CC-DRIVER

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

Policy Brief No. 4

May 2022

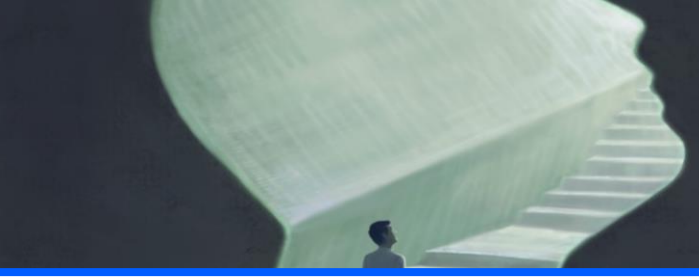
Who is this for?

This policy brief raises the various issues and barriers to the measurement and study of cybercrime from both a practical and methodological point of view. It is addressed to the CC-DRIVER Stakeholder Board, law enforcement agencies (LEAs) and academic organisations.

Highlights

1. While there is common agreement on the definition of specific cybercrime behaviours, a common cybercrime taxonomy has not been established, but many classifications of cybercrime exist for different purposes. Moreover, the hybridisation of many crimes rises question on the measurement of cybercrime through official statistics.
2. Despite the different data sources, it is still difficult to figure out a trend to study cybercrime due to the lack of data and disparities in the measurement of cybercrime among the statistics.
3. At this stage, official statistics should define a core set of cybercrimes that could be measured through different sources (police statistics and crime surveys) in order to establish a standard data collection methodology over time.
4. In particular, crime surveys should include questions regarding cybercrime victimisation, addressing both individuals and companies.
5. The exercise of measurement through surveys should be developed through a methodology replicable and applicable in different European countries, to allow for a cross-checking validation of results.

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



Challenges in measurement of cybercrime

Cybercrime is expanding exponentially; new online behaviours are evolving leading to several challenges on the measurement of cybercrime. However, despite the high number of cybercrimes, it is difficult to provide an overview of the current trend. Cybercrime is measured by different sources including official data such as police statistics and victimisation surveys, but also less typical sources from private company reports. All three sources of data fail to give accurate information regarding cybercrime trends, suffering from both validity and reliability measurement problems.

Factors impacting the measurement of cybercrime

The measurement of cybercrime is affected by various factors, which partly explains the current shortage of data. These factors are the following:

- Lack of common definition of cybercrime and of comprehensive classification on cybercrime behaviours
- Lack of a legal and harmonised framework surrounding cybercrime
- Lack of awareness of having been a victim of cybercrime
- Lack of agreement on the units of measurement of cybercrimes

Since cybercrime is a relatively vast and fast-moving phenomenon, it raises questions about its definition and the classification of the wide range of acts which are part of it, and are not always mapped. Indeed, different taxonomies are established on a different basis to classify the same cybercriminal act, although globally there is a consensus on the existing behaviours and their definition. The first steps towards this consensus and taxonomies emerged from the Budapest Convention of Cybercrime in 2001, providing guidelines to create legal provisions for certain behaviours. Thus, these differences in classification raise questions about the measurement of cybercrime. For this reason, studies on cybercrime show results that can be varied, for example in terms of the prevalence of a phenomenon as well as the characteristics of the victims, indicating that measures of some phenomena are not the same between different studies.

This lack of a standard classification of cybercrime, and particularly acts called hybrid combining acts committed online and offline, generates problems for the legal framework surrounding online crime. Numerous provisions struggle to qualify cyber-enabled crimes as well as hybrid acts as part of cybercrimes, thus associating the acts committed with offline legal provisions, impacting on the data collection of official statistics. Thus, there are disparities within different countries which adopt different provisions to sanction cybercrime, while it is a transnational phenomenon, making it difficult to compare the numbers among different countries.

In addition, the above-mentioned lack of definitional and legislative clarity has an impact on complaints to the police as well as on victimisation surveys as people are not always aware that certain acts are considered illegal or they are not aware of their right to complain, or sometimes not even aware of having been a victim.

Moreover, there is also some difficulty in comparing data. As a cybercrime act may involve multiple targets, cross-checking official statistics can be difficult. A single act measured by police statistics may be reported by a multitude of victims in victimisation surveys, resulting in discordant measures of the trend and using a different unit measure. This could be seen in the case of phishing attacks, for example, where one email may be sent to dozens or hundreds of people.

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

Limitations of data sources

The measures primarily mobilised, by policy makers, are official data including police statistics and victimisation surveys; data from private companies are now also being sought. These data sources provide different information and suffer from different limitations regarding the measurement of cybercrime trends linked with the issues presented above. These are presented below.

- Police statistics: constrained by the limits of legislation and underreporting number of crimes
- Victimisation survey: restricted questions measuring cybercrime, underreporting and count of victimisation number
- Private companies: specific data collected dependent of the product/services of the company

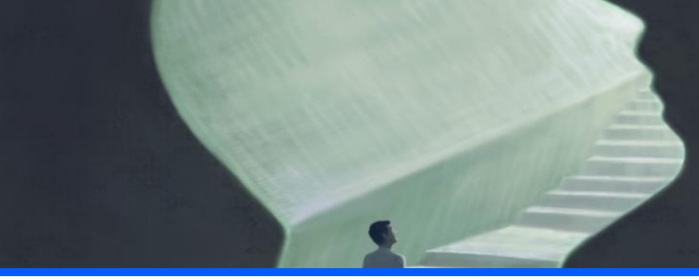
Police statistics are the main data used regarding crime, various data sources in addition to national sources collect this data, such as the Europol Internet Organised Crime Threat Assessment (IOCTA) report. However, in the cybercrime field, data recording is limited first due to the lack of provisions sanctioning cybercrime, to the challenge qualifying hybrid crimes and also due to the anonymity of the darknet platform. These might be sanctioned and recorded under a regular law, if an investigation is carried out, these data regarding the crime are usually more complete than other sources. If no provision exists regarding online offences, the recording procedure might shorten the number of crimes recorded using online devices. Besides, the underreporting of cybercrimes is also a factor biasing the figures. Indeed, cybercrime victims might not be aware they have been victims; and if they are, some might also not know what behaviours are considered as offences and their right to report them, as legislations regarding cybercrime are permanently changing. In addition, companies also avoid reporting the crime to authorities with fear that it would damage their reputation.

In order to reduce the dark figure, national victim surveys are effective tools to compensate information missing, especially for underreported crimes. One of them is the Internet Crime Complaint Center (IC3) implemented by the FBI, providing complaint information yearly. The national victimisation surveys also have the advantage of measuring behaviours without being restricted to legal provisions. However, the information collected by national victimisation surveys regarding cybercrime is limited, as they contain only few questions measuring cybercrime victimisation; and the questions are directed to individuals only, while companies are main targets of cybercrimes too. It should be pointed out that the information collected does not give accurate indications on the trend as some acts target more than one person or one person but multiple devices. Thereby the report would give more information on the victim and the reason why the crime was not reported than on the act itself. Finally, the answers to the victimisation survey are limited due to the lack of knowledge of being a victim, as already mentioned above.

Data sources from private companies are also included for the study of cybercrime as they are also particularly targeted. These data provide information about the cybercrimes that the company has experienced, thus reducing the black figure for a specific population and giving access to more detailed information about the trend. However, the data from these reports is limited to the company in question, collecting information on cyberattacks aimed at the specific products the company offers. Thus, one would expect data on cyber dependent crimes and in a very specific setting. In addition, companies also avoid reporting the crime to authorities with fear that it would damage their reputation.

The different data sources presented, and their limitations, illustrate the difficulty of measuring cybercrime and thus of establishing knowledge and trends. Although different sources exist, it is difficult

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



to collect data on this phenomenon, so comparison is difficult among different entities or countries, but also among the different data sources. This challenge is mainly the result of discrepancies in the types of behaviour measured, the way in which cybercrimes are counted and the lack of common agreement about the phenomenon. Thus, as cybercrime is one of the highest priority security issues worldwide, a more systematic and consolidated approach is needed.

Recommendations

Establish a core set of cybercrimes with a systematic data collection

Establishing a data set would provide a common basis for the various cybercrimes to be studied in the framework of official statistics. In addition, an agreement on data collection should be established to avoid measuring incidents in different ways depending on the act or the number of targets providing comparative bases.

Include specificity of cybercrime in national victimisation surveys

In order to reduce the black figure in police statistics, questions about a core set of defined cybercrimes should be included in victimisation surveys, both for individuals and for companies, asking for information about the crime, in order to link the different victims to the crime. This way it will be possible to make comparisons between victimisation surveys as is the case for national victimisation surveys.

Increase awareness about cybercrime

In order to increase the reportability of victims, they should be made aware of the different types of crime that exist and how to identify the signs of online victimisation, which would increase their knowledge of cybercrime, the different ways to report a crime and the importance of doing it.

Authors
Amandine da Silva, Christine Burkhardt and Stefano Caneppele
University of Lausanne, School of Criminal Justice

References

Fafinski, S., William H.D., and Helen Z. M., "Mapping and measuring cybercrime", OII working paper, No. 18, 2010.

Hargreaves C., and Daniel P. "Understanding cyber criminals and measuring their future activity", Lancaster University, 2013.

Mcguire, M. and Dowling, S. "Cyber crime: A review of the evidence", *Summary of key findings and implications. Home Office Research report*, 2013, vol. 75, p. 1-35

Further Reading

Lavorgna A., *Cybercrimes: Critical issues in a global context*. Red Globe Press 2020.

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