and typologies of cybercrime.
5. This review presents a new framework with which to conceptualise cybercrime.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.



CC-DRIVER

Cybercrime definitions, typologies and taxonomies

Purpose & methodology

This policy brief presents a review of cybercrime definitions, typologies and taxonomies. The corresponding journal publication includes 4 distinctive sections:

- An overview of methods, scope and aims
- An overview of cybercrime definitions, typologies and taxonomies
- Key challenges and recommendations
- Conclusions

The aim was to conduct a broad review of the key typologies of cybercrime in academia and the connections with traditional crime.

Method:

- Parameterized literature review
- Boolean search string identified 38,700 relevant materials
- Materials narrowed according to pre-defined parameters and relevance
- 47 sources informed the review

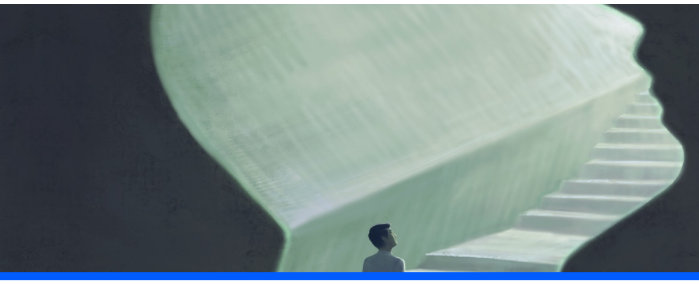
Researchers at the University of East London (UEL) lead this activity. The team consisted of: Prof Julia Davidson (Co-Principal Investigator, UEL), Prof Mary Aiken (Co-Principal Investigator, UEL), Prof Stefano Caneppele (Collaborating Researcher, UNIL), Christine Burkhardt (Researcher, UNIL), Kirsty Phillips (Research Assistant, UEL), Ruby Farr (Research Assistant, UEL).

Context: Cybercrime terminology

"A veritable arsenal of terminology is used, sometimes in combination with the prefixes cyber, computer, e-, internet, digital or information. Terms are bandied around, applied randomly, reflect overlap in content or reflect important gaps." [1, p. 19].

- Alternative terminology includes, for example: "cyberspace crime", "computer crime", "computer-related crime", "electronic crime", "e-crime", "technology-enabled crime", and "high-tech crime". [2, 3, 4]
- The variability in cybercrime terms and language highlights the lack of a shared lexicon amongst professionals working in the field.
- A clear conceptualisation of cybercrime is vital, as even small variations in the conceptualisation of cybercrime could affect the measurement of, and response to, cybercrime behaviours. [4]
- The problem is further compounded differences in by the fact that cybercrime legislation across jurisdictions which leads to cybercrimes being weighted and considered differently across jurisdictions. [5, 6]

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.



1. Findings: Cybercrime definitions

- It is broadly acknowledged that the term "cybercrime" is used to account for a variety of crimes and harmful behaviours.
- The term encompasses a wide number of acts, crimes or illicit conduct perpetrated by both individuals or groups against computers, computer-related devices, or information technology networks, as well as traditional crimes that are facilitated or maintained by the use of the internet and/or information technology. [7]
- A recent review identified the two most commonly cited academic definitions of cybercrime [9]:

> Thomas and Loader define cybercrime as *"computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks."* [12, p. 3]

> Gordon and Ford define cybercrime as *"any crime that is facilitated or committed using a computer, network, or hardware device."* [13, p. 14]

- *A principal finding of the review and the only consensus within the literature, is that there is no single clear, precise and universally accepted definition of cybercrime [3, 6, 7, 8, 9, 10, 5]: a fact that is acknowledged by both academics and organisations alike [8, 6, 11, 10].*

2. Findings: Categorising cybercrime

2 Factor		3 Factor	
Spectrum Approach [13]	**Categorical Approach [14]**	**Wall's Approach [15]**	**The European Commission's Approach [16]**
2006	**2007**	**2007**	**2013**
Type I	Cyber-dependent	"Crimes against the machine", a.k.a. computer integrity crimes	"Offences unique to computers and information systems (e.g., attacks against information systems, denial of service and malware)"
Type II	Cyber-enabled	"Crimes using the machine", a.k.a. computer assisted crimes	Traditional offences (e.g., fraud, forgery, and identity theft)
		"Crimes in the machine", a.k.a. computer content crimes	Content-related offences (e.g., online distribution of CSAM)
Academic	Academic & Institutional	Academic	Institutional

- The 2 Factor categorical approach, originally proposed by Brenner [14], which distinguishes between "cyber-enabled" vs. "cyber-dependent" crime is the most widely used and has been consistently adopted by researchers and policy makers. [17, 3, 10]

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

- There is broad agreement between both 2-factor systems as two what the two dimensions of cybercrime ought to be, however Gordon and Ford [13] propose that Type I and Type II cybercrimes represent the opposite ends of a cybercrime spectrum rather than distinct categories.
- Extensions have been added to 2-factor approaches:
  - Wall [18] added "cyber-assisted" crimes the categorical approach to account for the incidental involvement of technology in traditional crimes.
  - Sarre, Lau, and Chang [3] extend the spectrum approach through the addition of "Type III" cybercrimes to account for the use of advanced technology in the commission of crimes.
- Wall's [15] three category classification system was one of the first reported in academic literature and is therefore often cited, this approach was also adopted a few years later by the European Commission [16, p. 3, 10] however the terminology used differs to that of Wall.
- 3-factor approaches are advantageous over 2-factor approaches as there is greater appreciation of the breadth of cyber-enabled criminal behaviours.
- 3-factor approaches further distinguish between crimes against property and crimes against people and more accurately capture the breadth of cybercriminal behaviours.

Cyber-dependent crimes are crimes that arose with the advent of technology and cannot exist (i.e., dependent) outside of the digital world

Cyber-enabled crimes are traditional crimes that predate the advent of the technology, that are now facilitated or have been made easier (i.e., enabled) by cyber technology.

3. Findings: Typologies of cybercrime

- Four typologies were identified that illustrate the extent of the variation between prominent and most up-to-date typologies promoted in the academic literature:
  - The Council of Europe's (COE) Convention of Cybercrime typology is the single most important classification system as it represents "the only globally recognized agreement around cybercrime." [19, 20, p. 19]
  - Wall's [21] classification system was one of the first attempts to develop a typology in academic literature, which incidentally coincides with the time in which the COE typology proposed and yet significantly diverges from this approach.
  - Conversely, the Tsakalidis and Vergidis' [22] later classification system is rooted in the COE's typology (as acknowledged by the authors).
  - However, academic authors Marcum and Higgins [23] later classification system like Walls' typology significantly diverges from the COE's classification system and places equal emphasis on person-target based offenses.
- Each typology has identifiable gaps and does not represent a comprehensive classification of cybercrime offenses.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

4. Consolidating findings: A new framework

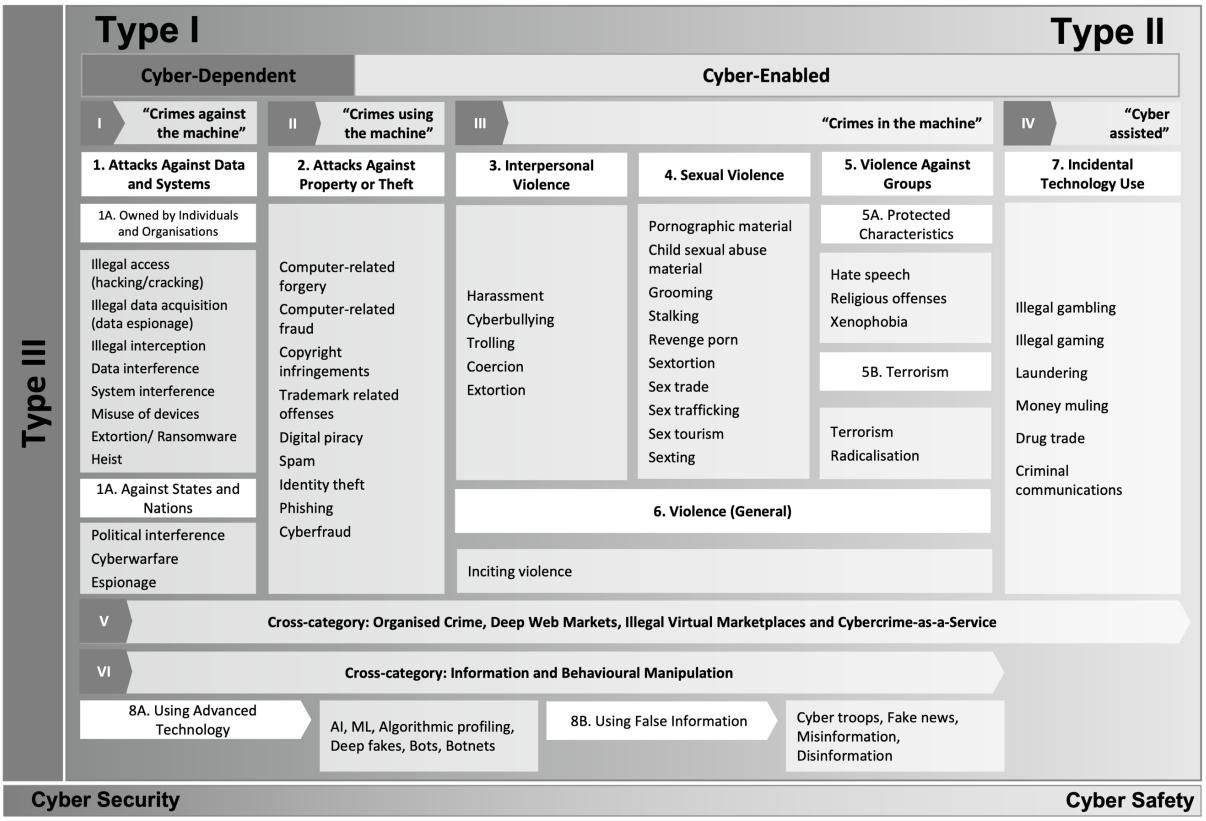


***Figure 1**: A new cybercrime and cyberdeviance classification framework to consolidate the findings of this review.*

This framework reads left to right (from technical to human) and includes:

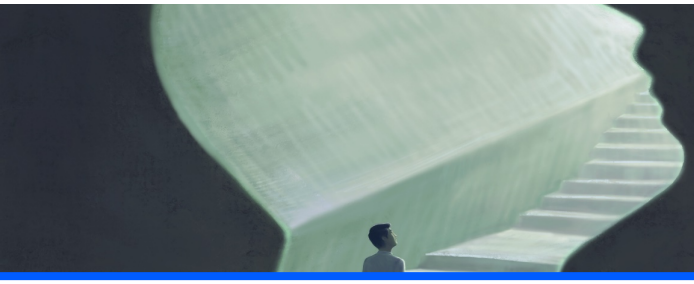
- the overarching spectrum - from where the use of technology is incidental to uses of advanced technology in the commission of crime online
- the categorical approach - cyber-dependent vs. cyber-enabled crimes
- 6 sub-categories (I-VI) that cover the entire spectrum
- 8 subtypes within these categories
- the corresponding "solutions" context - from cyber security measures to cyber safety measures ("SafetyTech") [24]

Recommendations

The purpose of the above framework is to map and facilitate discussion and analysis of the many inter-related topics and dynamics included under the umbrella term of 'cybercrime'. A key recommendation for future work is to develop a systematic, purposeful, and holistic classification system, that is evidence-based, flexible, readily updated, supported by a dedicated research initiative, and incorporates multidisciplinary input and international cooperation.

Authors:
Kirsty Phillips, Professor Julia Davidson, Ruby Farr, Christine Burkhardt, Professor Stefano Caneppele and Professor Mary Aiken

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.



CC-DRIVER

References

[1] R. C. Van der Hulst and R. J. M. Neve, High Tech Crime. Literature review about crimes and their offenders, The Hague: WODC (Research and Documentation Centre), 2008.
[2] L. Y. C. Chang, Cybercrime in the Greater China Region: Regulatory responses and crime prevention across the Taiwan Strait, Cheltenham: Edward Elgar Publishing, 2012.
[3] R. Sarre, L. Y.-C. Lau and L. Y. C. Chang, "Responding to cybercrime: current trends," Police Practice and Research, vol. 19, no. 6, pp. 515-518, 2018.
[4] M. McGuire, "It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime," in The Human Factor of Cybercrime, R. Leukfeldt and T. J. Holt, Eds., New York, Routledge, 2020, pp. 3-28.
[5] A. Black, K. Lumsden and L. Hadlington, "'Why Don't You Block Them?'Police Officers' Constructions of the Ideal Victim When Responding to Reports of Interpersonal Cybercrime," in nline Othering: Exploring Violence and Discrimination on the Web, K. Lumsden and E. Harmer, Eds., Basingstoke, Palgrave Macmillan, 2019, pp. 355-378.
[6] E. C. Viano, "Cybercrime: Definition, Typology, and Criminalization," in Cybercrime, Organized Crime, and Societal Responses, E. C. Viano, Ed., Cham, Switzerland, Springer International Publishing, 2017, pp. 3-22.
[7] C. Donalds and K. M. Osei-Bryson, "Toward a cybercrime classification ontology: A knowledge-based approach," Computers in Human Behavior, vol. 92, pp. 403-418, 2019.
[8] S. Broadhead, "The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments," Computer Law & Security Review, vol. 34, no. 6, pp. 1180-1196, 2018.
[9] N. Akdemir, B. Sungur and B. U. Başaranel, "Examining the Challenges of Policing Economic Cybercrime in the UK," Güvenlik Bilimleri Dergisi (International Security Congress Special Issue), vol. Özel Sayı, pp. 111-132, 2020.
[10] L. Paoli, J. Visschers, C. Verstraete and E. Van Hellemont, "The Impact of Cybercrime on Belgian Businesses," Intersentia, 2018.
[11] A. A. Gillespie, Cybercrime: Key Issues and Debates, New York: Routledge, 2015.
[12] D. Thomas and B. Loader, "Cybercrime: Law Enforcement, Security and Surveillance in the Information Age," in Cybercrime: Law enforcement, security and surveillance in the information age, D. Thomas and B. Loader, Eds., London, Routledge, 2000.
[13] S. Gordon and R. Ford, "On the Definition and Classification of Cybercrime," Journal in Computer Virology, vol. 2, no. 1, pp. 13-20, 2006.
[14] S. Brenner, "Cybercrime: Re-thinking crime control strategies," in Crime online, Y. Jewkes, Ed., Cullompton, United Kingdom, Willan Publishing, 2007, p. 12–28.
[15] D. S. Wall, Cybercrime: The transformation of crime in the information age, Cambridge: Polity Press, 2007.
[16] European Commission, "Cybersecurity strategy of the European Union: An open, safe and secure cyberspace.," 7 February 2013. [Online]. Available: www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.. [Accessed 8 July 2020].
[17] M. McGuire and S. Dowling, "Cybercrime: A review of the evidence: Summary of key findings and implications," Home Office, London, 2013.
[18] D. S. Wall, "The Internet as a Conduit for Criminals," in Information Technology and the Criminal Justice System, Thousand Oaks, CA, Sage, 2005/15, pp. 77-98.
[19] Council of Europe , "Convention on cybercrime," European Treaty Series, vol. No. 185, pp. 1-25, 2001.
[20] M. McGuire, "It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime," in The Human Factor of Cybercrime, R. Leukfeldt and T. J. Holt, Eds., New York, Routledge, 2020, pp. 3-28.
[21] D. S. Wall, "Cybercrime and the Internet," in Crime and the internet , D. S. Wall, Ed., New York, NY, Routledge, 2001, pp. 1-17.
[22] G. Tsakalidis and K. Vergidis, "A systematic approach toward description and classification of cybercrime incidents," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 4, pp. 710-729, 2017.
[23] C. D. Marcum and G. E. Higgins, "Cybercrime," in Handbooks of Sociology and Social Research, 2nd edition, M. D. Krohn, N. Hendrix, G. P. Hall and A. J. Lizotte, Eds., Cham, Springer Nature Switzerland, 2019, pp. 459-475.
[24] S. Donaldson, J. Davidson and M. Aiken, "Safer technology, safer users: The UK as a world-leader in Safety Tech," Department for Digital, Culture, Media & Sport (DCMS), London, 2020.

Read the full report here

Phillips, K.; Davidson, J.C.; Farr, R.R.; Burkhardt, C.; Caneppele, S.; Aiken, M.P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sci. 2022, 2, 379-398. https://www.mdpi.com/2673-6756/2/2/28

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.