CC-DRIVER

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

D5.1 — Review and gap analysis of cybersecurity legislation and cybercriminality policies in eight countries

WP5 — A cybercrime policy toolkit

Abstract

This report presents a review and gap analysis of cybersecurity legislation and cybercriminality policies in eight European countries. Findings are reported from desktop research, questionnaires and workshops, involving contributions from eight partners in the CC-DRIVER consortium from a diverse set of backgrounds including industry, research and law enforcement. The aim of these activities was to conduct a non-exhaustive but broad review and analysis of five elements forming an analytical framework for a gap assessment of existing legislations and policies, and to provide recommendations for improvement.

Key words: Cybercrime, cybersecurity, legislation, policy, review, analysis

Contributors

Lead

Information Security Forum (ISF) – Bruce Page & Aman Behl

Other

- Bavarian Police Academy (BayHfoeD)
- KEMEA
- Policia Juridiciaria (PJ)
- SIMAVI (SIV)
- Trilateral Research (TRI)
- University of East London (UEL)
- University of Lausanne (UNIL)
- Valencia Local Police (PLV)

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

Contents

Executive summary

Introduction

- The purpose of this document is to report findings from CC-DRIVER tasks T5.1 and T5.2
- This report was authored by Information Security Forum with review contributions from the University of East London, University of Lausanne and Trilateral Research Ltd

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

Methodology

- The review and analysis process followed by partners is outlined in Section 2
- The analytical framework proposed to evaluate five key elements in bolstering cybersecurity capabilities and fighting against cybercrime is presented in Figure 2

Strategy

- Findings from the review and analysis of national cyber security strategy (NCSS) documentation in the eight countries
- Questionnaires relating to cybersecurity strategies were completed by six partner organisations
- Workshops relating to cybersecurity strategies were attended by eight partners

Legislation

- Findings from the review and analysis of cybercrime-related provisions in criminal code documentation, where available, in the eight countries
- Questionnaires relating to the cybercrime legislative landscape were completed by six partner organisations
- Workshops relating to the cybercrime legislative landscape were attended by seven partners

Engagement

- Findings from the review and analysis of 45 engagement activities in the eight countries, at the European level and internationally
- Questionnaires relating to engagement activities were completed by six partner organisations
- Workshops relating to engagement activities were attended by nine partners

Enforcement

- Findings from the review and analysis of the enforcement landscape surrounding cybercrime in the eight countries
- Questionnaires relating to the enforcement landscape were completed by six partner organisations
- Workshops relating to the enforcement landscape were attended by seven partners

Assessment

- Findings from the descriptive analysis of cybercrime data collected from the bodies responsible for publishing national statistics in each of the eight countries
- Questionnaires relating to the collection, management, analysis and application of cybercrime data were completed by four partner organisations
- Workshops relating to the collection, management, analysis and application of cybercrime data were attended by seven partners

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

List of figures

List of tables

Table 1 - List of acronyms/abbreviations

Abbreviation	Explanation
BayHfoeD	Bavarian police academy
CaaS	Cybercrime-as-a-service
CBS	Central Bureau for Statistics
CLRNN	Criminal Law Reform Now Network
ECSC	European Cyber Security Challenge
ENISA	The European Union Agency for Cybersecurity
EU	European Union
EU-RES	EU restricted
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
ISF	Information Security Forum
ICT	Information communication technology
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
J-CAT	Joint Cybercrime Action Taskforce
KPI	Key performance indicator
LEA	Law enforcement agency
NATO	North Atlantic Treaty Organisation

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

NCA	National Crime Agency
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
NGO	Non-governmental organisation
NIS Directive	Network and Information Systems Directive
NIST	National Institute of Standards and Technology
ONS	Office of National Statistics
SEC	Statistical System of Crime
SIM	Subscriber identity module
T5.1	Task 5.1
UK	United Kingdom
UN	United Nations
UEL	University of East London
UNIL	University of Lausanne
WFH	Work-from-home
WP5	Work Package 5

Table 2 - Glossary of terms

Term	Explanation
Cybercrime	"Any crime that is facilitated or committed using a computer, network or hardware device." (Gordon & Ford, 2006, p. 14)
Cybersecurity	"The protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures." (UK NCSS, 2016-2021)
Cyberspace	"A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (NIST SP 800)

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

1. Introduction

1.1 Background

CC-DRIVER is a research and innovation project funded by the European Commission as part of the Horizon 2020 Programme. The goal of the project is to understand the drivers of cybercriminality and develop new methods to prevent, investigate and mitigate cybercriminal behaviour. The project consortium consists of 13 stakeholders from across Europe, including law enforcement agencies (LEAs), academic institutions, non-governmental organisations (NGOs) and organisations in industry.

1.2 Objectives

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 cyberdelinquency and crime. In support of this, Work Package 5 (WP5) involves development of a cybercrime policy toolkit, which contains a set of guidelines and tools to help policymakers and other stakeholders more effectively combat cybercriminality. The target audience for the cybercrime policy toolkit will primarily be LEAs and The European Union Agency for Cybersecurity (ENISA).

This deliverable responds to the Tasks 5.1 and 5.2 in WP5, which states the following:

- Conduct a policy review of cybersecurity policies in eight Member States
- Conduct a gap analysis of existing policies.

1.3 Structure of the report

This report is structured into nine chapters. The introduction locates this deliverable within CC-DRIVER's objectives and outlines the scope, strengths and limitations of the report. Following this is the methodology which describes the review and analysis processes conducted and how an analytical framework was developed. The subsequent chapters address each element of the analytical framework where WP5 Partners identified key similarities and differences across the countries and proposed recommendations based on the findings. The common observations applied across all eight countries under review but with varying levels of focus and specificity, while the differences concern observations which were identified in some or most countries, but not in all. Finally, the conclusion summarises the key findings of the report with suggestions for future work.

1.4 Scope, strengths, and limitations

This report represents the first of two outputs from WP5, a review and gap analysis of cybersecurity legislation and cybercriminality policies across eight European countries: France, Germany, Italy, Netherlands, Romania, Spain, Sweden, and the United Kingdom. The second output will be a toolkit for policymakers following the completion of Tasks 5.4 and 5.5.

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

The eight countries analysed in this report align with the geographic scope of research conducted in CC-DRIVER Work Package 3 (WP3), a survey investigating the drivers to juvenile cybercrime. The purpose of aligning countries was to enable cross-referencing of results across these CC-DRIVER Work Packages. As a result of this, Greece, Portugal, and Switzerland, which were originally in-scope countries for the WP5 review and gap analysis, were replaced by Italy, Netherlands, and Sweden.

A key strength of this deliverable was the empirical breadth of the research conducted. The approach taken enabled an overview of the legislative and policy landscape in eight countries without dedicating a disproportionate amount of focus to one single country or item of legislation. Another strength of this deliverable was the range of activities conducted and variety of stakeholders consulted to produce it. These activities included performing desktop research, analysing partner-completed questionnaires, and hosting roundtables and workshops attended by multi-disciplinary CC-DRIVER stakeholders and security professionals from ISF Member organisations. This set of activities allowed the consortium to gather input from a variety of sources, in keeping with the provisions of the Grant Agreement and so ensuring the quality and reliability of the output.

There were also a couple of limitations highlighted. Firstly, although the WP5 consortium is diverse, it would have been advantageous to have certain professionals present. For example, discussions surrounding the regulatory aspect on criminal law and criminal law procedure would have benefitted from contributions from a greater number of lawyers and legal experts. Secondly, partly due to the change of in-scope countries for alignment with other CC-DRIVER work packages, the WP5 consortium lacked Partners from four of the in-scope countries: France, Italy, Netherlands, and Sweden. The responsibility of collecting, reviewing, and analysing the dataset for these countries was shared among the existing WP5 Partners. As a result of this, some finer details mostly known by citizens of a country may have been overlooked to some extent.

It is also important to note that all work conducted under WP5 was classified as EU-restricted (EU-RES) by the European Commission. To adhere to EU-RES security requirements, all files exchanged between CC-DRIVER Partners and internally within ISF, were done so using Zed encryption software. Security processes followed were in accordance with documentation available on the Project's Google Drive repository and the training provided by the project coordinator.

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

2. Methodology

This chapter outlines the steps taken to produce the findings for this report: a review process, a gap analysis and the development of an analytical framework consisting of five elements.

2.1 Review

The first stage of producing this report was a review of cybersecurity legislation and cybercriminality policies in the eight in-scope countries. This was conducted under Task 5.1, a sub task of WP5, which took place between months 3 and 10 of the Project.

The review involved desktop research performed by all Partners in the consortium as well as special interest group roundtables with subject matter experts. Where possible, specific focus of the review was given to the human factors driving cybercrime and cybercriminality among young people, in accordance with the wider goals of the CC-DRIVER project.

Members of the project consortium who contributed to the review process were Hochschule für den öffentlichen Dienst in Bayern (Bavarian police academy) [BayHfoeD], KEMEA, Policia Judiciaria, SIMAVI, Trilateral Research Ltd, and Valencia Local Police.

2.2 Analysis

The second stage of producing this report involved analysing the information collected during the review stage, by conducting a gap analysis of cybersecurity legislation and cybercriminality policies in the eight countries. This involved identifying where legislation and policies are the same, similar or different with a view to recommending changes. This was conducted under Task 5.2, the subsequent sub task of WP5, which took place between months 11 and 16 of the project. The analysis was supported by questionnaires and workshops[1] completed and attended by the task consortium.

Five questionnaires were completed by partners prior to each workshop (see Appendix). The intended purpose was to ensure partners were briefed and had an opportunity to provide their initial thoughts on proposed issues to be covered during the workshops. Each questionnaire was completed by six partners on average also contained an average of six questions, typically requiring free-hand text answers. These questionnaires served their purpose of stimulating ideas for workshop discussions.

The five workshops conducted covered the strategy, legislation, engagement, enforcement and assessment of cybersecurity and cybercrime in the eight countries under review. The average attendance was eight partners, with a minimum attendance of seven Partners and a maximum attendance of nine partners. Attendees came from academic, law enforcement, NGO, and industry backgrounds. During these two-and-a-half-hour-long workshops, partners discussed the main

[1] R. Barbour, Doing focus groups. The SAGE Handbook of Qualitative Data Analysis Handbook, 2008.

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

points highlighted in the questionnaires and proposed recommendations to improve the effectiveness of the fight against cybercrime.

Members of the project consortium who contributed to the gap analysis were Policia Juridiciaria, SIMAVI, Trilateral Research Ltd, University of East London, and Valencia Local Police.

2.3 Analytical framework development

During the early stages of the review process, it became clear that legislation represents only one of many tools that can be employed to address the issues relating to cybersecurity and cybercrime. The partners contributing to WP5 understood that legislation can only be effective in strengthening cybersecurity capabilities and reducing cybersecurity-related offences when employed in tandem with other tools and techniques.

WP5 Partners developed a practical analytical framework to examine the various tools that need to complement legislation in order to be effective. This resulted in the establishment of a pragmatic approach to tackling cybercrime. The framework (as shown in Figure 1) illustrates the relationship between four elements: lawmakers on one side and the citizenry on the other, as well as two other key elements bridging the gap between them. Awareness aims to increase visibility for cybersecurity and cybercrime related issues while enforcement aims to apprehend the perpetrators of cybercrime.

The framework reads left to right, starting with the lawmakers who formulate legislation and policy that ultimately reaches the general population who are subject to them. In-between these two groups are awareness activities that aim to increase the reach of legislation and policies as well as enforcement activities, which principally involves LEA efforts to uphold cybercrime-related laws.

Figure 1 – A pragmatic approach to tackling cybercrime (v1)

This initial framework provided a basis for discussion amongst WP5 partners who further identified three main areas to improve it:

1 Firstly, the horizontal direction from left to right implies a linear relationship between the four elements. This fails to demonstrate a necessary feedback mechanism, which enables regular evidence-based revisions to each element over time to improve its effectiveness.

2 Secondly, there is no coverage of the overarching direction set for cybersecurity and cybercrime at a national level. This is typically disseminated in the form of national cyber security strategy (NCSS) documentation. WP5 partners agreed that strategy warrants inclusion in the framework because it tends to dictate and define activities supporting legislation and policy.

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

3 Thirdly, awareness is a sub-set of wider activities aimed at increasing engagement with cybersecurity and cybercrime issues. Other examples of engagement activities beyond awareness include the education and training of specific high-risk demographics such as young people or first-time offenders who are prone to reoffending. WP5 partners believed that this element should reflect all types of engagement activities.

Taking these three observations into account and consulting other frameworks, such as EU Policy Cycle to Tackle Organised and Serious International Crime[2], our analytical framework was revised to comprise five elements displayed in a continuous cycle (as shown in Figure 2) rather than the previous four-part linear chain.

Figure 2 – A pragmatic approach to tackling cybercrime (v2)

1	Strategy	The overarching direction and target objectives set for cybersecurity and cybercrime.
2	Legislation	The legal framework governing the behaviour of people in cyberspace.
3	Engagement	Activities aimed at increasing reach and awareness for cybersecurity and cybercrime related issues.
4	Enforcement	Ensuring compliance with laws, regulation, and standards typically performed by LEAs.

[2] Council of the European Union, Empact: The EU Policy Cycle to Tackle Organised and Serious International Crime, 2018.

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

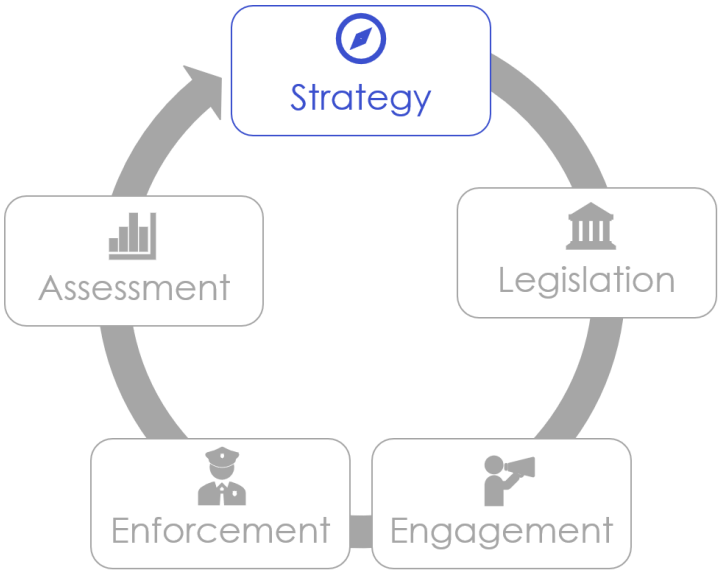
5	Assessment	The data collected on cybersecurity and cybercrime used to inform future decision making.

All elements of the framework contribute to the final element, assessment, where resulting data should then be analysed with a view to make evidence-based revisions to the four preceding elements. 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. No element of the framework should be conducted in isolation.

The framework for a pragmatic approach to tackling cybercrime allowed WP5 Partners to structure the review and analysis of the data gathered as well as present the findings of this report.

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

3. Strategy



Strategy concerns the overarching direction and objectives set for bolstering cybersecurity capabilities and tackling cybersecurity related offences. Strategies provide a plan for achieving desired objectives, typically within a specified timeframe. Strategic documents are produced at three levels:

1. Organisational level (e.g., corporate and security strategies)
2. National level (i.e., national cyber security strategies)
3. International level (e.g., the EU's Cybersecurity Strategy for the Digital Decade)

In this report, the partners review and analyse national cyber security strategies (NCSS) for all eight countries.

Table 3 – Strategic documents reviewed

DOCUMENT	COUNTRY	IMPLEMENTATION DATE
French National Digital Security Strategy	France	2015
Cyber Security Strategy for Germany	Germany	2016
The Italian Cybersecurity Action Plan	Italy	2017
National Cyber Security Strategy 2	Netherlands	2018
Cyber Security Strategy of Romania	Romania	2013
National Cybersecurity Strategy	Spain	2019

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

Comprehensive Information and Cyber Security Action Plan for the years 2019 – 2022	Sweden	2019
National Cyber Security Strategy	United Kingdom	2016

Each country in the European Union (EU) is required to produce a document of this type or equivalent. National Cyber Security Strategy is typically the overarching naming convention adopted, although other versions include National Digital Security Strategy and Cybersecurity Action Plan.

3.1 Common strategic objectives

WP5 partners identified five common strategic objectives in NCSS documentation.

1 **Highlighting cybersecurity as a shared responsibility for everyone in society**

Strategies across all eight countries emphasise that everyone should be considered as a stakeholder in cybersecurity and the fight against cybercrime. While each country has unique demographics and face different types and levels of threat, there is a consensus that all able members of society have a role to play in making cyberspace safer. However, this view must consider vulnerable populations, such as young people, who due to their vulnerability must be adequately protected at a policy level. In some nations' strategies, parallels are drawn between the need to manage security in cyberspace just as we manage security in the physical domain. For example, the Netherlands manage expectations by recognising that in a similar way to the physical domain, 100 per cent security in cyberspace is unattainable.

2 **Ensuring the protection of essential service providers and critical national infrastructure**

Nation states consider essential service providers and operators of critical national infrastructure to have control of mission-critical assets. Therefore, these providers and operators were a focus in all eight strategic documents. Severe disruption, damage and financial loss may be the result of mission-critical assets being comprised regardless of whether the threat vector is classified as adversarial, environmental, accidental or negligence. This is because of their high interdependence and the need for their use by the whole of society. While these mission-critical assets are frequently addressed in strategic documents, WP5 partners believe that they receive disproportionately little funding compared with their importance. Examples of essential service providers and operators of critical national infrastructure include sectors such as transport, energy, healthcare, telecommunications and finance.

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

3 Increasing international cooperation and coordination

The cross-border and multi-jurisdictional nature of cybercrime makes cooperation and coordination among national and international parties essential in preventing crime and prosecuting cybercriminals. Strategies highlight various relationships that achieve this, including bilateral relationships, unions (e.g., the EU), alliances (e.g., the United Nations (UN)) and the North Atlantic Treaty Organisation (NATO)) and others. The EU Cybercrime Action Taskforce (J-CAT)[3] launched in 2014 is an example of a mechanism specifically created to aid the coordination of European action against cybercrime and exchange of sensitive data. All eight of the countries under review are members of this Taskforce. Although mechanisms such as these exist, barriers to international cooperation and coordination remain due to growing tensions surrounding cyberespionage and cyberwarfare. Recent incidents, such as SolarWinds[4] and the Colonial Pipeline[5] attacks, demonstrate how fragile the international landscape is when it comes to cybersecurity.

4 Increasing collaboration and coordination between the public and private sector

The complex nature of cybercrime requires the public and private sectors to work closely together to leverage each other's strengths and mitigate weaknesses. For instance, LEAs and the public sector more generally tend to be weakened by resource constraints in terms of budget, people and technology, relative to private sector organisations. On the other hand, a strength of LEAs and the public sector is their ability to collect and analyse large amounts of sensitive data, which will be relevant to private sector organisations (e.g., threat intelligence data). These two examples demonstrate ways in which the public and private sector can assist each other to make collective gains in this space.

5 Developing human skills as well as technical capabilities

The strategic objectives outlined in NCSS documentation were balanced in terms of advancing both technical capabilities and human skills. A combination of both approaches is required to effectively improve cybersecurity capabilities and reduce cybersecurity-related offences. Often, countries and organisations can place significant weight on furthering technical capabilities and neglect the human aspect. This is potentially dangerous because a high proportion of cyber incidents can be attributed to the insider threat whether malice, accidental or negligent. For instance, 88 per cent of data breaches reported to the UK Information Commissioner's Office were attributed to human error, rather than vulnerabilities in the underlying technologies.[6] The measures outlined in strategies aimed at

[3] Europol, "Joint Cybercrime Action Taskforce (J-CAT)". https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

[4] Reuters, "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft President", 2021. https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R

[5] Reuters, "Colonial Pipeline paid hackers nearly $5 mln in ransom – Bloomberg News", 2021. https://www.reuters.com/business/energy/colonial-pipeline-paid-hackers-nearly-5-mln-ransom-bloomberg-news-2021-05-13/

[6] L. Ingram, "88% of UK data breaches caused by human error, not cyberattacks", Verdict, 2018. https://www.verdict.co.uk/uk-data-breaches-human-error/

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

developing human skills included awareness campaigns, education, training as well as dedicated evidence-based intervention mechanisms that are routinely evaluated and updated.

3.2 Differences in strategic objectives

Three main differences were also identified across NCSS documentation in the eight countries.

1 Protecting the fundamental rights and freedoms of citizens

Protecting the fundamental rights and freedoms of citizen's in cyberspace is equally as important as it is in the physical domain. While cybersecurity is at the core of privacy, the protection of personal data, the freedom of expression and access to information, instances such as the Pegasus spyware scandal demonstrate how these can be violated.[7] The reference to the protection of rights and freedoms was observed across most strategic documents reviewed, for example, The Netherlands indicate that cybersecurity cannot be achieved while ignoring fundamental rights, values, and socio-economic benefits.[8] However, Italy, Germany and Romania were exceptions to this as they made no reference.

2 Providing definitions for key terms underpinning proposed actions

A well-documented and longstanding barrier to progress in making cyberspace safer is the lack of consistency regarding the definitions of key terms. This issue is investigated in a review conducted by Phillips, et al. (2021) in which the principle finding was that there is in fact no single, clear, precise and universally accepted definition of cybercrime; the content that formed the basis of this paper also appears in CC-DRIVER deliverable D2.1 titled "Nature of and perspectives on cybercrime".[9] Through the review of strategic documentation, WP5 partners observed that this issue extends further to key terms other than cybercrime such as cybersecurity and cyberspace.

As part of the gap analysis of NCSS documentation, WP5 partners observed definitions for these three key terms: cybersecurity, cybercrime and cyberspace (see Figure 3). The results displayed in the table below illustrate the lack of definitions provided across strategic documentation. This limits progress in countering cybercrime as definitions are fundamental in providing the basis from which further action is derived. Notably, Romania and the United Kingdom provide definitions for all three key terms while France, Italy and Sweden do not provide definitions for any.

[7] S. Kirchgaessner., P. Lewis, D. Pegg, S. Cutler, N. Lakhani, and M. Safi, "Revealed: leak uncovers global abuse of cyber-surveillance weapon", The Guardian, 2021. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus
[8] National Cyber Security Strategy 2: From awareness to capability, Netherlands, p.17.
[9] Phillips, K., Davidson, J., Farr, R., Burkhardt, C., Caneppele, S., & Aiken, M. (2021). Conceptualising Cybercrime: Definitions, Typologies and Taxonomies. Manuscript submitted for publication.

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

Figure 3 – Coverage of key definitions in NCSS documentation

TERMS	FR	DE	IT	NL	RO	ES	SE	UK
Cybersecurity		X		X	X			X
Cybercrime					X	X		X
Cyberspace		X			X	X		X

3 Taking a risk-based approach to managing cybersecurity and cybercrime

A risk-based approach to managing cybersecurity should prioritise proposed activities and provide assurance on them once deployed. Within any organisation or nation, it is important to implement the highest-priority security measures first (i.e., those that make the greatest reduction of the highest-priority risks), as well as ensuring they work as intended and do not cause unintentional harm. Italy, the Netherlands and Sweden all make specific reference to employing a 'risk-based' approach to managing cybersecurity in their strategy documents. However, these three documents do not explicitly prioritise the objectives outlined, provide assurance on measures outlined in previous strategies or specify the criteria to do this against.

3.3 Recommendations to increase the effectiveness of strategy

Four recommendations have been proposed by WP5 partners aimed at improving the quality and effectiveness of NCSS documentation.

1 Provide comprehensive and balanced guidance for all stakeholders

Countries highlight that cybersecurity and cybercrime are a shared responsibility for everyone in society yet do not provide equal guidance for all relevant stakeholders. Guidance provided in NCSS documentation tends to be focused on a subset of stakeholders, typically governments, essential service providers, operators of critical national infrastructure and large organisations due to the high-stake consequences should these entities be compromised. Other crucial stakeholders, such as small and medium-sized organisations, as well as individuals from high-risk demographics such as young people, receive significantly less guidance while they comprise some of the most vulnerable in society.

2 Assign realistic timeframes to objectives and agree metrics to track progress

Tracking the completion of strategic objectives outlined in NCSS documentation is essential. Seven of the eight documents stated that objectives will be reviewed, however, with varying levels of frequency. Some countries were prescriptive, for example Spain, who used the

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

term 'annually', while others were more ambiguous and used terms such as 'regularly' or 'no fixed duration'. France was the only country that did not explicitly state a review process with which to revise the objectives in their NCSS. WP5 partners believe that countries would benefit from assigning realistic timeframes to each specific objective as well as defining key performance indicators (KPIs). This will facilitate a more transparent review process and provide increased assurance to stakeholders. Across the countries reviewed, Sweden was the only instance to have provided time range targets to achieve each objective.

3 Provide guidance to address all stages of the cybercrime lifecycle

Cybercrime is subject to a lifecycle in the same way as other concepts. The paper "Youth Pathways into Cybercrime" proposes a five-stage cybercrime lifecycle: identification, prevention, conviction, punishment and rehabilitation,[10] which helped WP5 partners to check for coverage of all stages. The first two stages of the cybercrime lifecycle (i.e., identification and prevention) receive significant attention in strategic documentation through information regarding the threats and vulnerabilities identified. However, this level of focus diminishes for the latter stages of the lifecycle. Conviction and punishment receive less attention with rehabilitation, the last stage, receiving little to no coverage at all. Addressing the rehabilitation stage is critical because this part of the lifecycle concerns both some of the most dangerous and vulnerable in society.

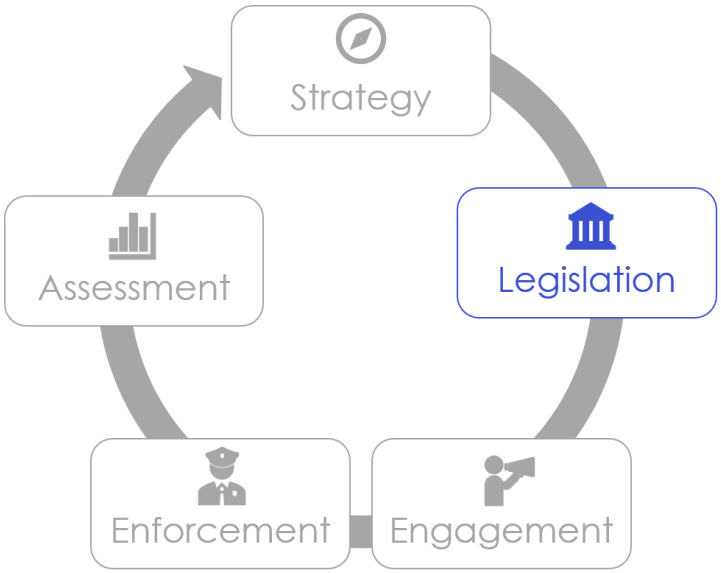
4 Produce NCSS documentation to allow for easy and accessible comparability and redressal of issues

Currently, there is no specified structure for NCSS documentation. While a common core set of strategic objectives was observed by WP5 partners, the structure of strategic documentation across the eight countries varies significantly, which makes comparability and analysis challenging. WP5 partners believe that the ability for countries, especially EU Member States, to compare their strategic objectives with peers will allow them to benchmark themselves but also learn from and replicate demonstrations of good practice. In addition, documents following a pre-defined structure will allow countries to redress their strategies more clearly and easily, enabling the writers of the document to continuously update it in line with the ever-changing cyber landscape.

[10] Aiken, M., Davidson, J., Amann, P., *Youth Pathways into Cybercrime*, University of Middlesex, 2016.

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

4. Legislation



Legislation concerns the legal framework surrounding cybersecurity and cybercrime governing the behaviour of people in cyberspace. While legislation is a fundamental element in the pragmatic approach to tackling cybercrime framework, it is essential that it is supported by, for example, engagement activities to raise the profile of new and updated items of legislation and law enforcement authorities who must uphold it. Legislation and other legally binding items are present at three levels:

1. Local legislation (e.g., bylaws)
2. National legislation (e.g., criminal codes)
3. Supranational legislation (e.g., EU Cybersecurity Act)

For this report, partners reviewed and analysed criminal code documentation, where available, in each of the countries. While there are several legislative documents that exist in each country, WP partners focussed on the most common legislative document that pertained to cybercrime, which was the criminal code.

However, the United Kingdom (England & Wales) does not feature a criminal code as part of its national legislation, although it has been recommended and attempted numerous times. The UK employs a common law system, which differs from the civil law system observed in other European countries. Accommodating this, WP5 partners substituted the UK's Computer Misuse Act (1990) as a replacement where cybercrime related provisions were reviewed.

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

Table 4 – Legislative documents reviewed

DOCUMENT	COUNTRY	CORRECT AS OF
Criminal Code of the French Republic	France	2005
German Criminal Code	Germany	2013
Italian Penal Code	Italy	2009
Criminal Code of the Kingdom of Netherlands	Netherlands	2012
Criminal Code of the Kingdom of Romania	Romania	2017
Criminal Code of the Kingdom of Spain	Spain	2013
Criminal Code of the Kingdom of Sweden	Sweden	2020
See section 4.2.1 for relevant criminal law	UK (England & Wales)	N/A

4.1 Common legislative observations

Seven observations were made by WP5 partners regarding the overarching legislative landscape in Europe.

1 Lack of harmonisation regarding cybercrime definitions, sentences and fines

The definitions, imprisonment lengths and monetary fines for the same cybercrime offence in criminal code documentation vary from country to country.

Firstly, the lack of harmonisation surrounding definitions is a well-documented and fundamental challenge in tackling cybercrime globally. From our data set, the definitions for illegal access offences can demonstrate this point well. For example, the Criminal Code of the Kingdom of Netherlands and United Kingdom's Computer Misuse Act specify that the crime of illegal access requires the perpetrator to act intentionally. However, this is not made clear in the definitions provided by other countries under review.

Secondly, it is difficult to compare the sentences of each cybercrime across the eight countries. This is because sentences vary depending on the severity of the crime committed and subject to judge subjectivity. To illustrate this gap, data interference offences can range from six months to 14 years depending on the country and severity. However, for other crimes, this range is less, for instance, illegal access offences, which can range from three months to three years depending on the country and severity.

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

Thirdly, limited data were available for the fines associated with cybercrimes in criminal code documentation. However, where this data was available, the partners observed differences across the eight countries. For example, illegal access offences in the Netherlands result in a fine of €11,250, while in France it is €30,000. This demonstrates the disparity of financial penalties across the data set.

2 Legislation relating to cybercrime is located across multiple documents limiting ease and accessibility

Each country under review has various other legislative documents which concern cybercrime offences to some extent. Stand-alone legislative items can exist for offences relating to data protection, monitoring, infrastructure and other sector-specific offences. WP5 partners believe that this variety of documentation can limit the ease and accessibility of legislation for a variety of stakeholders. This applies to perpetrators who need to be made aware of the consequences of their actions, victims who feel the need to improve their awareness and the general population who should educate themselves.

3 Adopting and revising legislation is relatively immobile

Legislation is relatively slow in terms of the speed of adoption and the implementation of amendments. In terms of the latter, while it is true that good legislation should be able to withstand future uncertainties, proposed amendments should be implemented as expediently as possible. A prime example of where this is the case is the Computer Misuse Act (1990) in England and Wales, which has come under criticism for being outdated. A report released by the Criminal Law Reform Now Network (CLRNN) in 2020 concluded that the Computer Misuse Act is 'crying out for reform'.[11] The report highlighted several shortcomings of the legislation, which includes providing a confused legal framework, using ambiguous terminology and lacking prosecution guidance.

4 Legislation can criminalise or deter non-culpable actors

In some instances, legislation can fail to protect or even deter individuals and groups who are trying to further cyber security capabilities and reduce cybercrime. This issue was another shortcoming of the Computer Misuse Act (1990) highlighted in the CLRNN report. Those acting without malice but at risk of falling victim to this include penetration testers, academics, researchers, journalists, or negligent members of the public. For example, under the Act, an individual who found a lost phone and checked it for the owner's contact details can be prosecuted. Also, under the Act, threat intelligence professionals are restricted from using the most effective means of testing and protecting systems. This may act as a deterrence because these professionals cannot test the capabilities being employed by cybercriminals and nation states. Ultimately, by criminalising or deterring non-culpable actors, systems, tools and technology will fail to be rigorously tested.

[11] McKay, S. et al, *Reforming the Computer Misuse Act 1990*, Criminal Law Reform Now Network (CLRNN), 2020.

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

5 Limited legislation specifically aimed at assisting the cross-border investigation of cybercrime

The cross-border and multijurisdictional aspect of cybercrime can make investigation difficult. To illustrate this, in 2018, the European Commission reported that in the EU 'more than half of all criminal investigations today include a cross-border request to access electronic evidence'.[12] Given this, the European Arrest Warrant[13] is one of a limited number of legislative items at the European level specifically aimed at aiding this process. LEAs must leverage techniques used in solving other forms of cross-border crime and apply them to the domain of cybercrime. It may be the case that countries are reluctant to be subject to such legislation because it may compromise the secrecy surrounding their cybersecurity capabilities. With the increasing frequency of cyberespionage and cyber-warfare in the form of state-sponsored cyber-attacks, this is a possibility.

6 Shortcomings in attempts at European and international harmonisation

Instruments such as the NIS Directive and the Budapest Convention on Cybercrime represent attempts at harmonising approaches to cybercrime at a European and international level, respectively. While these attempts are a step in the right direction, some notable shortcomings of both instruments have been observed.

The NIS Directive, is as it says, a European directive and not a regulation. This gives EU Member States the freedom of transposing requirements into national law. Naturally, this will result in diverging implementation of the directive in each country across Europe. Additionally, the responsibility of transposing the NIS Directive was given to pre-existing information security government agencies rather than to multiple fit-for-purpose, sector-specific authorities potentially meaning that issues are not viewed through a diversified lens.

In terms of the Budapest Convention on Cybercrime, there remains a significant time lag between countries signing the Convention and ratifying it. Ratification is the giving of formal consent to a treaty, contract or agreement, making it officially valid. To demonstrate this, while all eight countries under review signed the Convention in 2001, Romania was the earliest to ratify in 2004, while the United Kingdom ratified in 2011 and Sweden's ratification only come into force in August 2021. Another limiting factor is the ability for countries to make reservations to the Convention. While this allows countries to achieve partial adherence to the Convention it also dilutes it as fewer requirements are met. Of the countries reviewed, France (2), Germany (1) and England & Wales (3) have made reservations to the Budapest Convention on Cybercrime.

[12] Europol, "E-evidence - cross-border access to electronic evidence", 2019. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

[13] European Commission, "European arrest warrant". https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/european-arrest-warrant_en

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

4.2 Gap analysis of criminal codes

To facilitate a gap analysis of criminal codes, the partners outlined a set of cybercrimes for comparison. For this purpose, the partners use the Council of Europe's Convention on Cybercrime classification system.[14] This five-category system includes:

1. Offences against the confidentiality, integrity and availability of computer data and systems
2. Computer-related offences
3. Content-related offences
4. Offences related to infringements of copyrights and related rights
5. Acts of a racist and xenophobic nature committed through computer systems

The fifth category, acts of a racist and xenophobic nature committed through computer systems, was an additional protocol added to the Convention in 2003.[15]

The results of the gap analysis were split into two tables: cyber-dependent crimes (category 1) (as shown in Figure 4) and cyber-enabled crimes (categories 2, 3, 4 and 5) (as shown in Figure 5). Cyber-dependent crimes are defined as crimes committed using computers, computer networks or other forms of information communication technology (ICT).[16] Cyber-enabled crimes are traditional crimes that can be increased in their scale or reach by use of computers, computer networks or other forms of information communication technology (ICT).[17]

[14] Council of Europe (CoE), Convention on Cybercrime, 2001.
[15] Council of Europe (CoE), Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2003.
[16] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2017, p.18
[17] McGuire, M., and S. Dowling, *Cyber crime: A review of the evidence*, Chapter 2: Cyber-enabled crimes – fraud and theft, Home Office, 2013, p.4.

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

Figure 4 – Coverage of cyber-dependent crimes in criminal codes

CAT.	OFFENCE	FR	DE	IT	NL	RO	ES	SE
1	Illegal access	X	X	X	X	X	X	X
1	Illegal interception	X	X	X	X	X	X	X
1	Data interference	X	X	X	X	X	X	X
1	System interference	X	X	X	X	X	X	X
1	Misuse of devices	X		X	X	X	X	X

Figure 5 – Coverage of cyber-enabled crimes in criminal codes

CAT.	OFFENCE	FR	DE	IT	NL	RO	ES	SE
2	Computer-related forgery	X	X		X	X	X	
2	Computer-related fraud	X	X	X	X	X	X	X
3	Offences related to child sexual abuse material (CSAM)[18]	X	X	X	X	X	X	X
4	Offences related to infringements of copyright and related rights			X				
5	Dissemination of racist and xenophobic material through computer systems				X	X		
5	Racist or xenophobic motivated threats	X		X			X	X
5	Racist or xenophobic motivated insult	X	X	X	X	X	X	X
5	Denial, gross minimisation, approval or justification of	X	X	X		X	X	

[18] The term 'Child Pornography' is replaced here and in Figure 7 with Child Sexual Abuse Material (CSAM) as per Luxemburg Guidelines: "The term "child sexual abuse material" is increasingly being used to replace the term "child pornography". This switch of terminology is based on the argument that sexualised material that depicts of otherwise represents children is indeed a representation, and a form, of child sexual abuse and should not be described as "pornography" (p. 38).

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

	genocide or crimes against humanity							
5	Aiding and abetting	X	X	X	X	X	X	X

4.2.1 Gap analysis of UK (England & Wales) cybercrime criminal law

The UK legal system differs from European systems in that there is no criminal code, rather criminal law is rooted in a common law system. However, common law may be replaced or superseded by legislation (for example Acts of Parliament or statutes). Another primary source of law in the UK, aside from legislation, is case law and secondary sources concern legal opinion (including textbooks, commentary, opinions and decision of legal experts of the courts), all of which may be considered during a court proceeding. The UK has three distinct legal systems: England and Wales, Scotland and Northern Ireland. Many modern laws are applicable across all three jurisdictions but there also can be key differences[19]. In summary, the UK legal system is inherently complex.

The Crown Prosecution Service (CPS) prosecutes criminal cases investigated by authorised bodies in England and Wales. The CPS compiles guidance on applicable criminal law in relation to cybercrime, that is the most up to date record of changes to law and legal practice in this UK jurisdiction. Due to the differences in the England and Wales legal system to the rest on the jurisdictions in scope of this review, the legal review is considered separately here and summarises the guidance provided by the CPS in relation to the Budapest Convention's cybercrime framework, supplemented by The Criminal Law Reform Now Network (CLRNN)'s report evaluating the Computer Misuse Act 1990 ('CMA')[20].

Figure 6 – Coverage of cyber-dependent crimes in UK legislation (England and Wales)

CAT.	OFFENCE	UK (E&W)	RELEVANT CRIMINAL LAW OR LEGISLATION
1	Illegal access	X	Section 1 and Section 2 Computer Misuse Act 1990 ('CMA')
1	Illegal interception	X[21]	Computer Misuse Act 1990 ('CMA'), Investigatory Powers Act 2016
1	Data interference	X	Section 3 and Section 3ZA Computer Misuse Act 1990 ('CMA')

[19] Incorporated Council of Law Reporting, "The English legal system". https://www.iclr.co.uk/knowledge/topics/the-english-legal-system/
[20] McKay, S., et al, Reforming the Computer Misuse Act 1990, Criminal Law Reform Now Network (CLRNN), 2020.
[21] McKay, S., et al, *Reforming the Computer Misuse Act 1990*, Criminal Law Reform Now Network (CLRNN), 2020, Table 1 Correspondence between the CMA, the Convention on Cybercrime and the 2013/40/EU Directive.

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

1	System interference	**X**	Section 3 and Section 3ZA Computer Misuse Act 1990 ('CMA')
1	Misuse of devices	**X**	Section 3A Computer Misuse Act 1990 ('CMA')

Figure 7 – Coverage of cyber-enabled crimes in UK legislation (England and Wales)

CAT.	OFFENCE	UK (E&W)	RELEVANT CRIMINAL LAW OR LEGISLATION
2	Computer-related forgery	**X**	Sections 1-5 Forgery and Counterfeiting Act 1981; Sections 4-6 Identity Document Act 2010
2	Computer-related fraud	**X**	Section 2-3 of CMA; Sections 1–2 Fraud Act 2006; Section 6 Fraud Act 2006; Theft Act 1968 and Theft Act 1978; Section 1 Criminal Law Act 1977; Part 7 POCA; Forgery and Counterfeiting Act 1981; Section 170 DPA
3	Offences related to child sexual abuse material (CSAM)[18]	**X**	Section 1 of the Protection of Children Act 1978 ('PCA') is appropriate in the majority of cases as wording 'making' is inclusive of opening, downloading or viewing CSAM. Whereas Section 160 of the Criminal Justice Act 1988 ('CJA') refers only to 'possession' and is not inclusive of the above list.
4	Offences related to infringements of copyright and related rights	**X**	Sections 107, 198, 296ZB and 297; Copyright Designs and Patents Act 1988; Section 92 Trade Marks Act 1994; Sections 9-14 Video Recordings Act 2010; Fraud Act 2006; Part 7 POCA; Video Recording Act 2010
5	Dissemination of racist and xenophobic material through computer systems	**X**	Online communications may involve a range of offences against persons, public justice, sexual, public order offenses or communications offenses, which have existing statues prosecutors may consider. Sections 145 and 146 of the Criminal Justice Act 2003 provide for an increased
5	Racist or xenophobic motivated threats	**X**	

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

5	Racist or xenophobic motivated insult	**X**	sentence for hate crime offending, and these provisions apply to communication offenses also. There are a number of domestic and European case law that relate to hate crime online: e.g. DPP v Collins; Kuhnen v Germany 56 RR 205; Lehideux and Isorni v France [2000] 30 EHRR 665; and M'Bala M'Bala v France (application no. 25239/13)[22]
5	Denial, gross minimisation, approval or justification of genocide or crimes against humanity	**X**	
5	Aiding and abetting	**X**	Computer Misuse Act 1990 ('CMA'); Section 1 Criminal Attempts Act 1981; Section 8 Accessories and Abettors Act 1861[23]

4.2.2 Gap analysis conclusions

The data captured in Figures 4 and 6 highlights that there is good overall coverage of cyber-dependent crimes in criminal code and criminal law documentation across the target countries. Of the five cybercrimes in category 1 (offences against the confidentiality, integrity and availability of computer data and systems), it appears only the German Criminal Code does not include any provisions for the misuse of devices.

In terms of the cyber-enabled crimes captured in Figures 5 and 7, coverage of offences is more inconsistent when compared to cyber-dependent crimes. For these cybercrimes, technology is not the sole vector through which the crime can be committed. For instance, racist and xenophobic threats and insults can be perpetrated offline as well as online. It appears that when this is the case, reference to the 'cyber' element of the offence in criminal code documentation diminishes.

Notably, criminal law in England and Wales provides complete coverage of all 14 cybercrimes listed within the Budapest Convention's classification system. However, it is important to note that this framework is not a complete and exhaustive list of all cybercrime offenses in the UK. Key omissions include offenses pertaining to dark markets and organised cybercrime, offenses relating to online violence (e.g., cyber bullying and harassment), offenses relating to online sexual violence (e.g., coercion and control, cyberstalking, and disclosure of private images without consent) and offenses relating to child sexual exploitation and abuse (e.g., online grooming).

[22] The Crown Prosecution Service (CPS), "Social Media – Guidelines on prosecuting cases involving communications sent via social media", 2018. https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media

[23] McKay, S., et al, *Reforming the Computer Misuse Act 1990*, Criminal Law Reform Now Network (CLRNN), 2020, Table 1 Correspondence between the CMA, the Convention on Cybercrime and the 2013/40/EU Directive (p. 33)

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

4.3 Recommendations to increase the effectiveness of legislation

Five recommendations are proposed by WP5 partners to improve the effectiveness of legislation as a tool in combatting cybercrime.

1 Perform regular evidence-based reforms

It was commonly observed that legislation tends to be amended relatively infrequently even when research reports call for revisions. In addition to the Computer Misuse Act being outdated, the Budapest Convention on Cybercrime has also not seen regular updates to keep it in line with the constantly evolving nature of cybercrime. This widely recognised instrument was formally introduced in 2001, and the last update was made in 2003 when the additional protocol of acts of a racist and xenophobic nature committed through computer systems was introduced. WP5 partners advise that legislation and other legal instruments should be reviewed on an ongoing basis with a view to implementing evidence-based revisions as and when required.

2 Use technology neutral terminology when writing legislation

There is a clear and growing gap between the fast-paced nature of cyberspace, the continuously evolving capabilities of cybercriminals, and the ability of legislation to keep up. Outlining specific technologies used to perform crime in legislative documents, such as the criminal codes reviewed and analysed, can lead to their becoming quickly outdated. This is currently a common feature in legislative documents as cybercrimes are often categorised through the different types of technology involved. WP5 partners propose that legislation should be written in technology-neutral terminology. That is, legislation should not specify the technology used to perform the crime but instead define the underlying act that is illegal.

3 Maintain a web-based repository of cybercrime offences

Attempts have been made to alleviate the lack of accessibility of cybercrime offences enacted across several different legislative documents at both a national and European level. Examples of this includes the cybercrime prosecution guidance provided by the UK's Crown Prosecution Service[24] and the overview of domestic legislation on cyber-violence on the Council of Europe portal[25]. However, in the case of the latter, the database is not updated limiting its future applicability and relevance. WP5 partners recommend that ownership of the database be clearly defined to indicate who is responsible for updating it when required.

4 Encourage victims of cybercrime to explore civil law as well as criminal law

The conviction rate for cybercrime offences tends to be low compared with other criminal investigations. For example, only about two per cent of Criminal Misuse Act offences result

[24] Crown Prosecution Service, "Cybercrime – prosecution guidance", September 2019. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance
[25] Council of Europe, "Domestic Legislation on Cyberviolence". https://www.coe.int/en/web/cybercrime/domestic-legislation

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

in a police investigation; and only one per cent result in a prosecution or conviction.[26] These low figures may deter victims of cybercrime from reporting offences further contributing to the separate issue of significant underreporting. WP5 partners believe that victims of cybercrime should explore other avenues of legal remedy as well as criminal law to try and obtain more adequate outcomes. This is because civil law aims to compensate persons who have been wronged instead of prosecuting those who have done wrong, which is the case in criminal law.

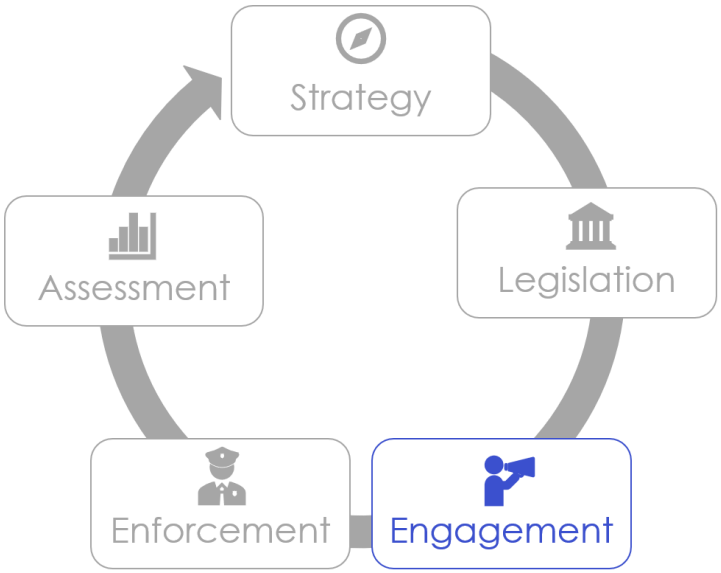
5 Provide guidance for non-culpable actors

Attempts should be made to reduce the criminalisation of non-culpable actors to enable genuine activity in cyberspace to be conducted. Through engagement activities, it may be beneficial to disseminate materials that provide guidance for these individuals or groups, such as, the creation of a checklist of do's and don'ts for penetration testers or similar actors. Another example could be the development of a potentially gamified sandbox bug bounty platform for relevant stakeholders in Europe, similar to those employed by private organisations such as Microsoft[27]. This would be beneficial for multiple reasons: non-culpable actors will be able to assess their capabilities, systems, tools and technology will receive rigorous testing, the gamification aspect may encourage young people and the platform will provide an increased amount of relevant data for the platform providers to analyse and disseminate accordingly.

[26] McKay, S., et al, *Reforming the Computer Misuse Act 1990*, Criminal Law Reform Now Network (CLRNN), 2020.
[27] Microsoft, "Microsoft Bug Bounty Program". https://www.microsoft.com/en-us/msrc/bounty

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

5. Engagement



Engagement refers to activities that support cybercrime legislation and policy by creating awareness, increasing reach and educating society. Engagement activities take many different forms including training, initiatives, campaigns and programmes. These activities are essential for a variety of reasons including making potential victims aware of cyber threats, advising them on how to avert potential harm, publicising ways to mitigate cyber risk, educating potential perpetrators on the consequences of committing cybercrime offences, and informing young people that the cyber skills they possess can lead to a career in cybersecurity.

A notable focus of CC-DRIVER is to better understand young people and the factors driving them into cybercrime. Due to young people featuring as one of the most common target demographics of engagement activities, reviewing and analysing this element helped WP5 partners to address this specific focus of the project. This segment of the research explored the methods used and evaluated the effectiveness of engagement activities.

5.1 Common observations across engagement activities

Five common observations summarise the review and analysis of engagement activities across the eight in-scope countries.

1 Young people are the primary audience for engagement activities

There are various demographics in society that can be deemed to be higher risk of falling victim to cybercrime or becoming a cybercriminal. The research showed that young people are the most targeted demographic. This is a critically important part of society to target because it is easier to influence the behaviour of young people in terms of good cyber hygiene compared to the adult population. Also, cybercriminals tend to be younger compared to the perpetrators of traditional crime, making them a key target for engagement

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

activities. In 2015, it was reported that the average age of cybercrime suspects in the UK was 17.[28] With more modern tools such as cybercrime-as-a-service (CaaS) reducing the barrier of entry into cybercrime, even younger individuals may be committing these offences.

2 Online platforms are the most common dissemination methods for engagement activities

The objective for most engagement activities is to reach as many people as possible. Since young people spend a significant amount of time on the Internet and social media platforms, it is understandable that online platforms are the most common dissemination methods used across the eight countries researched. Platforms such as Facebook and YouTube allow content to be accessed and shared relatively seamlessly making them an obvious option to disseminate engagement activities. However, careful consideration should be given in deciding which platforms to use. This is because certain companies, for example, those considered 'Big Tech', have been questioned concerning their data privacy practices.[29]

3 Engagement activities tend to be free or provided at minimal cost for participants

Whether subsidised by the public sector or an initiative by the private sector, engagement activities are typically low cost if not free for those who wish to participate. This is critical to the objective of increasing reach for cybersecurity and cybercrime issues as it ensures a low barrier to entry, especially for individuals in high-risk demographics such as those from low-income households.

4 Engagement activities are conducted at a local, national and international level

In a similar way to other elements in the framework, engagement activities are also conducted at various levels:

1. Local activities (e.g., Help to Prevent in Valencia, Spain)
2. National activities (e.g., Cyber Youth Connection in France)
3. European activities (e.g., the European Cyber Security Challenge)
4. International activities (e.g., Interpol's #Washyourcyberhands campaign)

Conducting engagement activities at these different levels enables varying levels of scalability with which to promote issues relating to cybersecurity and cybercrime. While it is true that some cybersecurity and cybercrime issues are unique to a certain country or countries due to underlying factors, such as demographic, there remain overarching issues that are shared across the world where international activities can prove effective.

[28] Vincent, J., "Average age of cyber crime suspects in the UK falls to 17", The Verge, 2015. https://www.theverge.com/2015/12/8/9870534/cyber-crime-average-age-uk-17
[29] Atkins. B., "Big Tech, Data Privacy and the Board's Role", *Forbes*, 2020. https://www.forbes.com/sites/betsyatkins/2020/11/12/big-tech-data-privacy-and-the-boards-role/?sh=668536995bba

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

5 Academic institutions face barriers when disseminating articles and reports

There are currently barriers for academic institutions when trying to promote their research surrounding cybersecurity and cybercrime. Learning from thought-leading academics is key to developing cybersecurity capabilities and reducing cybercrime in the long term. Examples of these barriers are the reliance on funding and research grants as well as the requirement for academic institutions to have an ethical approval board in order to publish articles, which many do not have.

5.2 Differences across engagement activities

Due to each country having its own unique demographic, engagement activities naturally differed across the eight-country scope. The review and analysis highlighted three main differences:

1 Rehabilitating cybercriminals is not a priority for engagement activities

Engagement activities can be classified by the demographics they target. One proposed categorisation system[30] differentiates between:

1. Those that target the general population (primary prevention)
2. Those that target the higher risk demographics (secondary prevention)
3. Those who have already broken the law (tertiary prevention)

The information captured in Figure 6 clearly shows that all countries within the research scope carry out engagement activities aimed at reaching the entire population (primary prevention) as well as specific high-risk demographics (secondary prevention). However, only the Netherlands and United Kingdom were observed by WP5 partners to carry out engagement activities aimed at those who have already broken the law (tertiary prevention). Hack_Right[31] in the Netherlands and the National Crime Agency's (NCA) 'rehab camp'[32] in the UK work with young cybercriminals to help them understand that their skills can be applied to careers in cybersecurity. It appears that the other six surveyed countries are neglecting, to some extent, a group who is at high risk of reoffending.

[30] Brantingham, P., and Faust, F., *A Conceptual Model of Crime Prevention*, Crime and Delinquency, 1976.
[31] Stupp, C., "Dutch Program Aims to Deter Young Hackers Before They Commit Crimes", *The Wall Street Journal*, 2020. https://www.wsj.com/articles/dutch-program-aims-to-deter-young-hackers-before-they-commit-crimes-11608546602
[32] Ward, M., "Rehab camp aims to put young cyber-crooks on the right track", BBC, 2017. https://www.bbc.co.uk/news/technology-40629887

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

Figure 6 – Coverage of preventative engagement activities

	FR	DE	IT	NL	RO	ES	SE	UK
Primary prevention	X	X	X	X	X	X	X	X
Secondary prevention	X	X	X	X	X	X	X	X
Tertiary prevention				X				X

2 Activities that not only upskill individuals but also provide job opportunities

Almost all the engagement activities providing cybersecurity training observed in the review did so without providing post-completion job opportunities. While skills-based training to enable a career in cybersecurity and countering cybercrime was often provided, there were few instances where tangible job prospects were available. Sweden, however, does provide this through their National Military Service, an initiative where talented teenagers are selected for training in tackling hackers.[33] While other engagement activities attempt to reach as many people as possible, this instance is a selective model involving a highly competitive recruitment process. It is important that this type of engagement activity exists, and all focus is not given to the mass population.

3 The topics covered through engagement activities are wide-ranging depending on the country, target audience and other factors

While there are overlaps in the topics addressed by engagement activities, there was no single engagement topic that was observed across all eight of the countries under review. Examples of engagement activities observed across most but not all countries include:

- Using the Internet
- Cyber bullying, hate speech and harassment
- Coding and software development
- Ethical hacking.

The maturity of a country's population and its appetite for progress in terms of cybersecurity capabilities are potential reasons for selecting which topics to prioritise through engagement activities.

[33] The Local, "Sweden to train 'cyber soldiers' during military service", 2019. https://www.thelocal.se/20190116/sweden-to-train-cyber-soldiers-during-military-service/

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

5.3 Recommendations to improve the effectiveness of Engagement activities

Partners propose seven recommendations that aim to improve the effectiveness of engagement activities.

1 Consider all demographics, not only young people

While young people are a justifiable primary audience of engagement activities, there are several other demographics that must receive attention regarding cybersecurity and cybercrime. Other groups who may warrant increased focus may include those with learning difficulties, mental health conditions, those from under-privileged backgrounds and the elderly.

2 Employ gamification techniques where appropriate

There are now more than 2.5 billion active gamers around the world, which is one billion more than just five years ago.[34] While gaming online can present its own challenges in terms of security and behaviour in cyberspace, the number of gamers is increasing rapidly. Engagement activities should leverage aspects of gamification that are proven to be effective. An example of this stems from another project in the Horizon 2020 Programme, RAYUELA, which is developing a 'fun way to fight cybercrime' through a serious gaming environment demonstrating progress in leveraging this trend.

However, there are notable risks to consider when employing gamification techniques. 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, who is employing gamification techniques is an important factor to consider because organisations such as LEAs, for example, may be scrutinised for gamifying activities that are meant to address serious issues relating to crime.

4 Consider dissemination methods outside of cyberspace

Although the Internet presents a great resource for all those who can access it, there will be a proportion of people who prefer to consume information offline. There are various reasons as to why this might be the case, for instance personal preference, the digital divide and parents restricting their children's access to online material when still at a young age. While these groups are limited in their time spent in cyberspace, they will nonetheless be required to use it at some point in their lives. Thus, it is crucial to have dissemination methods to reach these groups. Examples include magazines, books, seminars via school and community networks, and other analogue formats.

[34] Narula, H., "A billion new players are set to transform the gaming industry", WIRED, 2019. https://www.wired.co.uk/article/worldwide-gamers-billion-players

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

5 Introduce support programmes for victims of cybercrime

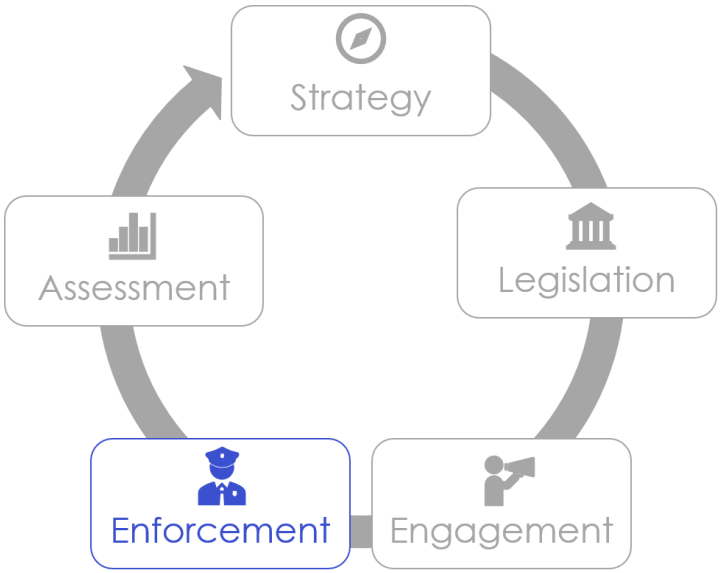
Most engagement activities observed are preventative in nature but WP5 partners argue that engagement activities must not only protect those at risk of falling victim to cybercrime and rehabilitate those who are first-time offenders, but also support those who have already fallen victim to cybercrime. Falling victim to any form of crime can leave that individual feeling isolated, making support programmes an essential part to reassuring victims. It is important for victims of cybercrime to understand the complexities of the issue. Victim support programmes should increase awareness and confidence through a two-way relationship where victims are able learn from their experiences, connect with other victims and share information to help others in future.

6 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 regarding cybersecurity and cybercrime. However, to many young people, police officers will not be relatable figures and therefore engagement activities delivered via police may not achieve the most effective results. WP5 partners recommend disseminating important messages regarding cybersecurity and cybercrime 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.

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

6. Enforcement



The enforcement element concerns LEAs' efforts to police cyberspace and protect citizens online. For this element of our framework, the review process relied on input from the LEA partners within the CC-DRIVER consortium and special interest group meetings conducted with industry experts. Three LEAs were involved throughout the research and analysis of the enforcement landscape across Europe: the Bavarian police academy, Policia Judiciaria and the Valencia Local Police. These organisations were able to provide the research with on-the-ground insights and recommendations.

6.1 Common observations in the enforcement landscape

WP5 partners identified three main observations across the enforcement landscape in the eight countries under review.

1 LEAs are restricted by both a lack of resourcing and by bureaucracy

This research confirmed that LEAs and the public sector experience a lack of resource and funding in terms of budget, people and technology in the eight countries under review. LEAs in the consortium also specified that they are restricted by bureaucracy limiting their ability to tackle cybercrime effectively. Excessive rules, standards and procedures reduce efficiency when trying to combat the fast-paced nature of cybercrime. Comparatively, cybercriminals and organised criminal groups do not carry these same resource and bureaucratic burdens. In today's climate, even relatively inexperienced and lesser-skilled cybercriminals can conduct illicit activity through increasingly available vectors, such as cybercrime-as-a-service obtainable on the dark web. Even with the taking down of underground markets, such as

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

Alphabay and Hansa, criminals have shifted to forums where cybercrime-as-a-service offerings have remained stable over time.[35]

2 Many cybercrimes go unreported each year

Only a fraction of fraud and cybercrime offences are reported to authorities. This is a common theme across our eight-country scope. As an example, in the UK, a review of Office of National Statistics (ONS) data shows the low number of computer misuse offences reported by individuals. During the 2020 lockdown period in England and Wales, an estimated 1.7 million computer misuse offences were committed with only 29,094 being reporting to authorities, representing less than two per cent.[36] This trend can be observed among organisational victims of cybercrime as well. While for individuals, the reporting process for cybercrimes is not as clearly understood compared with the reporting of traditional crimes, organisations often prefer to withhold information regarding cyberattacks due to fears of the potential adverse effect on their stock prices and the associated reputational damage.

3 The proliferation of cryptocurrencies has facilitated cybercrime

Recent years have seen the rise and proliferation of cryptocurrencies, which have enabled cybercriminals to receive payment and store funds in virtual wallets. It has rapidly become the preferred means of payment and exchange for cybercrimes such as ransomware, cybercrime-as-a-service and other dark web activities. In May 2021, the Colonial Pipeline ransomware attack in the United States saw nearly $5 million paid to hackers in Bitcoin demonstrating the use of the currency for illicit activity.[37] Notably, however, FBI investigators were able to recover $2.3 million using a private key, bringing into question the supposed untraceable nature of cryptocurrency wallets.

The use of cryptocurrencies is beginning to be restricted to some extent in certain countries that proscribe its ability to facilitate cybercrime. For example, in China, a ban was introduced on financial institutions providing services relating to cryptocurrencies.[38] More recently in Europe, the cryptocurrency exchange Binance has faced scrutiny by Germany and been censured by Italy and the United Kingdom over issues including securities rules and

[35] Akyazi, U., M. Eeten, C. Gañán, Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum, 2021.
[36] Hall, R., "ONS Cram data: Cybercrimes are going unreported", DWF Group, 2021. https://dwfgroup.com/en/news-and-insights/press-releases/2021/2/cybercrimes-are-going-unreported
[37] Bing, C., J. Menn and S. Lynch, "U.S. seizes $2.3 mln in bitcoin paid to Colonial Pipeline hackers", Reuters, 2021. https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/
[38] Reuters, "China bans financial, payment institutions from cryptocurrency business", 2021. https://www.reuters.com/technology/chinese-financial-payment-bodies-barred-cryptocurrency-business-2021-05-18/

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

customer protection.[39] The EU is currently in the process of negotiating a new regulation for crypto assets[40].

6.2 Differences observed in the enforcement landscape

Our research observed several differences in the processes, tools and techniques used by LEAs in the eight countries under review and analysis. It should be noted that the legislative landscapes within which the LEAs operate also differ markedly. Still, our research identified two main differences between the countries that may limit the effectiveness of the enforcement of cybercrime.

1 **The relationships with LEAs in other parts of the world compared with those in Europe**

The level of collaboration between LEAs vary internationally. Within Europe, Europol has furthered collaborative investigations regarding cybercrime. For instance, in 2020 Europol coordinated the arrest of 20 individuals laundering tens of millions of Euros on behalf of cybercriminals.[41] The investigation involved law enforcement officers from five of the eight countries reviewed in this report (Spain, United Kingdom, Italy, Germany and Sweden) along with others. While international organisations such as INTERPOL exist, LEA partners in the WP5 consortium expressed difficulties collaborating with LEAs and other organisations outside of Europe, namely Asian, African and South American countries.

2 **The technology and tools used by LEAs vary from country to country**

LEAs each operate leveraging different technology and tools. This was one of the first differences highlighted when consulting our LEA partners. Various tools are used to conduct law enforcement investigations including digital forensics and data analysis, among other tools. This inconsistency can limit the ability for LEAs to exchange like-for-like output data from these tools, which would be advantageous in terms of building a more robust international data set for cybercrime. Harmonising the technology and tools used by LEAs would benefit current and future investigations relating to cybercrime and facilitate further education in this domain.

[39] Samson, A., "Binance crackdown widens in Europe and Hong Kong", *The Financial Times*, 2021. https://www.ft.com/content/1f4ff647-088c-4ed2-b637-e675b9886ace

[40] Cengiz, F., "What the EU's new MiCA regulation could mean for cryptocurrencies", London School of Economics and Political Science, 2021. https://blogs.lse.ac.uk/europpblog/2021/07/05/what-the-eus-new-mica-regulation-could-mean-for-cryptocurrencies/

[41] Europol, "20 Arrests in QQAAZZ multi-million money laundering case", October 2020. https://www.europol.europa.eu/newsroom/news/20-arrests-in-qqaazz-multi-million-money-laundering-case

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

6.3 Recommendations to improve the effectiveness of enforcement

WP5 partners have proposed four recommendations aimed at improving the effectiveness of the law enforcement of cybercrime.

1 Provide incentives to encourage the reporting of cybercrime

Law enforcement, along with other stakeholders in the anti-cybercrime ecosystem, should make efforts to reduce the high number of cybercrimes going unreported each year. While monetary incentives would not be appropriate, WP5 partners recommend:

- making victims of cybercrime aware of the scale of cybercrime and the importance of reporting it,
- demonstrating how their contribution benefits the whole of society in the fight against cybercrime, and
- providing an opportunity for the victim to propose recommendations and be a part of the solution.

Ultimately, combating cybercrime is not just the sole responsibility of law enforcement agencies. Other stakeholders such as legislators and those conducting engagement activities also need to play key, coordinated roles in anti-cybercrime initiatives.

2 Train increased numbers of police staff in cyber security and cybercrime

Crimes in the modern world increasingly have a cyber element. Regardless of their area of specialism, police officers from all backgrounds should undertake cybersecurity training. Using the private sector as an example, if most employees are required to complete basic cybersecurity training regardless of the business function they work in, it seems appropriate for officers in the police force to do the same. The UK is an example of a country under review dedicating increased attention to this space in recent years. In 2018, the UK police partnered with Cisco to train 120,000 police officers in cybersecurity related topics.[42]

3 Report meaningful data about cybercrime to budget holders

The metrics used to report cybercrime are often ambiguous and thus cannot enable effective decision-making. This observation holds across both private and public sector organisations. Reporting on the risk of cybercrime in technical terms to non-technical stakeholders will provide little value and may even cause more harm than good. Without knowing the extent of the threat that cybercrime poses, LEAs and public sector organisations will continue to have trouble obtaining budget allocation required to effectively tackle cybercrime. WP5 partners recommend reporting risk associated with cybercrime in financial

[42] Cisco, "Cisco joins forces with the Police to help make the UK the safest place in the world to be online", November 2018. https://news-blogs.cisco.com/emear/2018/11/29/cisco-joins-forces-with-the-police-to-help-make-the-uk-the-safest-place-in-the-world-to-be-online/

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

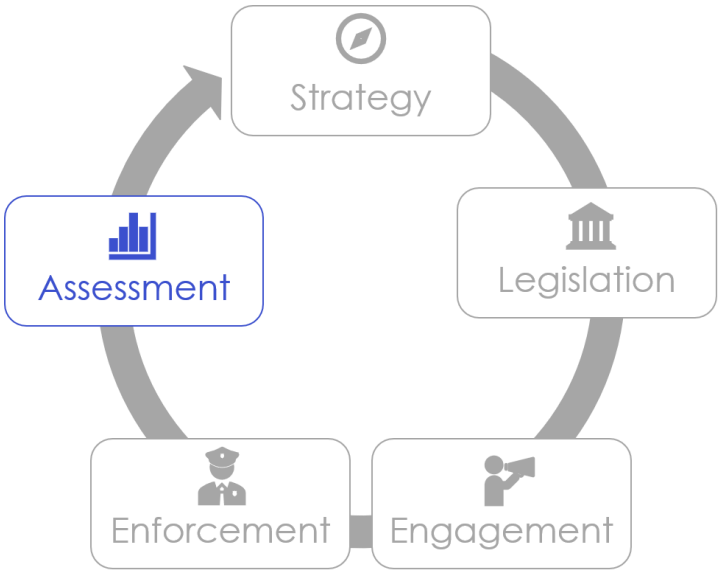
terms, where appropriate, allowing people from all backgrounds to accurately interpret the information and make evidence-based decisions.

4 Focus on actions to address root causes, not just immediate incidents

Responsive action against cybercrime should not be a knee-jerk reaction to high-profile incidents that receive significant media coverage, but instead should be the result of timely evidence-based reforms. While events such as the SolarWinds and Colonial Pipeline attacks generate awareness around the importance of cybersecurity, fixing the specific vulnerabilities exploited in these cases will do little to prevent future attacks. WP5 partners recommend dedicating equal focus to addressing the underlying root causes of cybercrime for greater longer-term effectiveness in reducing cybercrime, for example, investing further in the education and training of employees from all backgrounds.

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

7. Assessment



The fifth and final element of completing a pragmatic approach to tackling cybercrime is assessment. This concerns the collection, management, analysis and application of timely, accurate and reliable data relating to cybercrime.

WP5 partners collected data on a variety of cybercrime metrics across the eight countries between the years 2017 and 2019, the most recent data available. Primary data was obtained from the national bodies responsible for publishing statistics. However, for certain countries under review, primary data was not easily accessible and so in these countries WP5 partners instead obtained data from secondary sources such as academia, research, and industry. Once the data set was compiled, they conducted descriptive analysis to summarise the data and highlight any trends and patterns visible.

Table 5 – Primary cybercrime data sources

COUNTRY	PRIMARY DATA SOURCE
France	-
Germany	The Federal Criminal Police Office's Cybercrime Assessment and Police Crime Statistics
Italy	Italian National Institute of Statistics
Netherlands	Central Bureau for Statistics (CBS)
Romania	-

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

Spain	Statistical System of Crime (SEC)
Sweden	Swedish National Council for Crime Prevention
United Kingdom	Office of National Statistics (ONS)

7.1 Common observations across the dataset

The review and descriptive analysis of the dataset enabled WP5 partners to make two observations common across all eight countries.

1 Cybercrime is increasing

After reviewing and analysing the data set collected, WP5 partners substantiated conclusions from previous work done in this space. That is, cybercrime in general is increasing across all eight countries. However, it is difficult to place a figure on the exact extent of this increase. This is due to a variety of reasons but most notably:

- the range of metrics different countries collect to evaluate the current state of cybersecurity and cybercrime; and
- the well-documented underreporting of cybercrime offences by both individuals and organisations.

Examples of studies supporting this conclusion drawn by WP5 partners stated that, it is nearly impossible to estimate the amount of cybercrime that occurs in most nations around the world because of a lack of standardised legal definitions for these offences and few valid, reliable, official statistics.[43] Evidence demonstrates, however, that cybercrime rates are increasing as the rates for many forms of traditional street crimes continue to decrease.[44] The drop-off in traditional crime in highly industrialised Western countries, including Western Europe, may be attributed to this rise of online and hybrid offences.[45]

2 COVID-19 resulted in an increase in cybercrime offences

The global pandemic resulted in a notable increase in cybercrime. This can be attributed to a variety of reasons, including the shift from offices to work-from-home (WFH) environments and negligence of cyber hygiene due to health and financial stresses associated with the pandemic. Europol highlighted several cybercrimes that have seen a sharp upward trend throughout the pandemic, in particular ransomware, child sexual abuse material and

[43] Holt, T., and A. Bossler, Cybercrime in Progress: Theory and prevention of technology-enabled offenses, Routledge, 2017.
[44] Gottschalk, P., and M. Tcherni-Buzzeo, Reasons for Gaps in Crime Reporting: The Case of White-Collar Criminals Investigated by Private Fraud Examiners in Norway, Deviant Behavior, Vol. 38, Issue 3, 2017.
[45] Caneppele, S., and M. Aebi, Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes, *Policing*, Vol 13, No. 1, 2017, pp. 66–79.

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

payment fraud in the form of SIM swapping.[46] Social engineering and phishing were also highlighted as vectors that enable other forms of cybercrime.

7.2 Differences observed across the dataset

The review and descriptive analysis of the dataset also allowed WP5 partners to identify three key differences in the way data is collected, managed and analysed in the eight countries under review.

1 **Countries collect a variety of metrics making data analysis difficult**

Each country collects and reports slightly different metrics for cybercrime data. Differences in the way data are collected and reported can make the comparison and aggregation of data challenging, and potentially misleading. To illustrate an example of this from our dataset, Germany reports cybercrime on the number of incidents per year, while Spain reports on the number of incidents managed by the National Cyber Security Institute. While both may be accurate and the nature of the data collected is similar, there are differences that could prove misleading should one attempt to directly compare or aggregate these two datasets.

2 **The accessibility of primary cybercrime data in different European countries**

For the majority of the eight in-scope countries, it was relatively easy to obtain primary data relating to cybercrime from the body responsible for publishing national statistics. However, for certain in-scope countries primary data were much less accessible, namely France and Romania, respectively. For these two countries, secondary data was obtained as a replacement. The inaccessibility of data in these countries restricted WP5 partners from conducting detailed comparative analysis across the eight-country scope and aggregating the data collected to make detailed overarching inferences.

3 **The prominent vectors of cybercrime and most common victims of cybercrime in each country**

While the overarching direction of cybercrime is seen to be increasing, there are notable differences in terms of specific aspects of the dataset. When looking at the different types of vectors used to perpetrate cybercrime, each country is different and experiences each vector to varying extents. For example, in 2019, computer fraud was the most prominent vector of cybercrime in Germany, while in Sweden it was the unlawful access to, or use of, computer systems. A similar discrepancy can be seen when looking at the age groups of cybercrime victims across countries. In 2018, in the Netherlands the most common age group falling victim to cybercrime was 18-24 year olds, while in Spain in the same year it was 26-40 year olds. These examples demonstrate how each country's demographic and varying levels of cybersecurity capabilities can contribute to unique results. However, these

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

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

differences may be simply due to the infancy of cybercrime statistics, which will prove more consistent over time.

7.3 Recommendations to improve the collection, management, and analysis of cybercrime data

WP5 partners propose five recommendations to improve the collection, management and analysis of cybercrime data.

1 **Harmonise metrics to measure cybercrime at a European/international level to facilitate comparisons**

To overcome the challenges of comparing and aggregating a variety of metrics relating to cybercrime, WP5 partners have proposed a selection of metrics to collect for each of the elements of the pragmatic approach to tackling cybercrime framework. 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.

Figure 7 – Recommended metrics to collect on cybersecurity and cybercrime

ELEMENT	RECOMMENDED METRICS
Strategy	• Success rate of achieving strategic objectives (within agreed timeframes) • The types of cybercrime perpetrated • The types of vulnerability exploited
Legislation	• Conviction rate for cybercrime offences • Average amount of monetary fines handed • Average sentence length for committing cybercrime offences
Engagement	Crime rates based on: • Age • Gender • Household income • Country/region • Sector/industry Victimisation rates based on: • Age • Gender • Household income • Country/region
Enforcement	• Percentage of reported incidents assessed or actioned • Percentage of cybercriminals who re-offend • Monetary amount of cybercriminal profit prevented • Number of requests for international cooperation

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

2 Ensure that cybercrime datasets are more accessible to all relevant stakeholders

For certain countries under review, WP5 partners found the availability of primary data relating to cybercrime to be limited. Learning from data is essential to bolstering cybersecurity capabilities and tackling cybercrime for academics, researchers, policymakers, and others. In a similar way to the repository proposed by WP5 partners for cybercrime legislation, a central repository should be created for publicly available cybercrime data in European countries. The data stored in the repository should also be conveyed in understandable terms for all types of stakeholders. Such a repository will need updating on a regular basis to keep up with the ongoing collection of data. WP5 partners believe that Eurostat will be an appropriate body to coordinate national statistics institutes due to its established reputation of publishing high quality European-wide statistics.

3 Inferences from analysis should consider the limitations of data collection

Datasets relating to cybercrime, including the one compiled by WP5 partners, have several limitations. Firstly, any inferences should acknowledge that there is estimated to be widespread underreporting of cybercrimes by both individuals and organisations. Thus, available data sets likely represent some distortion with regard to the actual state of affairs. Secondly, the lack of consistent definitions internationally means that the classification of cybercrimes is likely to vary from country to country. For instance, what is classed as an illegal access offence in one country may not be classified in the same way in another. For example, actions violating social norms, for example cyberbullying, are sometimes classed as a cybercrime and in other cases are not. This also challenges the integrity of multi-country data sets.

4 Leverage information-sharing mechanisms to verify cybercrime data and promote collaboration

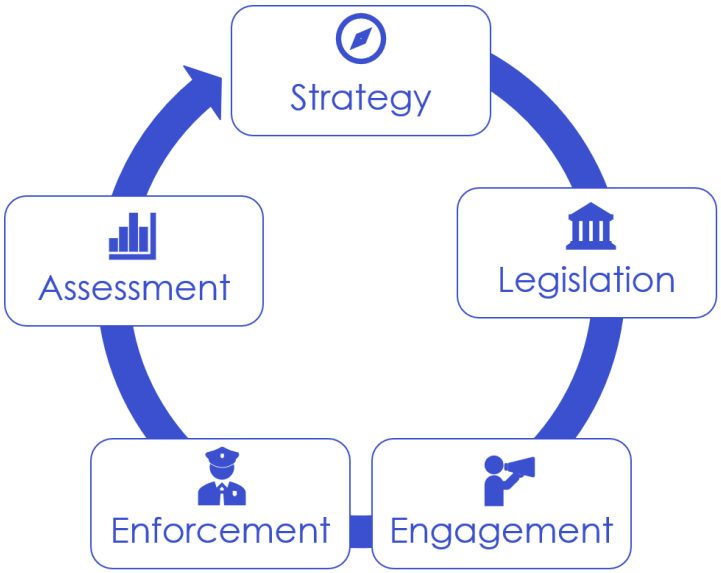
One of the common themes realised throughout this review is the need for improvement and innovation regarding the exchange of information. In the case of assessment, all the relevant stakeholders, such as government, LEAs, academics, organisations, and others should develop secure mechanisms in order to transfer data so that domestic and international parties in both the private and the public sector can build more robust cybercrime datasets and each learn from the data collected and analysed by each other. WP5 partners recommend the creation of rapid response mechanisms as well as secure communication channels to greater facilitate the exchange of data relating to cybercrime.

5 Use cybercrime data to reinform strategy, legislation, engagement, and enforcement

The assessment element of a pragmatic approach to tackling cybercrime is designed to reinform the preceding four elements of the framework: 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.

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

8. Conclusion



The principal finding of this report is that no single tool can be responsible for bolstering cybersecurity capabilities and tackling cybercrime. There are a range of tools available to achieve these objectives, five of which form the pragmatic approach to tackling cybercrime framework: strategy, legislation, engagement, enforcement, and assessment. Each of these five elements, along with others (*see 8.2 Recommendations for further research*), has a critical role to play in making cyberspace safer for everyone in society. The review and analysis conducted by WP5 partners provided insight into the landscape and mechanisms of each of the five elements. Critically, it also highlighted the important interdependencies between them that must exist to combat cybercrime.

As can be expected, certain aspects of each element in each country are performed well, while others not so well. The pragmatic approach framework can be used by all stakeholders, from policymakers to citizens, to take a holistic view of cybersecurity and cybercrime. The five elements can be used as a basis to shape the cost-benefit analysis for future decisions regarding cybersecurity and cybercrime. Each element contributes to cohesion and synchronisation across various contributors to cybercrime reduction initiatives.

The 21 common observations, 11 key differences, and 25 recommendations proposed in this report will be of value to key stakeholders in progressing cybersecurity and tackling cybercrime. The table below (*see Figure 10*) summarises the recommendations proposed by WP5 partners in this report.

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

Figure 8 – Summary of WP5 Partner recommendations

ELEMENT	RECOMMENDATIONS
Strategy	1. Provide comprehensive and balanced guidance for all stakeholders 2. Assign realistic timeframes to objectives and agree key metrics to track progress 3. Provide guidance to address all stages of the cybercrime lifecycle 4. Produce NCSS documentation to allow for easy and accessible comparability and redressal of issues
Legislation	1. Perform regular evidence-based reforms 2. Use technology neutral terminology when writing legislation 3. Monitor the relationship between sentences, fines, and reoffending 4. Maintain a web-based repository of cybercrime offences 5. Encourage victims of cybercrime to explore civil law as well as criminal law 6. Provide guidance for non-culpable actors
Engagement	1. Consider all demographics, not only young people 2. Employ gamification techniques where appropriate 3. Conduct engagement activities regularly, not as a one-off activity 4. Consider dissemination methods outside of cyberspace 5. Introduce support programmes for victims of cybercrime 6. Use relatable individuals and role models to communicate important messages to young people
Enforcement	1. Provide incentives to encourage the reporting of cybercrime 2. Train increased numbers of police staff in cybersecurity and cybercrime 3. Report meaningful data about cybercrime to budget holders 4. Focus on actions to address root cause, not just immediate incidents
Assessment	1. Harmonise metrics to measure cybercrime at a European/international level to facilitate comparisons 2. Ensure that cybercrime datasets are more accessible to all relevant stakeholders 3. Inferences from analysis should consider the various limitations of data collection 4. Leverage information sharing mechanisms to verify cybercrime data and advance collaboration 5. Use cybercrime data to reinform strategy, legislation, engagement, and enforcement

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

8.1 Recommendations for future research

Both cybersecurity and cybercrime are extremely complex and wide-ranging fields that require ongoing research to build capability, halt perpetrators, and protect victims. The limitations of this report, previously identified in chapter 1.4, surrounding the inability to comprehensively exhaust all possible findings and reach the desired level of granularity, has provided an initial scope for future work. Three main areas have been identified by WP5 partners as warranting further investigation that are relevant to all eight in-scope countries as well as other countries in Europe in terms of developing pragmatic approaches to tackling cybercrime.

1 Review and analyse internationally recognised security standards

At the organisational level, compliance with widely recognised security standards is kept in high regard, such as those provided by ISF, ISO and NIST. While it is dangerous to believe compliance equates to protection, adherence with these standards does ensure that a degree of protection and controls are in place. As a result, WP5 partners believe that a review and analysis of security standards has merit to determine their effectiveness in preventing cyber incidents.

2 Review and analyse the school curriculum for teaching young people about behaviour in cyberspace

This report included a scope for engagement activities which covered cybersecurity related courses, training, and further education. However, WP5 partners believe that the current state of compulsory education for cyber hygiene and behaviour in cyberspace should also be reviewed and analysed to determine to what extent cybersecurity is taught and examined in a similar way to other fundamental subjects such as mathematics, languages, and the sciences.

3 Build a robust data set and conduct more advanced forms of analysis beyond descriptive analysis

In the Assessment element of this report WP5 partners conducted the most rudimentary form of data analysis, known as descriptive analysis. As previously mentioned, this type of analysis aims to summarise past data collected. As cybercrime datasets evolve, future work analysing cybercrime should look to employ more advanced techniques of data analysis, including:

1. Diagnostic analysis, which aims to find the causes of the outcomes identified in a dataset
2. Predictive analysis, which aims to estimate what is likely to happen in the future based on a dataset
3. Prescriptive analysis, which aims to determine what action to take for a problem or decision based on observations in the dataset

These three techniques of data analysis will prove more effective in assisting evidence-based improvements to elements of the framework.

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

9. Appendix

9.1 Proposed recommendations omitted by WP5 partners

The recommendations summarised in Figure 10 were suggested to increase the effectiveness of each element of the pragmatic approach to tackling cybercrime framework and were subsequently discussed and approved by WP5 partners. However, there were also other proposed recommendations for certain elements that were omitted from the report due to WP5 partners questioning their validity and/or applicability at workshop discussions. We provide this here as further background.

9.1.1 Strategy

1 Update national cyber security strategies more frequently

The length of time before the renewal of strategy documentation varies across the eight in-scope countries, with certain countries updating the document less frequently than others. WP5 partners discussed recommending that countries update their NCSS more frequently, however, this proposal was dismissed because there is no amount of time proven to be correct for updating any type of strategy documentation. When looking at organisational strategies, there is also no fixed time after which they are required to be refreshed. WP5 partners concluded that instead security strategies must be flexible to address the evolving nature of cyberspace.

2 Act as thought leaders on the international stage

The ability to act as a world leader in cybersecurity and cybercrime will also vary across the eight in-scope countries. While countries such as the United Kingdom and the Netherlands demonstrate relatively high maturity, others do not. These less mature countries may not have the capability or capacity to be thought-leading in these domains. Instead of recommending all countries to act as leaders, WP5 partners believe that countries should demonstrate active participation and collaboration, while the European Union as a collective act as a leader on the international stage.

9.1.2 Legislation

1 Give key international instruments the power of regulation

Giving instruments such as the Budapest Convention on Cybercrime the power of a regulatory instrument such as the General Data Protection Regulation (GDPR) may have merit. Firstly, this would reduce the significant time lag between countries signing the Convention and ratifying it. Secondly, this would also reduce or eliminate the number of reservations countries are able to make to the Convention. However, WP5 partners ultimately omitted this recommendation from the report because for this to be the case,

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

countries would have to forego an element of state sovereignty and autonomy, two factors that countries may be reluctant to give up.

2 Give judges increased discretion when sentencing cybercrime offenders

The review and analysis of legislation found discrepancies in the length of sentences and fines handed to cybercriminals depending on the severity of crimes across the in-scope countries. The recommendation initially proposed by WP5 partners was to give judges increased discretion when sentencing cybercriminals. However, after discussion it was determined that this may increase levels of human bias. An example of human bias in judicial decision making came out of a study of eight Israeli judges and more than 1,000 parole decisions in 2011.[47] One of the conclusions of the study was that judges were much more likely to approve prisoners applying for parole at the beginning of the day compared with the end. Giving judges more autonomy may increase the ability of human biases such as these to influence decisions.

9.1.3 Engagement

No recommendations omitted by WP5 partners.

9.1.4 Enforcement

1 Extradite cross-border cybercriminals to face harsher sentences

The severity of punishment for perpetrators of cybercrime varies among the eight in scope countries. For those countries where sentences and fines are deemed not to be harsh enough, it may be useful to extradite cybercriminals, where possible, to the countries of their victims in order to receive harsher sentencing. While it is true that a proportion of cybercrime is performed across borders, domestic cybercriminals, who cannot be extradited, also present significant dangers. Extradition of criminal individuals or groups is only viable in a select number of circumstances, so it was decided to not include this recommendation as a pragmatic approach to tackling cybercrime.

9.1.5 Assessment

No recommendations omitted by WP5 partners.

[47] Danziger, S., J. Levav, and L. Avnaim-Pesso, Extraneous Factors in Judicial Decisions. Proceedings of the National Academy of Sciences of the United States of America, 2011.

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

9.2 Questionnaires completed by WP5 partners

9.2.1 Strategy

1 Summarise the current state of cybersecurity strategy in the country.
2 What does the country do well and less well in terms of cybersecurity strategy?
3 What do you believe is best practice in terms of cybersecurity strategy?
4 How do you propose the country transitions from its current state to best practice?

9.2.2 Legislation

1 Summarise the current state of cybercrime-related legislation in the country.
2 Provide a list of the legislative items relating to cybercrime in the country.
3 Does the country's criminal code adequately cover cybercrime offences?
4 What pitfalls do you observe in the current legislative landscape for cybercrime?
5 What do you believe is best practice in terms of cybercrime-related legislation?

9.2.3 Engagement

1 Summarise the current state of engagement activities in the country.
2 Which demographics do engagement activities cover in the country?
3 What dissemination methods are used for engagement activities in the country?
4 What topics are covered through engagement activities in the country?
5 What can be learnt from engagement activities in the country?
6 How do you propose the country improves the effectiveness of engagement activities?

9.2.4 Enforcement

1 What common observation can be made in the cybercrime enforcement landscape across Europe?
2 What challenges do LEAs enforcing cybercrime face in general?
3 What information sharing mechanisms are in place between LEAs or with government agencies?
4 What unique techniques or tools are used to enforce cybercrime in the country?
5 How do LEAs measure the 'success' or 'effectiveness' of cybercrime enforcement?
6 What cybercrimes do LEAs observe to occur the most and least in the country?
7 What challenges do LEAs enforcing cybercrime face in the country?
8 How do you propose the country improves the enforcement of cybercrime?

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

9.2.5 Assessment

1 Provide a list of effective metrics to evaluate cybercrime.
2 What common observations can be made across the eight-country dataset?
3 What are any noteworthy datapoints observed in the country?
4 Provide a list of further sources from which to obtain cybercrime data.
5 What recommendations would you made to improve the collection, management, and analysis of cybercrime data?

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