CC-DRIVER

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

Policy Brief No. 3

October 2021

ISF

Who is this for?

This policy brief presents the high-level findings of a review and gap analysis of cybersecurity legislation and cybercriminality policies in eight European states. The content is aimed at providing value for all CC-DRIVER stakeholders, in particular the European Commission, legislators, law enforcement agencies (LEAs), organisations and academics.

Highlights

1. National cyber security strategies tend to focus on the needs of businesses and other organisations more than on the needs of individuals.
2. There is a lack of cohesion in Europe and internationally on cybercrime legislation, which hampers attempts to prosecute cybercriminals who work across borders.
3. Engagement activities primarily target young people, although cybercriminals target victims in a range of demographics.
4. The challenges facing law enforcement agencies in combating cybercrime are both numerous and evolving.
5. The collection, management and analysis of cybercrime related data is problematic, leaving the true extent of cybercrime still unknown.

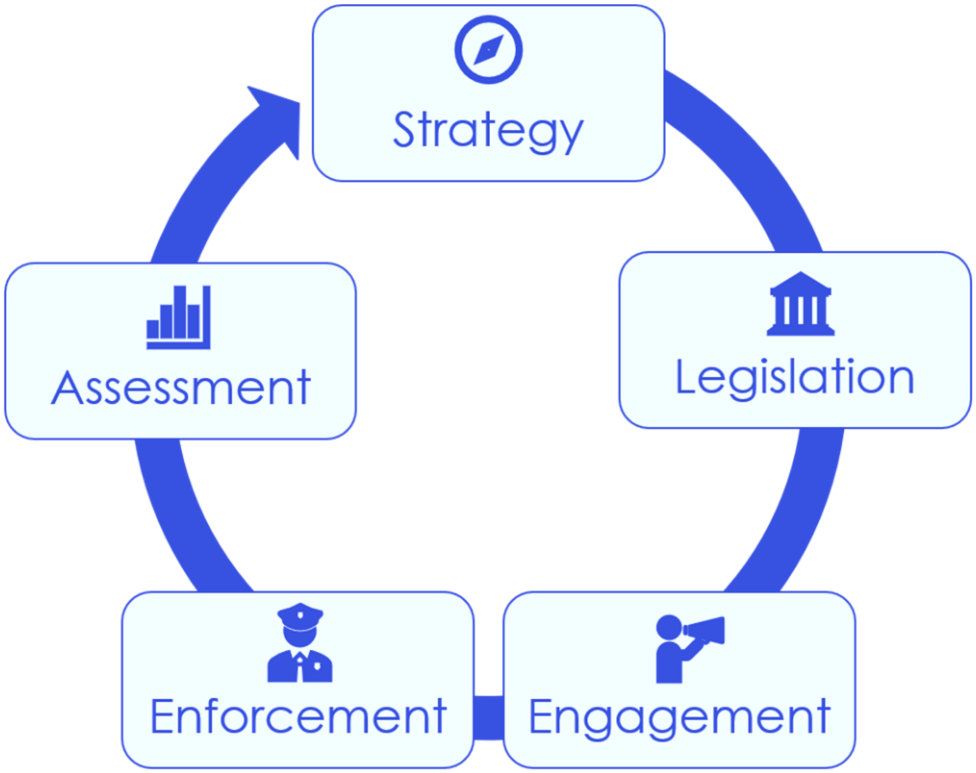
This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

Review and gap analysis of cybersecurity legislation and cybercriminality policies in eight countries

A pragmatic approach to tackling cybercrime

To facilitate a review and gap analysis of existing cybersecurity legislation and cybersecurity policies in eight European countries an analytical framework was required. (see Figure 1). Through conducting research and speaking to experts, a pragmatic approach to tackling cybercrime was developed (see Figure 1).

Figure 1 – A pragmatic approach to tackling cybercrime



The framework is comprised of five elements, all of which are critical to combat cybercrime and bolster cybersecurity capabilities. All elements contribute to the final element, assessment, where resulting data from each of the proceeding four elements should be analysed with a view to make evidence-based revisions. This ongoing feedback mechanism is demonstrated through the framework taking a continuous cycle. While the five elements in the framework follow a logical order (from strategy to assessment), each element has a relationship with and supports each of the others. To achieve optimal output across the entire cybercrime landscape, no element of the framework should be conducted in isolation.

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

A summary of findings

Setting strategy

Target audience

National cyber security strategies outline how states plan on tackling cybercrime and bolstering cybersecurity capabilities. Strategies address a variety of stakeholders, including government agencies, law enforcement agencies (LEAs), organisations and educators. While it is common consensus that cybersecurity is a shared responsibility for everyone in society, the level of attention given to different audiences varies among the different states analysed. It was observed that less attention is given to the individual simply navigating the Internet compared with other stakeholders such as large organisations and businesses. This is arguably one of the biggest vulnerabilities in cyberspace as individuals may not possess the necessary knowledge or capabilities to avoid falling victim to cybercrime.

Perceived threats, threat actors and vulnerabilities

A number of threats, threat actors and vulnerabilities were identified in national cybersecurity strategy documentation. These vary from country to country, however, certain observations made were common across all countries. Cyber-attacks targeting critical national infrastructure and essential service providers, cyber espionage by nation states and vulnerabilities in key sectors such as finance, energy and telecommunications were highlighted across the eight-country scope. This reinforces the observation that strategies tend to focus on the high-profile actors in society rather than on individuals.

Writing legislation

Lack of international cohesion on cybercrime

The legal framework regarding cybercrime and cybersecurity is fragmented and complex. At a fundamental level there is no clear, precise and universally accepted definition for cybercrime. This is compounded by variations in the definitions for individual cybercrime offences and severity of punishment in the form of financial penalties and imprisonment among the countries analyzed. In addition, cybercrime offences can be found across multiple legislative documents, which makes it difficult for interested parties to clearly document cybercrime legislation, and to educate themselves on cybercrime.

Shortcomings in attempts of international harmonisation

The Budapest Convention on Cybercrime is one of few attempts aimed at harmonising the approach to cybercrime between international parties. While an important initiative, the Convention has its shortfalls. For instance, there have been cases of a significant lag between countries signing the treaty and ratifying it (i.e. giving of formal consent making it officially valid). Certain countries have taken as long as 10 years to ratify the Convention, frustrating efforts to act in a timely manner. Countries can also make reservations to elements of the Convention (i.e. a caveat to a state's acceptance of a treaty). Three countries reviewed made at least one reservation limiting the Convention's effectiveness.

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

Facilitating engagement

Target demographics

Engagement ranges from activities that target the general population to activities that focus on specific demographics, generally those identified as high-risk of falling victim to cybercrime. Examples of these groups may include people with learning difficulties, mental health conditions, those from under-privileged backgrounds and the elderly. However, it was observed that young people are the primary focus for the majority of engagement activities, where they are educated on best practices in cyber hygiene, basic cybersecurity skills and employing their cyber-related skills in legitimate lines of work.

Types of engagement

Engagement activities come in many different but typically involve training, initiatives or campaigns. It was observed that engagement tends to be conducted through online mediums, such as social media platforms, as content can be accessed and shared relatively seamlessly by many people globally. In addition, these activities aimed at increasing engagement for cybersecurity and cybercrime issues tend to be provided for free or at minimal cost. This ensures a low barrier to entry for participants, which is particularly important when high-risk demographics are their focus.

Enforcing cybercrime

Keeping up with the criminals

Cybercriminals are becoming increasingly sophisticated at harnessing new technology for adversarial purposes, which presents a significant challenge for LEAs. LEAs and the public sector more generally tend to be severely underfunded in terms of budget, people and technology leaving them without adequate resources to tackle cybercrime most effectively. Comparatively, cybercriminals do not carry this resource burden. More and more inexperienced and less skilled cybercriminals can conduct illicit activity through cybercrime-as-a-service products on the dark web, which are becoming increasingly available.

Cybercrimes going unreported

A significant number of cybercrimes go unreported each year. To illustrate this, during lockdown in the UK less than two per cent of cybercrime offences under the Computer Misuse Act were reported to authorities. The underreporting of cybercrimes is true for both individual and organisational victims. The process for an individual reporting a cybercrime to authorities is not as clear compared with the process for reporting a traditional crime. Organisations often choose to withhold information on cyber-attacks in an attempt to prevent adverse effects on stock prices, reputational damage and regulatory fines.

Assessing results

Cybercrime is proliferating

The data collected on reported cybercrime offences in the timeframe, 2017 to 2019, indicates that cybercrime offences are increasing. Notably, in the case of certain countries, such as the

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

Netherlands, traditional crimes are decreasing in frequency while cybercrime is proliferating. It was also observed that the COVID-19 pandemic sparked a further uptrend in cybercrime offences, in particular ransomware, child sexual abuse material and payment fraud with phishing and social engineering playing an important role in facilitating other forms of cybercrime.[1]

Difficulties collecting and analysing cybercrime data

The collection of cybercrime data is in its relative infancy which means a lack of accessibility and consistency to some extent. In some countries under review the national body responsible for publishing statistics did not do so for data relating to cybercrime. As a result, data was instead obtained from secondary sources. Compounding this is that each country collects and reports different metrics for cybercrime making the comparison or aggregation of data potentially misleading. The underreporting of cybercrime adds further uncertainty to data analysis.

Recommendations

1. Provide comprehensive and balanced guidance for all stakeholders
2. Maintain a web-based repository of cybercrime offences across Europe
3. Engage with all high-risk demographics, including victims of cybercrime
4. Train more police officers in cybersecurity and provide incentives to report cybercrime
5. Harmoise metrics at a European level to facilitate robust data analysis

For more detail on the common observations and differences between the eight-country scope and to view the complete list of all 25 recommendations proposed by the consortium read the full report (available on the CC-DRIVER website).

References

[1] Europol, "COVID-19 sparks upward trend in cybercrime" (2020), https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime

Further Reading

- CC-DRIVER D5.1 - Review and gap analysis of cybersecurity legislation and cybercriminality policies in eight countries
- EU Cybersecurity Strategy for the Digital Decade
- ISF Legal and Regulatory Implications for Information Security

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