CC-DRIVER

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

Policy Brief No. 9

April 2023

Who is this for?

Policy-makers, LEAs, other stakeholders interested in cybercrime policy

Highlights

1 Cybercrime policymaking should take into account the differences in cybersecurity strategies in different countries.

2 Policymakers at the Member State level should ensure congruence with EU-level policy.

3 Effective implementation of engagement tools is required.

4 Good policy needs to be translated into good practice based on examples of effective policy implementation.

5 The credibility of initiatives should be assessed and reassured.

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

CC-DRIVER Policy Toolkit

This Policy Brief gives an overview of the CC-DRIVER Policy Toolkit, which provides high-level guidance for decision-makers but might also be of interest to law enforcement agencies and other stakeholders interested in cybercrime policy. The CC-DRIVER Policy Toolkit consists of five sections, comprising the following:

- Strategy: What are the cybersecurity strategies in different countries
- Legislation: How to create, revise and implement a legislative framework, standards or relevant general principles
- Engagement: How to create effective implementation of engagement tools
- Enforcement: How to translate good policy into good practice, examples of effective policy implementation
- Assessment: How to ensure the credibility of initiatives

Strategy

Key takeaways from the section on strategy are that policy-makers should

- Stress that cyber security is a shared responsibility for everyone
    - More specifically, policymakers should perform a stakeholder mapping exercise to each of the various objectives set out in strategy documentation to ensure complete and equal coverage of all stakeholder groups.
    - Policymakers and LEAs should set goals and empirical indicators to measure the implementation of the desired outcomes.
- Highlight the value of international cooperation and coordination
    - More specifically, LEAs should improve information exchange mechanisms with counterparts in other jurisdictions, including those outside of Europe.
    - Policymakers and LEAs should increase participation on the international stage, such as EU Cybercrime Action Taskforce (J-CAT), which was launched in 2014.
- Highlight the value of public-private sector cooperation and coordination
    - More specifically, policymakers and LEAs should familiarise themselves with organisational cyber security strategies at a high level to ensure alignment with national cyber security strategy documentation.
    - Policymakers should improve the relationships between organisations and regulators by increasing transparency. This will enable the dissemination of industry specific findings and recommendations.

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

- Address human skills as well as technical vulnerabilities
    - More specifically, LEAs should explore the implementation of compulsory cyber hygiene education in the school curriculum.
    - Outline how the fundamental rights and freedoms of citizens will be protected in cyberspace
- Provide definitions for key terms that underpin the objectives outlined
- Assign timeframes and define key performance indicators (KPIs) for each strategic objective
    - More specifically, policymakers should assign realistic target dates for the completion of each strategic objective, as well as interval dates to perform reviews on progress.
    - Policymakers should clearly define the KPIs on which each strategic objective should be measured.
- Provide guidance to address each stage of the cybercrime lifecycle
    - More specifically, policymakers should work closely with the relevant stakeholders who are responsible for the various stages of the cybercrime lifecycle (e.g., legislators for conviction and judges for punishment).
    - Policymakers should perform a lifecycle mapping exercise to each of the various objectives set out in strategy documentation (i.e., national cyber security strategies, or equivalent) to ensure complete and equal coverage of all stages.

Legislation

Many legislative challenges need to be addressed. One of them concerns the question of whether providers of cybercrime-as-a-service (CaaS) can be seen as committing a criminal offence themselves. This depends on whether an offence was already committed, or whether we consider the culpability of the act of offering/facilitating CaaS. Another concerns the role played by the “provider” of CaaS in the context of legal frameworks such as the Budapest Convention and EU legislation.

Moreover, instead of focusing rigidly on the narrow definition of technology, it is better to rely on broader notions of functionality (what is the core technical activity at stake, what function does the technology serve?) and culpability (what is the socially condemnable behaviour at play?).

Juvenile sanctions can be found in the criminal code and specific legislation. Educational measures are given priority, while penalties are used only as a last resort when lenient measures are not sufficient or when the situation requires it.

Identification of an offender and collection of e-evidence must be in compliance with applicable data protection laws, including the General Data Protection Regulation (GDPR) and the Law Enforcement Data Protection Directive.

Digital evidence might be deleted or hidden. The regulators have to carefully consider the scenarios demonstrating the need to preserve evidence and ensure due respect for the fundamental rights of affected individuals and service providers.

Another challenge concerns access to evidence held by providers of online services. The legal framework has to clearly describe the scope of allowed access requests, ensure the cooperation of service providers, set the procedures affecting the response time and consider the fundamental right of both affected individuals and service providers.

Anonymity-oriented measures make locating, gathering and accessing credible e-evidence more difficult. The situation is even more complex because readily available anonymity measures enable of fundamental rights such as the right to privacy, right to data protection and the freedom of expression and information, all protected by the Charter of Fundamental Rights of the EU.

In order for evidence to be used in court, prosecutors have to ensure and demonstrate its integrity. Cybercrime evidence is especially vulnerable to manipulation and accusations of manipulation, due to its digital and (at times) highly technical nature.

Cybercrime investigations might be costly. Regulators have to take into account the limited resources of digital investigators and ensure the existence of efficient, proportional pathways to digital evidence.

Engagement

The CC-DRIVER Policy Toolkit (based on the outputs of the project) makes the following recommendations to foster engagement in cybercrime policymaking.

- **Consider all demographics, not only young people**: In addition to young people, other groups who warrant increased focus are those with learning difficulties, mental health conditions, from under-privileged backgrounds and the elderly.
- **Employ gamification techniques where appropriate**: Engagement activities should leverage aspects of gamification that are proven to be effective. However, while gamification may increase engagement, it can also increase the risk of young people treating criminal acts in the same way as they would in a game. In addition, an important factor to consider is who is employing gamification techniques.
- **Consider dissemination methods outside of cyberspace**: It is crucial to have dissemination methods to reach people who prefer to consume information offline. Examples include magazines, books, seminars via school and community networks, and other analogue formats.
- **Introduce support programmes for victims of cybercrime**: Engagement activities must not only protect those at risk of falling victim to cybercrime and rehabilitate those who are first-time offenders, but also support those who have already fallen victim to cybercrime. Victim support programmes should increase awareness and confidence through a two-way relationship where victims are able to learn from their experiences, connect with other victims and share information to help others.

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

- **Use relatable individuals and role models to communicate important messages to young people**: A select number of engagement activities targeting young people in schools, colleges and universities use police officers to share information and they may not be relatable figures to many young people. Important messages regarding cybersecurity and cybercrime should be disseminated to young people through more familiar faces, such as teachers or inspiring individuals such as celebrities and sports figures, who may represent trusted role models for young people.

Enforcement

- The enforcement section emphasises, amongst other things, that
- regardless of their area of specialism, police officers from all backgrounds should undertake cybersecurity training;
- risk associated with cybercrime ought to be reported in financial terms, where appropriate, allowing people from all backgrounds to accurately interpret the information and make evidence-based decisions;
- cybercrime law should target those who enable cybercrime too;
- responsive action against cybercrime should not be a knee-jerk reaction to high-profile incidents that receive significant media coverage. Instead, they should be the result of timely evidence-based reforms;
- basic data revealing communication between individuals and groups should be retained for a longer period of time so investigators can get access to such data in hindsight. Any such effort needs to be reconciled with data protection norms and rules;
- data exchange should be organised internationally in a way that suits investigative needs;
- more research is needed on the acquisition of solutions to increase victim identification as well as tools for cryptocurrency tracing and decryption and further data analysis tools;
- cybercrime law should lay the ground for investigators to use the undercover capabilities they need.

Assessment

The CC-DRIVER Policy Toolkit (based on the outputs of the project) makes five recommendations to improve the collection, management and analysis of cybercrime data, which are described as follows.

- **Harmonise metrics to measure cybercrime at a European/international level to facilitate comparisons**. These metrics are intended to report meaningful information to stakeholders to indicate areas of strength, pain points, and which areas may deserve a higher allocation of future resource.

- **Ensure that cybercrime datasets are more accessible to all relevant stakeholders**. A central repository should be created for publicly available cybercrime data in European countries. The data stored in the repository should be understandable and updated on a regular basis. Eurostat will be an appropriate body to coordinate national statistics institutes due to its established reputation of publishing high-quality European-wide statistics.
- **Inferences from analysis should consider the limitations of data collection**. Inferences should acknowledge that the widespread underreporting of cybercrimes by both individuals and organisations. Tthe lack of consistent definitions internationally means that the class ification of cybercrimes is likely to vary from country to country.
- **Leverage information-sharing mechanisms to verify cybercrime data and promote collaboration**. Secure and rapid response mechanisms should be developed to transfer data so that domestic and international parties in both the private and public sectors can build more robust cybercrime datasets and learn from the data collected and analysed by each other.
- **Use cybercrime data to reinform strategy, legislation, engagement and enforcement**. The data collected and analysed should be applied to each element to make regular evidence-based reforms. This process can help to make incremental improvements over current approaches to tackling cybercrime.

Concluding Remarks

Further information on the policy recommendations as laid out above, including a Checklist for Policymakers can be found by consulting the CC-DRIVER Policy Tool.

Further Reading

- CC-DRIVER Policy briefs
- CC-DRIVER Newsletters
- CC-DRIVER Press releases
- CC-DRIVER blog

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