CC-DRIVER

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

Policy Brief No. 11

April 2023

Who is this for?

This policy brief contains key recommendations from the CC-DRIVER Strategy for addressing the socio-economic aspects of cybercriminality. This brief is designed for all professionals working within the area of cybercrime and key stakeholders, including LEAs, Academics, Criminal Justice, and Policy Makers.

Highlights

The CC-DRIVER Strategy for addressing the socio-economic aspects of cybercriminality recommends the expansion of ENISA's remit by the EC to conduct an annual socio-economic impact assessment of cybercrime in the EU, in relation to 5 key areas:

1. **Definitions** – how we should define the terms 'cybercriminality' and 'socio-economic issues raised by cybercriminality' for the purposes of this report.
2. **Measures** – of cybercriminality and its socio-economic impacts and which would be useful to develop and track
3. **Method** – how best to measure and quantify the cost and socio-economic impacts of cybercriminality and which relevant bodies should so tasked.
4. **Awareness** – methods that EU authorities can use to educate and raise awareness of cybercriminality and its socio-economic impacts, and advice for citizens and relevant stakeholders on how best to minimise their exposure to cybercrime risks.
5. **Strategy** – recommendations and next steps arising from the analysis above to inform a solutions-based approach.

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

CC-DRIVER

1. **Definitions:** Definitions of 'cybercrime' and 'socio-economic'

To address the socio-economic aspects of cybercriminality, the terms 'socio-economic' and 'cybercriminality' need to be carefully considered.

A key barrier to estimating impact is the lack of well-formed definitions and classification systems capable of accounting for the full range of cybercrimes [1]; "imprecision about concepts in social science contexts can often have negative (and very real) socio-economic consequences for at-risk groups in society" [2, p. 5]. Defining crime-related phenomena hinges on two factors: "the behaviour as behaviour, and … the definitions by which specific behaviour comes to be considered crime or non-crime" [3, p. vi]. Inconsistencies in cybercrime definitions hamper not only the measurement and understanding of cybercrime across jurisdictions and across disciplines but the legal responses to cybercrime as well as global initiatives and cooperative efforts to tackle cybercrime. For the purposes of the CC-DRIVER research project, the term 'cybercrime' refers to broad spectrum of behaviours encompassing all online behaviours that result in harm; including online harms, cyberdeviance, cyber delinquency and crimes (both cyber-dependent and cyber-enabled) conducted in cyberspace or through the use of digital technology. This is represented within the new framework presented in CC-DRIVER Policy Brief No.7 and corresponding published journal article [4]. See the journal article for an in-depth discussion of cybercrime definitions as well as a discussion of key challenges and future recommendations on this topic.

To address the socio-economic aspects of cybercriminality, all aspects of cybercriminality have been considered as well as the costs to society of combating and limiting cybercriminality, including, but not limited to: attacks against systems; theft against property; violence against groups and individuals, including interpersonal violence, sexual violence, online hate, online terrorism; and illegal consequences of incidental technology use.

Much more research is needed to assess the costs and impacts of cybercrime in the EU. Socio-economic costs have also been described as direct and indirect economic burdens on society. A proper socio-economic impact assessment needs to consider the impacts that are difficult to measure (let's say, the indirect costs) as well as those that are more easily measured (let's say the direct costs).

Key recommendations

The EC should ask CEN to standardise cybercrime definitions. Researchers and policymakers would benefit from agreement on socio-economic impact assessments (costs and impacts) of cybercrime and what methodologies are appropriate to these factors and to whom those costs and impacts should be reported. EC annual reports should include, at at least, the above subsets of cybercrime and their socio-economic impacts. Such reporting of the costs and impacts of cybercrime in the EU will help policymakers give an appropriate priority to measures to address these challenges.

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

2. **Measures:** Measuring cybercrime and its socio-economic effects

Having defined what is meant by the socio-economic aspects of cybercriminality, an attempt must be made to consider and measure both its costs and impacts.

Measuring cybercriminality and socio-economic impact of cybercriminality at regular intervals, on at least an annual basis, would offer an opportunity to improve the following three areas:

1) The tracking of changing patterns of cybercriminality;
2) The responsiveness of official policies to prevent and limit cybercriminality; and
3) Public awareness of the evolving threat of cybercriminality.

When attempting to measure the extent and impact of cybercrime, several serious challenges are apparent, primarily surrounding definitional issues and key data gaps (termed in criminology the 'Dark Figure of Crime', referring to the crimes that are unreported or unknown). Key data gaps result from lack of awareness of cybercrimes, lack of awareness in reporting mechanisms and the fact that national statistics and crime data only represent a subset of all crimes committed.

Key issues resulting from these fundamental knowledge gaps include:

- varying definitions and measures of cybercrime by law enforcement agencies;
- incomplete measures of cybercriminality; incomplete reporting of cybercrime by victims;
- incomplete reporting of cybercrime and irritations that fall short of crime due to their trivial impact; and,
- incomplete reporting as victims may not be aware that they have been an object of crime.

Key recommendations

There is a need to develop measures of the extent and socio-economic impact of cybercrime that incorporate the following features:

- Agreed definitions: considered definitions of cybercriminality and of its component elements that can be agreed and used by policymakers across the European Union. The CC-DRIVER project has published recommendations for steps towards a cohesive and comprehensive understanding of cybercrime definitions: see Phillips, et al. (2022) [4] and CC-DRIVER Policy Brief No.7
- Measurement incidence: methods of estimating the socio-economic impacts of cybercriminality that overcome incomplete measures used at national level.
- Measurement victimology: methods of estimating the socio-economic impacts of cybercriminality that overcome incomplete reporting by victims, whether out of potential embarrassment, the trivial level of loss suffered or simple lack of knowledge that they have been victims of crime or not knowing to whom to report their being victimised.

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

3. **Method:** Classifying the extent of cybercriminality

The CC-DRIVER project recommends adopting the WHO's public health approach (WHO's Violence Protection Alliance (VPA) approach to combating violence) for the research and measurement of cybercrime. After developing a definition and typology, which has been provided by CC-DRIVER (see above), the next stage is to: "Define the problem through the systematic collection of information about the magnitude, scope, characteristics and consequences of violence".

There are three broad dimensions to any incident of cybercrime: the nature of the crime; the specific cybercrime technique used; and the extent of damage suffered by the target or victim. Therefore, the subsets of cybercrime identified in Phillips, et al. (2022) [4] and CC-DRIVER Policy Brief No.7 can be considered and expanded in a definitional context to provide a more comprehensive spectrum of cybercrime that can be used for classification purposes with a corresponding consensus among researchers and policymakers about what and how to measure the costs and impacts of cybercrime. Direct socio-economic costs may include for example losses due to hacks, online theft or fraud, or illegal profits of cybercrime laundered into the legitimate economy. Indirect socio-economic costs may include for example: compromises to national security, threats to democracy, reputational damage, psychological impact on cybercrime victims, and costs associated with inequalities.

The CC-DRIVER project has published a landmark study exploring the (D2.2) "Drivers, Trends, and Technology Evolution in Cybercrime". The report identifies and analyses both human and technical drivers of cyber-dependent cybercrimes as well as the techniques and tactics of these cybercriminals and cybercrime-as-a-service. A similar project is needed to systematically review the techniques and tactics of cyber-enabled crimes. There are many different ways in which the extent of damage done by cybercriminality could be classified. See the CC-DRIVER study on the socio-economic impacts of cybercrime, which references different SEIA models and a recommended model. The challenge is to design a system that is simple yet comprehensive, inclusive of a range of harms from catastrophic harms to no financial or physical harm/damage.

Key recommendations

Conduct research [Primary responsibility ENISA, in cooperation with other bodies with public accountability and transparency such as Eurobarometer] using these methods to assess the extent of cybercrime and its socio-economic impacts, including but not limited to: surveys; examination of published data; data from bodies that track cybercrime as part of their regular activities (e.g., Europol and ENISA); and selected academic research. Ensuring the reliability, validity, and credibility of cybercrime research, and appropriate stratification across various demographic factors (such as socio-economic status, education, age, gender).

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

4. **Awareness:** Developing awareness of cybercriminality and of its socio-economic impacts

The 'Engagement' section of the CC-DRIVER wiki[1] provides key recommendations in relation to cybercrime and online harms leadership; formal education (school age); informal education, tertiary education, and professional education; public awareness; engaging stakeholders; and international and regional engagement to develop real-world solutions to combat cybercrime and increase online safety. These areas can also incorporate the measures below to combat the socio-economic impacts of cybercrime.

Developing awareness of cybercrime and its socio-economic impacts among the public is important to alert citizens to the risks they face and the countermeasures they can take to minimise the overall costs of cybercrime to society; and policymakers so that national and international policy adapts to a fast-changing cyber environment and to optimise policy to limit and prevent cybercrime.

There are several ways in which awareness can be developed and enhanced. These range from the formal and technical to the informal and popular, including to:

- task organisations such as national crime agencies to identify and promote stories in conventional and social media that boost awareness of cybercrime and of steps that can be taken to minimise its impacts.
- hold expert conferences, on at least an annual basis, that will bring together IT practitioners, academic experts and policymakers to review developments in the cybercrime field and communicate matters of mutual concern.
- publish regular periodic reports that assess developments in the cybercrime area.
- hold regular opinion polling (e.g., Eurobarometer) on cybercriminality will permit the attainment of several objectives. The Eurobarometer poll offers a template, in the co-development of a strategy for addressing the socio-economic aspects of cybercriminality that could be profitably followed in the future.
- although potentially expensive, advertising could be used to boost awareness of cybercriminality (including advertising via TV, radio and social media and use of novels).
- the availability of TV sponsorship funding could make the difference to whether a new TV series focussing on cybercriminality (on Netflix, Sky or Amazon Prime etc) gets made or not.

Key recommendations

Develop awareness of cybercriminality and of its socio-economic impacts [Primary responsibility ENISA, in cooperation with other bodies], adopting the above strategies.

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

5. Strategy for addressing the socio-economic aspects of cybercriminality

The following elements should form part of a coherent EC strategy (using the key recommendations captured in this document) to minimise the socio-economic impact of cybercriminality:

- Recommit to over-arching objective – to minimise the socio-economic impacts of cybercriminality.
- Expand ENISA's remit to research and report on the annual costs and impacts of cybercrime in the EU.
- Report to the European Parliament annually on the socio-economic impacts of cybercrime in the EU and beyond
- Mobilise institutional allies – to better advance this objective.

Allies are going to be found in several categories of organisation:

Category	EU-level	National level
Government	European Commission	National government
Police force	Europol (EC3)	National police forces
Statistics agency	Eurostat	National statistics agencies
Polling organisation	Eurobarometer	National government polling organisations

The EU is best placed to direct a coherent, public response to the socio-economic threat posed by cybercriminality. This will require the leadership of ENISA and the mobilisation of institutional allies at EU and Member State level across government, police forces, statistical and polling agencies.

The EC should ask CEN to standardise cybercrime definitions. The EC should expand ENISA's remit to conduct an annual socio-economic impact assessment of cybercrime in the EU. ENISA should, in cooperation with other bodies, conduct research into cybercrime and its socio-economic dimensions. This can take the form of conducting opinion poll surveys of people building on the work already done by Eurobarometer, examining published data and summarising selected academic research and assembling data from bodies such as Europol that track cybercriminality as part of their regular responsibilities.

ENISA should then, in cooperation with other bodies, develop awareness of cybercriminality and of its socio-economic impacts by holding expert conferences, publishing annual surveys (covering recent research, statistics and opinion poll data), formulate and deliver education and awareness raising campaigns aimed at the public, designed to address identified awareness gaps among particular socio-economic groups regarding the prevalence, dangers and impact of cybercrime.

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. Barn and B. Barn, "An ontological representation of a taxonomy for cybercrime," Istanbul, Turkey, 2016.

[2] 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.

[3] G. Vold, *Theoretical Criminology*, New York: Oxford University Press, 1958.

[4] K. Phillips, J. C. Davidson, R. R. Farr, C. Burkhardt, S. Caneppele and M. P. Aiken, "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies," *Forensic Sciences*, vol. 2, no. 2, pp. 379-398, DOI:10.3390/forensicsci2020028, 2022.

Further Information:

ABOUT THE CC-DRIVER PROEJCT

- CC-DRIVER RESOURCE: "Ethical, data protection and socio-economic impact assessment"
- CC-DRIVER RESOURCE: "CC-DRIVER Wiki Pages"
- CC-DRIVER RESOURCE: "CC-DRIVER Policy Briefs"
- CC-DRIVER EDUCATION RESOURCES: "Crossing the Line into Cybercrime: Useful Information for Young People, Parents, Caregivers, and Educators"
- CC-DRIVER PUBLICATION: "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies"
- CC-DRIVER PUBLICATION: "2021 European Youth Survey"
- CC-DRIVER DELIVERABLE: "Nature of and perspectives on cybercrime and crime as a service"
- CC-DRIVER DELIVERABLE: "Landscape Study of Cybercrime-as-a-Service"
- CC-DRIVER DELIVERABLE: "Review and gap analysis of cybersecurity legislation and cybercriminality policies in eight countries"
- CC-DRIVER DELIVERABLE: "LEA Working Group on human and societal aspects of cybersecurity"

Read the full report ("CC-DRIVER Strategy for addressing the socio-economic aspects of cybercriminality"), authored by CC-DRIVER partners at the University of East London, Institute for Connected Communities: Professor Julia Davidson, Professor Mary Aiken, Project Manager Kirsty Phillips, external contributor Economist Cormac Lucey and David Wright (TRILATERAL RESEARCH, CC-DRIVER). Thank you to the team at Trilateral Research (CC-DRIVER) for organising the workshops to inform the development of this task.

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