CC-DRIVER

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

2022 Research Report

Authored by project co-leads Professor Julia Davidson OBE and Professor Mary Aiken, Project Manager Kirsty Phillips and Research Assistant Ruby Farr (CC-DRIVER partners at the University of East London, Institute for Connected Communities).

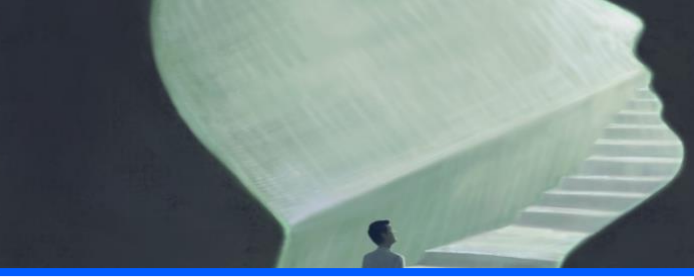
Who is this for?

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

Summary: CC-DRIVER 2021 European Youth Survey

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 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

About the Survey

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 (Hutchings & Holt, 2019). CC-DRIVER has one overarching issue to be solved, that is, understanding the technical and human drivers of cybercrime and how to use that knowledge to reduce cybercrime and to deter young people from engaging in high risk and cybercriminal activity. Adolescence has long been identified as a key transitional developmental period in which young people are more inclined to engage in risk taking, it is imperative to understand how the criminogenic medium of digital technology intersects with teens' natural propensity for risk taking.

Key Terminology and Definitions	
Cybercrime	The two most commonly cited academic definitions of cybercrime are (Akdemir, Sungur, & Başaranel, 2020): 1. "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (Thomas & Loader, 2000, p. 3); and, 2. "any crime that is facilitated or committed using a computer, network, or hardware device" (Gordon & Ford, 2006, 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 (Cioban, Lazăr, Bacter, & Hatos, 2021)
See 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies' Policy Brief and corresponding journal publication (Phillips, et al., 2022) for a more in-depth discussion of terminology and definitional issues.	

The aim of the CC-DRIVER 2021 European Youth Survey was 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. The study was conducted in accordance with the ethical standards of the British Psychological Association (BPS). This study was approved by The University of East London's Ethics Committee (application ID number: ETH2021-0065) as well as an independent CC-Driver Ethics Board. Data was collected in adherence with U.K. and EU (GDPR) data protection regulation. This is the largest study to date investigating youth cybercrime and cyberdeviance, with a multi-national sample across nine European countries.

Survey: Instrument Design

This survey has been developed based on the expertise of four Professors, each an expert in their respective fields: Professor Julia Davidson, Professor Mary Aiken, Professor Michel Walrave and Professor Koen Ponnet. To inform survey content a number of scoping exercises were conducted to identify variables to be measured within the survey: foundational work investigating youth pathways into cybercrime (Aiken, Davidson, & Amann, 2016); an extensive literature review conducted under CC-Driver (task and deliverable 3.1, 2020); targeted searches of relevant literature (2020-2021); scoping of questions/items to be measured within the survey from previous large-scale studies in the area; scoping of psychometric measures to be included in survey from previous studies conducted within the fields of criminology, psychology and cyberpsychology; and interviews with 36 juvenile cybercrime experts (CC-Driver, 2020).

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

These exercises identified an extensive list of variables, psychometric measures and concepts that are relevant to assessing juvenile cybercriminality, cyberdelinquency and cyberdeviancy. The following variables, among others, were the final items included within the survey:

- **Demographic variables** (country, area, age, gender, ethnicity, education, employment, socio-economic status, and number of other people in the household);
- **Tech device ownership and use** (variables include number/types of devices owned, frequency of device use, brands of devices, number of hours online, early use and ownership of devices, and where young people store their devices);
- **Social media use** (variables include use of social media platforms, frequency of platform use, use of multiple/fake accounts, reasons for use of multiple/fake accounts, use of private social accounts);
- **Prevalence of risky and harmful behaviours** (variables include engagement in cybercriminal and/or cyberdelinquent acts, and frequency of behaviours);
- **Tech Drivers** (variables include confidence in technical skills/abilities, tech competency, use of tech security measures and other online networks (outside of social media));
- **Offline risky or harmful behaviours** (variables include engagement in real-world deviant behaviour and frequency, and deviant friendship groups);
- **Cyber-related attitudes** (variables include propensity engaging to in cyber risky behaviours, attitudes towards cybersecurity and prosecution of cybercrime, and online disinhibition); and,
- **Individual difference factors** (variables include problematic and risky internet use, average hours of sleep and sleep interruptions, mental health diagnoses and/or conditions, depression, stress, anxiety, self-esteem, self-control, 'dark' personality traits).

Survey: Sample & Data Collection

Participants were recruited via a research agency (ResearchBods), using established participant panels, and a quota sampling approach was used. Sample was recruited evenly according to country (or region), gender and age. Firstly, the sample was recruited according to country or region with 1000 (12.5%) recruits in each of the eight regions, namely the U.K., France, Spain, Germany, Italy, Netherlands, Romania, and Scandinavia (comprised of 70% Sweden and 30% Norway). Within each region, the sample was recruited have an even split of the age range (25% 16,17,18, and 19-year-olds) and even split of gender (50% male and female, participants with other gender identities were also recruited). Aside from the demographic variables used to recruit the sample (county, age, and gender), additional demographic variables were measured within the survey, namely household income, residential location, education, occupation, and household makeup. The survey was live for a 3-month period beginning of June to end of August 2021. In this time period 37,341 in total were recruited; of this sample 10,155 (27.2%) withdrew or did not complete, 4387 (11.7%) were excluded for exceeding quota limits; 14830 (39.7%) were excluded due to low quality, inconsistent responses, or excessive speeding (completing the survey in less than 7.5 minutes). The remaining sample was therefore 7974 (21.4%) high quality responses. In terms of representativeness, the sample includes a range of different incomes, and is arguably representative of the wider population as only a minority identify as being in the upper income bracket relative to income ranges specific to each country/region. As is common with this age groups, just over a quarter of the sample indicated that they did not know their household income. Additionally, 8.4% chose not to disclose their household income.

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

Key Findings

1. Technology Use

The majority of participants report to spend a significant amount of time online, with only 11.6% reporting to spend 0-3 hours a day online. Approximately half spend 4-7 hours per day online, with 37.8% spending more than 8 hours (equivalent of a day's work) online each day.

With regards to technology use and ownership:

- 84% own a smartphone
- Approximately three quarters own their own laptop
- Approximately half own their own smart TV
- Only 1.5% report to not own digital devices

Young people are very immersed in technology and with their devices, in particular smartphones:

- 84% own their own smartphone and the majority of which are Apple smartphones
- 86.6% use their smartphone several times a day
- The majority keep their phone either in bed or in reach of their bed (82.4%)

2. Social Media Use

Participants were asked about their use of commonly used social media platforms, only 0.5% (N=36) of the sample report to not have used any social media. The most popular five platforms used were (in order): YouTube, Instagram, WhatsApp, TikTok, Snapchat. Next are Facebook and Twitter, use is estimated at approximately 50%.

In particular, Instagram proves to be a unique platform:

- Instagram is the second most popular platform with 93.6% of the sample being Instagram users.
- Instagram is the platform most frequently used platform with 64.7% using Instagram several times a day.
- Instagram is the **only** platform where users are more likely to have multiple accounts, over half of users (53.2%) have a second account, which equated to just under half the sample, 49.7% - no other platform comes close to this frequency of multiple accounts.
- Instagram is the **only** platform where the majority of users have made their primary account private (65.4% of the sample) – across all other platforms the majority of users do not make their primary account private

Two thirds of the sample, 67.2% (N=5359) and 67.5% of all social media users only, report to have multiple accounts on at least one platform. The most common reason being "to post content that I only want some of my friends to see", supporting the phenomenon termed 'finsta' or fake insta(gram), where young people have multiple accounts, most commonly on Instagram; one for public or more open use and one that is private, and the content is for a select group. This points to covert uses of social media and a small number (3% of the sample) report to have used social media for catfishing.

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

3. Technological Ability

Participants were asked to rate their own technical abilities from "I know the basics only" to "I think I am an expert". Participants most commonly (N=3153, 39.5%) thought that they were average ("I think my tech skills are average"), 38.1% greater than average (combining 'Above Average', 'Advanced' and 'Expert') and 22.4% less than average (combining 'Below Average' and 'Basic'). Therefore, whilst immersed in technology, young people may not be as knowledgeable as previously perceived. In addition to the above self-assessment participants were asked about their use of security and privacy enhancing technologies (PET), technologies designed to support data protection and privacy. **Notably, approximately one in eight (N=1017, 12.8%) have not used any form of privacy enhancing technology (PET).**

Use of security and/or privacy enhancing technologies (PET):

- Most common (approx., 50%) - antivirus software (53.5%), deleting cookies or browsing history (51.3%) and use of "incognito" or "private" mode when using a web browser (49.5%)
- Least common (less than 10%) - virtual machine (9.7%), use of TOR (9.1%), cryptocurrency (7.3%) and a security-oriented operating system (e.g., Whonix or Tails) (5.4%)
- Approx. one in eight have not used any form of security or privacy enhancing technology (PET)

4. Risky Online Spaces

Participants also report to engaging in risky online spaces, in order: 51.3% report to use Online Forums and Chat Rooms; 51.2% report to use Online Gaming Forums; 19.0% report to use Peer-to-peer (P2P) networks (e.g., BitTorrent); 11.8% report to use Dark Web Forums; and, importantly, **10.7% report to use Darknet Markets.** Approximately 1 in 10 are using online forums and chat rooms and/or online gaming forums at least once a day. Only a very small minority (less than 2%) are using Dark Web Forums or Darknet Markets at least once a day.

5. Offline deviancy and with friends

Offline delinquency is a very strong predictor of online delinquency (Brewer, Cale, Goldsmith, & Holt, 2018). The "Deviant behaviour variety scale' (DBVS) was adopted within this study (Sanches, Gouveia-Pereira, Marôco, Gomes, & Roncon, 2016) to measure offline delinquency. This scale has been validated and designed for use with adolescents (see Sanches et al. (2016)). Within this study, this scale was also found to be highly reliable (α=0.95). Prevalence rates ranged from 11.7% ("Used a motorbike or a car to go for a ride without the owner's permission") to 64.5% ("Lied to adults"). Participants were asked to rate their agreement on scale from 0-3 (0= Never to 3= Always) on 5 items assessing various delinquent peer behaviours; engagement in drinking or drugs, vandalism, shoplifting, computer delinquency, or general antisocial behaviour (attempts to annoy or frighten others). Prevalence rates for these behaviours were: 10.3% ("Shoplift just for fun"), 12.8% ("Smash or vandalize things just for fun"); 21.1% ("Frighten or annoy people around you just for fun"); 24.4% ("Use online gaming hacks"); and 32.7% (Drink a lot of beer/alcohol or take drugs"). This demonstrates that some forms of online anti-social behaviours are conducted at a similar level as offline anti-social behaviours with friend groups, and use of online gaming hacks/cheats is a well-established pathway into criminal hacking.

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

6. Cybercrime and Cyberdeviancy

20 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 (2022) new classification framework (presented in this journal publication and policy brief no.7) and an in-depth literature review; behaviours were selected that were more likely to be found in youth populations based the findings of previous academic research. Participants were asked "Over the last year, using an Internet-connected device, did you at any point..." asked to rate their agreement on a 5-point Likert scale from 0= "Never" to 4= "Very Often". As this study was conducted in the summer of 2021, the 'last year' referred to mid 2020-2021. A follow-up question asked participants "Do you think any of these behaviours increased due to COVID-19 restrictions/lockdowns?" and approximately half, 46.8% (N=3730), believed that these behaviours did increase during COVID-19 lockdowns.

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

Whilst it is still very much debated in academic literature to what extent and in what nature, there are potential risks associated with youth exposure to pornography, see here for an overview of the debates and relevant findings. It has a proven association with sexual violence, and as shown is this report is significantly associated with all other behaviours measured in this study (e.g. sextortion, sexting, revenge porn). However, figures remain high even when removing this common behaviour measured, namely watching pornographic material, at 63.7% (N=5077).

Prevalence rates range from 7.8% (least common) to 44.1% (most common). Prevalence rates correspond to significant minorities, approximately:

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

6.1. Differences in Gender

Gender differences were considered in relation to the 20 behaviours observed. Of the males that participated in the survey 73.6% report to have engaged in some form of cybercrime or cyberdeviancy from mid 2020-2021 compared to 64.6% of females. Whilst this doesn't indicate a large gender

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

difference overall, when looking at proportional differences across individual acts for almost all behaviours those who engage in the behaviour are more likely to me male. There is only one exception, for online tracking *("Track what someone else was doing online without their knowing"*), where those who engage with the behaviour are slightly more likely to be female. The gender difference is largest for racist and xenophobic abuse online and hate speech, but for most behaviours is approximately two thirds male and one third female (in order of highest gender difference: Illegal trade of virtual items; Revenge Porn; Harassment; Sextortion; Phishing; Encourage violence; Cyberbullying; Cyberfraud; Identity Theft; Hacking; and Spam). However, there is approximately gender parity for self-generated sexual images, digital piracy, and tracking.

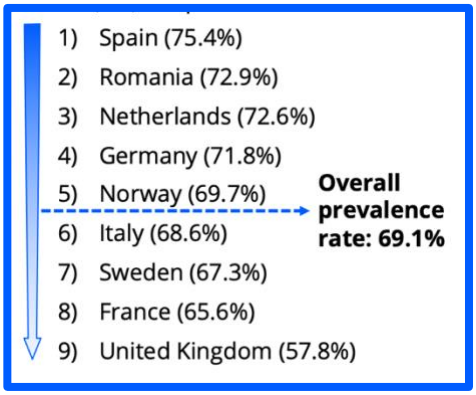
6.2. Differences in Age

Age differences were considered in relation to the 20 behaviours observed. Overall, there is a small trend that cybercrime and cyberdeviance increases across the ages sampled within this survey. Furthermore, this pattern is fairly consistent across all the forms of cybercrime and cyberdeviance measured.

6.3. Differences Across Countries

Whilst there is variability across all the behaviours, when looking at all 20 behaviours measured 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%).

Figure. Prevalence by Country



6.4. Cybercrime as a cluster of behaviours

A unique and significant finding from this research was to investigate to what extent these 20 behaviours are associated with each other (*20 key behaviours: "Watch Pornography"; "Digital Piracy"; "Tracking"; "Trolling"; "Encourage violence"; "Sexting"; "Illegal trade of virtual items"; "Spam"; "Self-generated sexual images"; "Money Muling"; "Harassment"; "Hate Speech"; "Hacking"; "Cyberbullying"; "Phishing"; "Racism or Xenophobia"; "Revenge Porn"; "Cyberfraud"; "Identity Theft" and "Sextortion"*). 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. Correlation analysis shows that all 20 key behaviours highly correlated and statistically significant ($p<0.001$). Furthermore, all behaviours are positively correlated meaning 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 from correlation analysis identified a cyberdeviance/cybercrime cluster (CcCd-Cluster) of 11 behaviours that are very highly interrelated (*11 behaviours: "Sextortion"; "Revenge Porn"; "Identity Theft"; "Cyberfraud"; "Cyberbullying"; "Racism and Xenophobia"; "Phishing"; "Hate Speech"; "Harassment"; "Hacking"; and "Money Muling"*). All associations have a large correlation coefficient ($r>.50$) and according to Cohen's (1988) interpretation of correlation coefficients, 0.5 indicates a large effect size, which shows that these behaviours are very

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

strongly correlated. Importantly, **this cluster cuts across the entire spectrum** as described in 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies' (Phillips, et al., 2022) and includes hacking, financial related cybercrimes, sexual violence online, online interpersonal violence, online hate, and incidental technology use. Findings 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 rather than treating cybercrimes as categorical, as cybercrimes are currently conceptualised, legislated against and investigated as independent silos.

Key Conclusions

Adolescents are the most digitally connected generation in history (Odgers & Jensen, 2022). This research demonstrates 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, and when taking into account cyberdeviant behaviours this number increases to just over two thirds (69.1%, N=5507). Whilst prevalence rates for individual behaviours range from approximately 1 in 2 to 1 in 13, there is significant evidence that all forms of cybercriminal and cyberdeviant behaviours are significantly interconnected (CcCd-Spectrum). This finding necessitates a shift from the categorical approach to a spectrum-based approach, as there is evidence that any individual behaviour is significantly associated with all other behaviours as well as any other individual behaviour. In particular there is a cluster (CcCd-Cluster) of cybercrime behaviours (*"Sextortion"; "Revenge Porn"; "Identity Theft"; "Cyberfraud"; "Cyberbullying"; "Racism and Xenophobia"; "Phishing"; "Hate Speech"; "Harassment"; "Hacking"; and "Money Muling"*) which are very strongly associated.

Based on the spectrum and cluster findings, a significant shift from the categorical silo approach is needed in how cybercrimes are conceptualised, investigated, and legislated. These findings therefore have significant implications for industry, practice, and regulation as online safety legislation is planned in many jurisdictions. This work has significant implications for policy and practice particularly in the context of prevention and intervention. Findings will inform our evidence-based education and awareness, and intervention initiatives; CC-DRIVER intervention materials (for youth, parents, caregivers and guardians, and educators) will be disseminated broadly in Europe as part of Safer Internet Day 2023 and via Europol EC3.

References

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.

Brewer, R. C., Cale, J., Goldsmith, A. J., & Holt, T. (2018). Young people, the Internet, and emerging pathways into criminality: A study of Australian adolescents. *International Journal of Cyber Criminology, 12*(1), 115-132, DOI:10.5281/zenodo.1467853.

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.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (Vol. Second Edition). Hillsdale, NJ: Lawrence Erlbaum Associates.

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

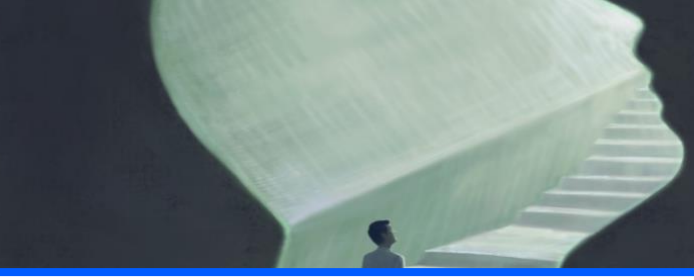
Hutchings, A., & Holt, T. (2019). Interviewing cybercrime offenders. *Journal of Qualitative Criminal Justice and Criminology*, 1-35, DOI:10.17863/CAM.24191.

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.

Sanches, C., Gouveia-Pereira, M., Marôco, J., Gomes, H., & Roncon, F. (2016). Deviant behavior variety scale: development and validation with a sample of Portuguese adolescents. *Psicologia: Reflexão e Crítica, 29*(1), 31-38, DOI:10.1186/s41155-016-0035-7.

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.

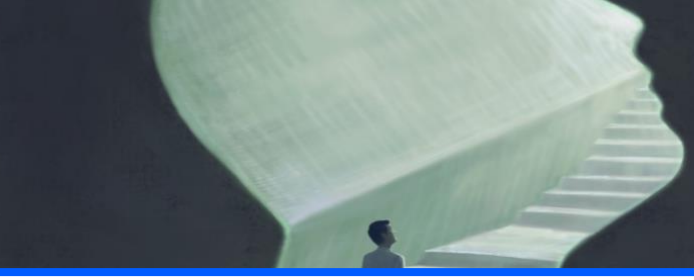
This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.



Appendix A: Behaviours and item descriptions

Behaviour Label	Item Description
"Watch Pornography"	Look at images or videos that were pornographic (sexual in nature)
"Digital Piracy"	Copy, upload or stream music, movies or TV that hasn't been paid for
"Tracking"	Track what someone else was doing online without their knowing
"Trolling"	Start an argument with a stranger online for no reason
"Shared Violent Materials"	Share stories, images, memes or videos that were violent or harmful in nature
"Sexting"	Send messages containing sexually explicit content or materials
"Used Illegal Virtual Marketplaces"	Buy or trade lootbox items from a virtual marketplace
"Spam Messages"	Send out 'spam' or junk messages
"Self-Generated Sexual Images"	Make and share images or videos of yourself that were pornographic (sexual in nature)
"Money Muling" (or laundering)	Allow someone else to use your bank account to transfer money
"Online Harassment"	Threaten, embarrass or hurt others online
"Hate Speech"	Say or write something online to hurt someone because of their religion, age, ethnicity, gender, sexual orientation, or disability
"Hacking"	Try to / or successfully gain access to another individual's / organization's computer system without their permission
"Cyberbullying"	Repeatedly target, threaten, embarrass or hurt a person online
"Phishing"	Use email messages (links or attachments) to get someone to download a virus onto their devices
"Racist/Xenophobic Speech"	Insult or threaten someone because of their religion, ethnicity or because of where they come from
"Revenge Porn"	Share images or videos of someone else that were sexual in nature, without their permission or knowledge
"Cyberfraud"	Try to scam someone into giving you money or finances of any description
"Identity Theft"	Try to get someone to give you their personal information or payment details
"Sextortion"	Threaten to share images or videos of someone else that were sexual in nature, to get them to do something you wanted

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



CC-DRIVER

Appendix B: Other metrics included in survey

The range of variables (included psychometric scales) studies within this survey allows for multiple avenues of exploration to investigate predictors (of spectrum and cluster behaviours). All psychometric measured used were found to be reliable (α <.7) and means and standard deviations for scales and subscales were approximately in line with previous research, indicating that these measures are also valid measures of target constructs. All of these constructs have been investigated by previous research and shown to have a significant effect on one or more forms of cybercrime, furthermore theses constructs are identified by academic theory across 5 key domains (primarily criminology, psychology, cyberpsychology, but also neuroscience and digital anthropology). These scales, sources, number of subscales, reliability and whether or not they can be used in further statistical tests are shown in the below table.

Concept	Name of Scale	Subscales	Reliability α	Can be tested?
Tech Ability	'Technical Competency Scale' – Brewer, et al. (2018)	N/A	0.92	☑
Risky Internet Use	Problematic and Risky Internet Use Scale (PRIUSS-18), including Emotional Impairment, Social Impairment and Risky/Impulsive Use subscales - (Jelenchick, et al., 2014)	3	0.94	☑
Risky Cybersecurity	Adapted Risky Cybersecurity Behaviours Scale' (RScB) - Hadlington (2017)	N/A	0.79	☑
Guardianship Attitudes	Adapted 'Attitudes Towards Cybersecurity and Cybercrime in Business' (ATC-IB) scale - Hadlington (2017)	N/A	0.81	☑
Online Disinhibition	'Online Disinhibition Scale' (ODS), including Toxic and Benign Disinhibition – Udris (2014)	2	0.86	☑
Low self-control	Low self-control scale including Impulsivity, Risk Seeking, Self-Centredness and Temper subscales - (Grasmick et al, 1993)	4	0.89	☑
Offline Delinquency	Deviant behaviour variety scale (DBVS) including Minor and Serious Infractions - Sanches, et al., 2016)	2	0.95	☑
Deviant Peer Association	Scale adapted study – Holt, et al. (2020)	N/A	0.78	☑
Dark Personality Traits	SD4 including Machiavellianism, Psychopathy, Narcissism and Sadism subscales	4	0.97	☑
Negative emotion	Depression, Anxiety and Stress Scale (DASS-21), including Depression, Anxiety and Stress subscales- (Lovibond & Lovibond, 1995)	3	0.97	☑

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