CC-DRIVER

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

Policy Brief No. 8

April 2023

Who is this for?

This policy brief contains key findings from the CC-DRIVER 2021 European Youth Survey and corresponding conclusions. This brief is designed for all professionals working within the area of cybercrime and key stakeholders, including LEAs, Academics, Criminal Justice, Policy Makers, and Educators.

Highlights

1. This is one of the largest studies to date exploring youth cybercriminality. The survey is informed by 5 key disciplines: cyberpsychology, criminology, psychology, neuroscience, and digital anthropology.
2. Results confirm that cybercrime and cyberdeviance (risk-taking and harmful behaviours online) is prevalent – survey finds that two thirds (69%) of European youth self-report to have committed at least one form of cybercrime or online harm or risk taking, and just under half 47.76% (N=3808) report to have engaged in criminal behaviour online, from summer of 2020 to the summer of 2021.
3. Survey finds that males are more likely (74%) than females (65%) to self-report having been involved in at least one form of cybercrime or online harm or risk taking in the last year and results confirm that the majority of cybercrime and cyberdeviant behaviours are gendered.
4. Survey analysis demonstrates that cybercriminal and online harm or risk-taking behaviours form a cluster of 11 behaviours that are highly interrelated (CcCd-Cluster) and that cybercrime and online harm or risk-taking behaviours represent a spectrum (CcCd-Spectrum).
5. A significant shift from a siloed, categorical approach is needed in terms of how cybercrimes are conceptualised, investigated, and legislated.

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

CC-DRIVER 2021 European Youth Survey

Purpose & context

This policy brief presents summary of results of a youth survey to explore and identify the drivers that may encourage and enable some young people to engage in cybercrime, cyberdeviancy and cyberdelinquency, with a view to informing new theoretical approaches across disciplines.

Research focusing on juvenile cyber delinquency is limited, especially when considering perpetration rather than victimisation. This is especially the case with empirical research rather than theoretical or conceptual works [1]. This is the largest study to date investigating youth cybercrime and cyberdeviance, with a multi-national sample across nine European countries.

Key Terminology and Definitions	
Cybercrime	The two most commonly cited academic definitions of cybercrime [2]: 1. "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" [3, p. 3]; and, 2. "any crime that is facilitated or committed using a computer, network, or hardware device" [4, p. 14]
Cyberdeviance	Refers to the violation of established norms and approved rules, encompassing serious behaviours, including crimes and delinquent acts (crimes conducted by juveniles), and behaviours that are not always punishable by law but that are either antisocial or harmful to the individual or others [5]
See 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies' Policy Brief and corresponding journal publication [6] for a more in-depth discussion of terminology and definitional issues.	

Methods

This survey was developed based on the expertise of UEL Professors Julia Davidson and Mary Aiken. We would like to acknowledge the contribution of Professors Michel Walrave and Koen Ponnet in terms of assisting in the design of Theory of Planned Behaviour (TPB) aspects of the survey. The survey was designed based on several scoping exercises to identify variables to be measured within the survey:

- Foundational work investigating youth pathways into cybercrime [7]
- Extensive literature review conducted under CC-Driver (task and deliverable 3.1, 2020)
- Targeted searches of relevant literature (2020-2021)
- Questions/items from previous large-scale studies in the area
- Psychometric measures from previous studies conducted within the fields of criminology, psychology and cyberpsychology
- Interviews with 36 juvenile cybercrime experts (CC-Driver, 2020).

Participants were recruited from U.K., France, Spain, Germany, Italy, Netherlands, Romania, and Scandinavia (comprised of 70% Sweden and 30% Norway) via a research agency (ResearchBods), using established participant panels, and a quota sampling approach. Sample was recruited evenly according to country (or region), gender and age. In total, responses from 7974 participants were included in this survey.

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

1. Prevalence & demographic factors of cybercrime behaviours

- Twenty key behaviours, shown in the table below, were selected to measure cybercriminal and cyberdeviant behaviours within this survey.
- This approach was informed by Phillips et al.'s [6] new classification framework (presented in this journal publication and policy brief no.7) and an in-depth literature review.

69.1% (N=5507) report to have committed at least one form (across the 20 key behaviours) of cybercrime or cyberdeviance (potentially risky or harmful behaviours) in the last year.

Cyberdeviant, Risky or Harmful		Cybercriminal	
Behaviour Label	**Prevalence**	**Behaviour Label**	**Prevalence**
Watch Pornography	1 in 2	Digital Piracy	1 in 3
Tracking	1 in 4	Used Illegal Virtual Marketplaces	1 in 5
Trolling	1 in 4	Money Muling (or laundering)	1 in 8
Sexting	1 in 5	Online Harassment	1 in 8
Shared Violent Materials	1 in 5	Hate Speech	1 in 10
Spam Messages	1 in 7	Hacking	1 in 10
Self-Generated Sexual Images	1 in 7	Cyberbullying	1 in 10
		Phishing	1 in 11
		Revenge Porn	1 in 11
		Cyberfraud	1 in 11
		Identify Theft	1 in 11
		Racist/Xenophobic Speech	1 in 11
		Sextortion	1 in 13

47.76% (N=3808) report to have engaged in a behaviour that could be considered criminal offense (in at least one jurisdiction) when online.

Differences Across Countries

- Whilst there is variability across all the behaviours, the perpetration rates across the countries surveyed from highest to lowest was: Spain (75.4%); Romania (72.9%); Netherlands (72.6%); Germany (71.8%); Norway (69.7%); Italy (68.6%); Sweden (67.3%); France (65.6%); and, United Kingdom (57.8%).

Differences in Gender

- Males are more likely to engage in the measured behaviours, with the only exception being online tracking ("Track what someone else was doing online without their knowing").

Differences in Age

- There is a small trend that cybercrime and cyberdeviance that increases across the ages sampled within this survey.
- This pattern is fairly consistent across all the forms of cybercrime and cyberdeviance measured.

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

2. Key findings: Spectrum & clustering of cybercrimes

- A unique and significant finding from this research was to investigate to what extent these 20 behaviours are associated with each other.

> *No other survey to date has explored such a broad range of behaviours and no other survey to date and of this size has explored both cybercriminal and cyberdeviant (risky and harmful) behaviours.*

- Results indicated that the occurrence and frequency of any one behaviour significantly predicts the occurrence and frequency of the other behaviours measured in this study.
- These findings show that cybercrime behaviours do in fact represent a spectrum (CcCd-Spectrum) and this has major implications for policy and practice.
- Further unique and significant finding is that cyberdeviance/cybercrime cluster (CcCd-Cluster) of 11 behaviours are very highly interrelated.

Sextortion	Cyberfraud	Phishing	Hate speech
Revenge porn	Identity theft	Cyberbullying	Hacking
Racism & xenophobia	Harassment	Money muling	

- These behaviours are very strongly correlated.
- Importantly, this cluster cuts across the entire spectrum as described in 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies' [6].
- This includes hacking, financial related cybercrimes, sexual violence online, online interpersonal violence, online hate, and incidental technology use.

Key Conclusions

- This research further confirms what is widely known, that young people are immersed in technology.
- It is of grave concern however, that approximately half of the sample reported 47.76% (N=3808) engaging in some form of cybercrime.
- When taking into account cyberdeviant behaviours, this number increases to just over two thirds (69.1%, N=5507).
- There is significant evidence that all forms of cybercriminal and cyberdeviant behaviours are significantly interconnected (CcCd-Spectrum).

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

Recommendations

Findings from the 2021 European Youth Survey have significant implications for policy and practice as they point towards a more general concept of deviancy, risk taking and harm, or a general propensity for anti-social behaviours online. Some of the key recommendations and conclusions for policy makers include:

1. Primarily, findings of this survey (CcCd-Spectrum) empirically support the spectrum approach to understanding cybercrime, as outlined in Phillips et al.'s (2022) definitions framework.
2. To support the development of framework of cybercrime, that can utilised across multiple jurisdictions (similar to the Budapest Convention's framework) that is inclusive of the full range of cybercrimes, as supported by behavioural data: "establishing a shared lexicon will be useful to all professionals working in the field, from policy makers discussing and proposing effective solutions to front-line workers seeking practical guidance on what does and what does not constitute a cybercrime" [6, p. 394].
3. Cybercrime and cyberdeviant behaviours are more generalised than is currently accounted for in how cybercrimes are conceptualised, measured, investigated, and legislated against; cybercrimes are conceptualised, legislated against, and investigated as independent silos, following a categorical approach.
4. A significant shift from the categorical silo approach is needed in how cybercrimes are conceptualised, investigated, and legislated for industry, practice, and regulation as online safety legislation is planned in many jurisdictions. As findings point towards a general propensity for anti-social behaviours online, requiring a more general concept of deviancy, risk taking and harm.
5. A unique and significant finding is the identified cluster (CcCd-Cluster) of 11 cybercriminal and cyberdeviant behaviours that are very highly interrelated. If it is known that they are significant overlaps between all forms of cybercrime, this could have implications for how cybercrimes are identified, investigated, and prosecuted.
6. Combatting cybercrime would benefit from further understanding of the cyberdeviance/cybercrime behaviour intersectionality.
7. Raising the public's, and particularly young people's awareness of the different types of cybercrimes and how they can avoid becoming victims and perpetrators would be an integral prevention strategy.
8. Tackling cybercrime and cyberdeviant behaviours would have to include initiatives to divert youths towards safe, non-criminal cyber activities.
9. Findings from this study have already been translated into evidence-based education and awareness, and intervention initiatives, disseminated broadly in Europe as part of Safer Internet Day 2023 and via Europol EC3.
10. CC-DRIVER intervention materials (for youth, parents, caregivers and guardians, and educators) can be readily adopted by key stakeholders (including LEAs, Academics, Criminal Justice, Policy Makers, and Educators) for community awareness raising and formal online safety education (see the next section for these materials).

Authors: *Professor Julia Davidson, Professor Mary Aiken, Kirsty Phillips, Ruby Farr, and Dr Ainul Hanafiah*

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

CC-DRIVER

2023 Safer Internet Day

It is important to educate young people and adults about knowing what types of online behaviours are risky, harmful, or criminal. CC-DRIVER translated the findings from 2021 European Youth Survey into educational materials that were shared for Safer Internet Day 2023 on Tuesday 7th February 2023: find see these resources here on the Safter Internet Day website and here on CC-DRIVER website. These have been shared Safer Internet Centres across all of Europe, in the hope of sharing these evidence-based interventions with young people and reducing online crime at national levels. The resources have also been shared here and endorsed by Europol's EC3 European Cybercrime Centre.

1. "What are cybercrimes?" Poster - This poster describes what cybercrimes are, gives examples of different types of criminal behaviours online, and gives examples of what individuals can do to reduce their risky online behaviours.

2. "Crossing the line into Cybercrime" Youth Quiz and Score Sheet (for ages 12+) - to educate young people about potential online risks and what measures can be taken to reduce and avoid behaviours that are risky, harmful, and associated with online crime.

3. "Pathways into Cybercrime" Resource for parents, caregivers, and educators - a checklist resource to help inform parents, caregivers, and educators about potential online risks that young people might be taking, the various factors that are associated with online risk-taking and what potential measures can be taken to reduce and avoid behaviours that are risky, harmful, and associated with online crime.

References

[1] Hutchings, A., & Holt, T. (2019). Interviewing cybercrime offenders. *Journal of Qualitative Criminal Justice and Criminology*, 1-35, DOI:10.17863/CAM.24191.

[2] Akdemir, N., Sungur, B., & Başaranel, B. U. (2020). Examining the Challenges of Policing Economic Cybercrime in the UK. *Güvenlik Bilimleri Dergisi (International Security Congress Special Issue), Özel Sayı*, 111-132.

[3] Thomas, D., & Loader, B. (2000). Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. In D. Thomas, & B. Loader (Eds.), *Cybercrime: Law enforcement, security and surveillance in the information age.* London: Routledge.

[4] Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13–20.

[5] Cioban, S., Lazăr, A. R., Bacter, C., & Hatos, A. (2021). Adolescent Deviance and Cyber-Deviance. A Systematic Literature Review. *Frontiers in psychology, 12*(748006), 1-27, DOI:10.3389/fpsyg.2021.748006.

[6] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences, 2*(2), 379-398, DOI:10.3390/forensicsci2020028.

[7] Aiken, M., Davidson, J. and Amann, P. (2016). Youth pathways into cybercrime.

Read the full report here:

- **2022 Research Report**: This report contains key findings from the CC-DRIVER 2021 Youth Survey and corresponding conclusions. Read the report here.
- Findings were also published U.K. in **The Guardian**, see this article here.
- UEL CC-DRIVER research team Professor Julia Davidson, Professor Mary Aiken, Kirsty Phillips & Ruby Farr.

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