RISING TO THE PROLIFERATION OF CYBERCRIME CHALLENGING LAW ENFORCEMENT AGENCIES ACROSS EUROPE

David Wright
Krzysztof Garstka
Richa Kumar
Trilateral Research, London[1]

ABSTRACT
Law enforcement agencies (LEAs) face serious challenges in addressing the growing wave of cybercrime across Europe. They have limited human and financial resources to push back against this wave. Their tools and technologies are often a generation behind those of cybercriminals and terrorists on the dark web, deep web and dark nets. LEAs have to operate with ethical, data protection and social constraints that are meaningless to cybercriminals. They also have to respect national borders that don't exist in cyberspace. This article briefly refers to the economic and social impacts of cybercrime, before discussing some of the principal challenges facing LEAs in responding to those impacts. We then focus on the EU-funded CC-DRIVER project, which is helping LEAs to address those challenges. Finally, we draw some conclusions on the near-term future of responses to cybercrime.

Keywords: *social and economic impacts, proliferation of cybercrime, technological challenges, jurisdictional limitations, stakeholder collaboration*

1 Authors' emails: david.wright@trilateralresearch.com, krzysztof.garstka@trilateralresearch.com, richa.kumar@trilateralresearch.com

1 Introduction

Cybercriminality[2] is now ubiquitous and continues to grow.[3] Multiple stakeholders face multiple threats from multiple sources; for instance, in 2019, Mastercard had to fend off some 460,000 intrusion attempts on a typical day, up 70 per cent compared to 2018 (Cowley & Perloth, 2019).

The coronavirus pandemic has greatly increased the amount of time and activities conducted online. As a result, there is already evidence of a corresponding increase in cybercrime. The recent Global Incident Response Threat Report (2020)[4] found that, in an April 2020 survey, 53% of incident response specialists encountered or observed a surge in cyberattacks exploiting COVID-19. In the same month, the US FBI reported a spike of more than 300% in cybercrimes since the beginning of the COVID-19 pandemic (Miller, 2020).

Law enforcement agencies (LEAs) face serious challenges in addressing this growing wave of cybercrime. They have limited human and financial resources to push back against this wave. Their tools and technologies are often a generation behind those of cybercriminals and terrorists on the dark web, deep web and dark nets.[5] LEAs have to operate with ethical, data protection and social constraints that are meaningless to cybercriminals. They also have to respect national borders that don't exist in cyberspace. And, despite attempts to harmonise the laws, the limits and constraints of harmonisation are a challenge for LEAs (Schroeder 2008, Rozmus et al. 2010).

This article briefly refers to the economic and social impacts of cybercrime, before discussing some of the principal challenges facing LEAs in responding to those impacts. We then focus on the EU-funded CC-DRIVER project, which is helping LEAs to address those

2 Eurojust and Europol (2017) use "cybercrime … in a broad sense... i.e. attacks on information systems (cyber-attacks), cyber- enabled crimes (such as non-cash payment frauds and various crimes related to child sexual exploitation online) and investigations in cyberspace, in the context of organised and serious cross-border criminality" (p. 2). Sallavaci (2020) distinguishes between cyber-enabled and cyber-dependent crime. Cyber-enabled crimes are traditional crimes facilitated by the use of ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT (p. 2).

3 https://www.hiscox.com/articles/cost-and-frequency-cyber-attacks-rise-yet-companies-are-less-prepared-combat-attacks

4 https://www.carbonblack.com/blog/black-hat-usa-2020-vmware-carbon-black-releases-global-incident-response-threat-report-detailing-surge-in-cyberattacks-amid-covid-19/

5 Europol (2019) says the darknet is the encrypted part of the Internet accessed using specific software that in themselves are not criminal, such as the Tor browser. The dark web comprises the many criminal websites and services hosted on these networks (p. 44). The European Commission & the High Representative of the Union for Foreign Affairs and Security Policy (2017) define the darknet as consisting of content in overlay networks that use the Internet but require specific software, configurations or authorisation to access. The darknet forms a small part of the deep web, the part of the Web not indexed by search engines (p. 15).

challenges. Finally, we draw some conclusions on the near-term future of responses to cybercrime.

2 Proliferation of cybercrime and its economic and social impacts

Measuring the growth in cybercrime is not straightforward; cybercrimes frequently cross jurisdictions and available statistics are fragmentary. Even more challenging for LEAs, cybercriminality is proliferating, evolving and taking on new forms (McLean, 2019). The space where offenders used to meet has moved into cyberspace, further challenging law enforcement operations with jurisdictional fences. Cybercrime is significantly under-reported, so it is difficult to precisely estimate its scale and cost. Such crimes can have a pecuniary and non-pecuniary impact on victims.

Despite the difficulties in obtaining accurate measurements of the societal and economic scale and impact of cybercrime, most experts agree they are severe. Cybercrime seriously impacts the physical and psychological safety, security and stability of our society (Europol, 2019, p. 4). Cybercrimes and cyberattacks put at risk the infrastructures and networks on which we rely for energy, transport, financial services, hospitals and much else. The threat of falling victim to cybercrime, whether real or perceived, might have a significant impact on people's trust in online services and, as a result, many legitimate uses of technology may suffer. In addition, widespread cybercrimes such as bullying, grooming or stalking may have a devastating impact on the psyche of the victim, sometimes resulting in the victim's suicide.[6]

Our economies suffer serious damage from cybercrime. In 2018, cybercrime was generating at least $1.5 trillion in profits in the US, according to one study (McGuire, 2020). Of this amount, $860 billion came from illicit, illegal online markets, $500 billion from illicit trade in trade secrets and intellectual property, $160 billion from data trading, $1.6 billion from crimeware and cybercrime as a service and $1 billion from ransomware. It should be noted, though, that each ransomware incident can have devastating consequences; in one attack alone, a company lost €60 million in revenue (National Crime Agency, 2019, p. 46).

While there are many studies on this topic, there can be no doubt that cybercrime has a substantial economic impact, it can generate significant profits, and it can cause great harm to our society, to individuals, companies, public bodies and more. This cybercrime swamp poses great challenges, in particular to law enforcement agencies, who need to

6 https://www.stltoday.com/suburban-journals/stcharles/news/stevepokin/my-space-hoax-ends-with-suicide-of-dardenne-prairie-teen/article_0304c09a-ab32-5931-9bb3-210a5d5dbd58.html; also see: https://eu.news-leader.com/story/life/2014/11/19/pokin-around-biggest-story-young-girls-suicide/19291825/

investigate cybercrimes and apprehend their perpetrators. We address some of these challenges in the following section.

3 Challenges facing Law Enforcement Agencies

As criminals adopt new technologies, apps and platforms, law enforcement and legislators must also innovate in order to address these challenges. This section gathers a selection of challenges that LEAs face when tackling various forms of cybercrime.

3.1. Shortage of resources

The first such challenge is the chronic lack of resources. Publicly funded LEAs have limited resources (financial, human, technological) to deal with the ever-changing cybercrime landscape of threats and agents; cybercriminals are not bound by such resource constraints. This challenge can be demonstrated through two distinct examples.

First example: Fighting cybercrime requires many experts in cyber investigation, law and regulation, cutting-edge technology and management, economics. There are three main lines of competition in this regard. First, the lucrative private sector may offer prospective candidates employment conditions beyond those that LEAs can afford. Second, cybercriminals themselves can recruit individuals who could otherwise be their adversaries. Third, LEAs are competing among themselves as well as the rest of the world for cybersecurity talent, of which there is a growing shortage. The situation is exacerbated by the cybersecurity skills gap for professionals working in the private sector in Europe, predicted to be 350,000 by 2022 (European Commission & the High Representative of the Union for Foreign Affairs and Security Policy, 2017, p. 15).

Second example: The transnational and technical nature of cybercrime requires co-operation between various private and public actors, which in turn requires LEAs to invest matching resources. This need manifests in the context of detecting and tackling specific crime incidents. In 2019, referrals from industry and third country partners reached a record high, putting a serious strain on the capacity of LEAs in the EU to investigate these crimes. At least 18 Member States received referrals from the USA through Europol (2019) alone which further constrains the limited resources available to LEAs (p. 30).

The less visible, yet in the long run crucial, category of co-operative expenses is tied to multiangular analysis of data hiding valuable information about the cybercrime ecosystem. LEAs often lack resources to gather and analyse the data about cybercrime. For example, the increasing amount of child sexual exploitation material (CSEM) detected online by law enforcement and the private sector continues to strain LEA resources to conduct criminal investigations (Europol, 2019, p. 7). LEAs need to leverage their limited

resources by collaborating with private and public actors to identify and apprehend cybercriminals.

3.2. Identifying cybercriminals

Identifying cybercriminals is a multi-pronged challenge for the LEAs with two core aspects being technical and human identification.

Technical identification is made difficult by technologies focused on helping cybercriminals to hide their activities by leaving misleading tracks – or no tracks at all. Recent trends such as the increasing criminal use of encryption, anonymisation tools, virtual currencies and darknets have led to a situation where law enforcement may no longer (reasonably) establish the physical location of the perpetrator, the criminal infrastructure or electronic evidence. It is often unclear which country has jurisdiction and what legal framework regulates the real-time collection of evidence or the use of special investigative powers such as monitoring of criminal activities online and various undercover measures (Eurojust & Europol, 13). The use of obfuscating technologies and platforms is evident – more than three-quarters of cybercrime investigations in the EU have involved the use of encryption (Europol, 2015, p. 50).[18]

Human identification is made difficult by diversity in the ranks of cybercriminals. Cyber threats come from both non-state and state actors: they are often criminal, motivated by profit, but they can also be political and strategic (European Commission & the High Representative of the Union for Foreign Affairs and Security Policy, 2017, p. 2). There are many types of cybercriminals, including individual threat actors, organised gangs and states along with technologically talented young people who may not be aware of the consequences of their behaviour. In some cases, state agencies are directly involved; in other instances, states sponsor free-lance gangs who work on their own behalf as well as their state handlers. Consequently, cybercriminals are driven by a range of motives that include profit, idealism, curiosity, thrill-seeking and the desire to harm and/or target others (Dalins 2018, Turvey 2011, Toby 1962).

3.3. Confronting the availability of new cybercrime technologies

In addition to increases in sophistication of cybercrime-related technologies, their accessibility and ease of use pose another crucial challenge for the LEAs (National Crime Agency, 2019). In many cases, it no longer requires a sophisticated or carefully planned operation to break into IT systems. The hacking tools and malware available on the dark web have lowered the barrier to entry into cybercrime, making it possible for amateur and unsophisticated hackers to cause enormous damage.

An important contributor to this state of affair is the rise of cybercrime as a service (CaaS), which makes easy-to-use exploit kits, ransomware and customised malware easily avail-

able on the dark web for use in assisting the commission of cybercrime. Cybercrime as a service offers every service as a conventional business ranging from product development to technical support, distribution, quality assurance, and even help desks. Some groups offer subscription services for exploiting unpatched system vulnerabilities (Osborne, 2017).

3.4. Approaching young people

Young people may be more digitally savvy than their parents or grandparents, but they may also be more complacent about cybersecurity. The most vulnerable members of society, children, are being targeted, radicalised, groomed, coerced, monetised, sexually abused and exploited. Young people are not just victims of cybercrime; they are also at risk in terms of entry into cybercrime, from cyber risk-taking to cyber juvenile delinquency. Increasingly, they are being drawn down pathways into cybercriminality.

Europol describes the amount of child sexual exploitation material (CSEM) online as "staggering" and continuing to increase. The online solicitation of children for sexual purposes remains a serious threat in the EU, with many Member States reporting a rise in the crime (Europol, 2019: p. 31). Self-generated explicit material (SGEM) has also become common, driven by growing access of minors to high-quality smart phones and a lack of awareness about the risks. Offenders use various ways and platforms to disguise online CSEM, making it more challenging for LEAs to detect such images and videos. Peer-to-peer sharing remains the most popular conveyance of CSEM (Europol, 2019: p. 30).

Europol has also expressed concern about improvements of so-called deepfakes. Cybercriminals have already put the faces of celebrities on existing pornographic videos. Although deepfake technologies are relatively new, they are rapidly improving, becoming more accessible and easier to use. It may be just a matter of time before the first deepfakes appear depicting online CSE, in the generation of new 'personalised' CSEM. This can also have serious implications for law enforcement authorities, as it might raise questions about the authenticity of evidence and complicate investigations. Fighting CSE is a joint effort between law enforcement and the private sector; a common platform is needed in order to coordinate efforts and prevent a fragmented approach and the duplication of effort (Europol, 2019, p. 34).

3.5. Cybercrimes don't respect national boundaries

In 2018, the European Commission found that in the EU "more than half of all investigations involve a cross-border request to access [electronic] evidence."[7] The principle of territoriality limits the jurisdiction and investigative powers of LEAs and the judiciary in such cases. Differences between domestic legal frameworks in the Member States and

7 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

international instruments continue to be a serious impediment to the international criminal investigation and prosecution of cybercrime (Europol, 2019, p. 57).

Transnational cooperation in criminal matters, including cross-border access to evidence located outside the jurisdiction of the investigating or prosecuting authority, has traditionally been regulated via international agreements. Within the EU, the European Investigation Order (EIO) provides for the gathering and transfer of evidence between MSs and for deadlines of 120 days, which is still too long for accessing e-evidence in cybercriminal investigations given the particular fast-paced nature of the evolution of cyberspace and cybercrime. The proposed e-evidence framework seeks to address the problems with the existing mechanisms for cross-border access to e-evidence while respecting fundamental rights and the principles enshrined in the Charter of Fundamental Rights (CFR) of the EU and other key international instruments (Sallavaci, p. 30).

3.6. Legislation as a challenge to effective actions against cybercrime

In the case of *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (2014) Joined Cases C-293/12 and C-594/12, the European Court of Justice (CJEU)[8] overturned the Data Retention Directive (DRD).[9] This and further judgments in the field[10] and the implementation of the General Data Protection Regulation (GDPR) in 2018 have left law enforcement and prosecutors uncertain about the legality of obtaining data from private parties. In some Member States, there is (still) legislation in place to ensure that Internet service providers (ISPs) retain data for law enforcement purposes, whereas in other MS, national legislation has been annulled in the wake of the CJEU judgment.

8 With the entry into force of the Treaty of Lisbon on 1 Dec 2009, the official name of the European Court of Justice (ECJ) was changed from the "Court of Justice of the European Communities" (CJEU) to the "Court of Justice". The Court was -- and is -- often referred to as the European Court of Justice, with the abbreviation ECJ still frequently used in preference to CJEU. In this article, we are using CJEU for all decisions after 2009 in line with the Treaty of Lisbon.

9 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources.*

10 Such as *Tele2 Sverige AB v. Post-och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others* (2016) Joined Cases C-203/15 and C-698/15.

Data retention legislation in EU Member States post-*Digital Rights Ireland* and *Tele2/Watson* – (2019) – selection of countries[11]	
Country	**Data retention legislation in force?**
Austria	No – Constitutional Court invalidated the national legislation
Belgium	Yes – references to the CJEU pending
Bulgaria	Yes – pre-Data Retention Directive legislation is still in force
Croatia	Yes
Cyprus	Yes – national legislation upheld by Supreme Court in 2015
Czech Republic	Yes – currently challenged before the Constitutional Court
Denmark	Yes – challenged at the national court (Eastern High Court)
Estonia	Yes
Finland	Yes
France	Yes – preliminary ruling requests pending at the CJEU
Germany	Yes – legislation currently challenged before the German Constitutional court
Greece	Yes
Hungary	Yes
Ireland	Yes
Italy	Yes
Latvia	Yes
Lithuania	Yes
Luxembourg	Yes
Malta	Yes – challenge brough at national level
Netherlands	No – data retention act no longer applicable after Hague Civil Court ruling from 2015
Poland	Yes
Portugal	Yes – national legislation (pre-DRD) upheld by Constitutional court
Romania	Yes – new, post-*Digital Rights Ireland* law enacted
Slovakia	Yes – provisions contradicting CJEU rulings were annulled by the Slovak Constitutional Court
Slovenia	No – Slovenian Constitutional Court annulled the legislation
Spain	Yes
Sweden	Yes

11 Council of the European Union, Working Paper on Data Retention Legislation, WK3103/2019 INIT, 6 March 2019, available at https://www.statewatch.org/media/documents/news/2019/may/eu-council-data-retention-ms-situation-wk-3103-19.pdf

The lack of unified retention of electronic communication data across the EU has proven a key challenge to investigating cross-border cybercrime. LEAs contend that electronic communication data is key to the successful investigation and prosecution of serious crimes (including cybercrime) (Eurojust & Europol, 2017, p. 4).

While some LEAs may find responding to the strictures of the General Data Protection Regulation to be somewhat challenging, Europol has spoken hopefully of the GDPR's having a positive impact on data breaches and leading to enhanced data security as a result of the high fines allowed by the GDPR in the event of data breaches as well as the media headlines that often arise from big data breaches. It has also emphasised the need for law enforcement to engage with policymakers, legislators and industry to "have a voice in how our society develops" (Europol, 2018, p. 4).

3.7. Finding the right degree of reliance on new technologies

Many LEAs look to new technologies that might help compensate for a shortage of human resources. While some technologies are helpful in their investigations, some have generated a lot of controversy, even among LEAs. One of those has been predictive policing applications. Essentially, there are currently two main types of predictive policing tools, both of which are problematic. One type is based on location – it identifies where and when crimes have occurred, so LEAs can police those areas more to apprehend actions before they happen.[12] The second type focuses on the likelihood that someone will commit a crime. It's a form of profiling. There have been increasing calls for abandoning predictive policing algorithms until such time as the biases can be better addressed (Heaven, 2020).

Another technology used by LEAs that has also generated a lot of controversy is facial recognition. Clearview AI, a US start-up, has devised a ground-breaking facial recognition app that enables a police officer to take a picture of a person, upload it and then get to see public photos of that person, along with links to where those photos appeared. The Clearview AI app includes programming language to pair it with augmented-reality glasses; users would potentially be able to identify every person they saw in the street. The system's backbone is a database of more than three billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo and millions of other websites. The company also claims that more than 600 LEAs are already using its app (Hill, 2020).

The Estonian Forensic Science Institute is leading a consortium of European agencies undertaking the EU-funded TELEFI project (Towards the European Level Exchange of Facial Images) on how facial recognition is currently being used for the investigation of crime across Member States.[13] The consortium is also considering the potential for implement-

12 See, for example, https://www.predpol.com/hot-spot-policing/

13 https://www.ekei.ee/en/projects

ing the exchange of facial images within the Prüm framework, which enables mutual searching of interconnected DNA, fingerprint and vehicle registration databases for law enforcement.

A report drawn up by the national police forces of 10 EU Member States, led by Austria, calls for the introduction of EU legislation to introduce and interconnect such databases in every Member State, with a central role played by Europol in the exchange of facial recognition and other biometric data (Campbell & Jones, 2020).

3.8. Gaining public trust and raising awareness

Despite the challenges they face, LEAs do have a relatively good standing amongst the public. Data from European countries shows that trust in the police tends to be higher than trust in the political and legal systems. In the majority of European countries, people trust the police more than they trust each other.[14] Trust is important for many reasons, for social solidarity and the effective governance of our institutions. Some studies have shown that trust has a causal impact on economic outcomes (Algan & Cahuc, 2010).

Trust is hard to earn, but easy to lose. Hence, the use of controversial technologies such as predictive policing, facial recognition and other Big Brother surveillance risks damaging public trust in the police.

As held by CJEU in its Opinion 2/13, "the principle of mutual trust between the Member States is of fundamental importance in EU law" (CJEU, 2014). This principle hinges on the mutual trust of MS in each other's criminal justice systems: trust "is grounded, in particular, on their shared commitment to the principles of freedom, democracy and respect for human rights, fundamental freedoms and the rule of law" (Sallavici, 2020: p. 30).

Trust is built on transparency. Hence, LEAs must find the right balance between transparency and confidentiality in everything they do. Europol (2019) favours cyber simulation exercises to help raise awareness of the roles, responsibilities and capabilities of each actor in the exercises and increase the level of trust and collaboration. It also says law enforcement must continue to build trust-based relationships with cryptocurrency-related businesses, academia, and other relevant private sector entities, to more effectively tackle issues posed by cryptocurrencies during investigations (p. 24).

14 https://ourworldindata.org/trust. See also https://www.nwo.nl/en/news-and-events/news/2018/05/police-enjoy-greater-level-of-trust-than-other-institutions-in-europe.html

4 How CC-DRIVER addresses the challenges

In this section, we refer to the EU-funded CC-DRIVER project, a three-year project that began in May 2020. The project is aimed at understanding the technical and human drivers of cybercrime and how to use that knowledge to reduce cybercrime and to deter young people from a life of crime. The CC-DRIVER consortium comprises 13 partners from nine countries across Europe: Finland, France, Germany, Greece, Finland, Romania, Spain, Switzerland, UK. The CC-DRIVER consortium is addressing the challenges, in whole or in part, mentioned in the preceding section.

4.1. Leveraging resources

CC-DRIVER responds directly to the lack of resources described in section 3.1 above. With public funding in the fight against cybercrime, we are alleviating some of the financial pressure on LEAs by reviewing legislation, developing policy and technical toolkits that may assist them in tackling cybercrime. By engaging the project's LEAs with a diverse team of European researchers, we are helping to remedy the pressure on LEAs' human resources while developing synergies and possibilities of collaboration among LEAs across Member States. We are also leveraging the project's resources and impacts by having formed a cluster with eight other H2020 projects focused on LEAs and new technologies to ensure that each project develops new and effective technology to cater to LEA challenges with minimal duplication.

4.2. Identifying cybercriminals

CC-DRIVER is responding to the challenges of technical and human identification of cybercriminals, as follows.

First, our project aims to assist in technical identification of perpetrators by developing and enhancing sets of cybercrime awareness and investigation tools. They include a threat intelligence portal, analysing and correlating data and intelligence across multiple relevant sources, including OSINT, data available for LEAs and data collected by cybersecurity vendors; an automated notification tool for LEAs and CERTs for cases when attack-related information can be attributed to a specific country or area; and technologies for extracting forensics data from breached systems, with added automated analysis and data mining capabilities.

Second, in the search for relevant human factors, CC-DRIVER is identifying different types of cybercriminals and undertaking a broad review of the characteristics of offenders, victims and societal impact. The consortium will better understand these drivers after interviews with experts working directly with young people involved in cybercrime to further explore motivations, human factors and key drivers of cybercriminality. In addition, the partners are interviewing academics across the key disciplines of psychology,

cyberpsychology, criminology, neurobiology and anthropology and specifically digital anthropology.

Third, the consortium is interviewing LEAs to have their perspectives on cybercriminality and juvenile cybercriminality, in particular. The consortium is especially interested in how young people act differently online. A major input to understanding such drivers will be the results of a CC-DRIVER survey of 8,000 young people between the ages of 16-19 in each of eight EU countries. Led by University of East London, these questions will address the prevalence of juvenile delinquency and cybercrime, drawing on digital anthropological constructs along with theories of criminology that may have explanatory value regarding deviance and anti-social behaviour, digital anthropological constructs with theories of criminology (https://www.ccdriver-h2020.com).

4.3. Confronting the availability of new cybercrime technologies

CC-DRIVER is approaching the trend of growing availability and accessibility of cybercrime tools by investigating the various manifestations of cybercrime as a service (CaaS), its modalities, purveyors and trends. The survey will review the range of cybercrime as a service activities on the surface and dark web, including cyber theft, cyber fraud, espionage, money-laundering, ransomware, blackmail and extortion, social engineering and phishing, disinformation, fake news, deepfakes, cyber sabotage, cyber stalking, bullying and child sexual abuse, defacement, denial of service and more.

The survey includes those in the EU who offer and use cybercrime as a service and will investigate different types of business models. It will report on the evolution of websites that support cybercriminal services over time and the ways in which human factors influence technical and business strategies and choices of criminals. The survey will also include a review of trends: is cybercrime as a service increasing? Does it have geographic roots? How are cybercriminal tactics, techniques and models evolving? Attention will be given to emerging threats that target IoT and related devices.

4.4. Approaching young people

One of the principal tasks in the CC-DRIVER project is to understand how to divert young people and teenagers from cybercrime towards non-criminal cyber activities. Thus, the project is conducting a multidisciplinary study of the drivers of cyber juvenile delinquency and cybercriminality across a range of offences. Cyber offences vary between jurisdictions; hence, we will investigate a range of online behaviours from risk-taking and delinquency to criminality, to include an analysis of drivers and motivations. The online survey will be self-completion, employing a stratified sample of youth population in each of the eight EU countries.

The partners will create an online questionnaire that young people and organisations can use to assess their vulnerability to cybercrime. We will create an online assessment, awareness and educational tool to enable youth to develop insights regarding their vulnerability to becoming involved in cybercriminal activity. Our "Cyber Expert or Cybercriminal" metric will build on Europol's public awareness and prevention campaigns. We will create a parent, caregiver, educator and other stakeholders' 'Pathways into Cybercrime' checklist (PCC), a resource that will 'red flag' youth behaviours or attitudes that may facilitate cyber delinquency or criminality.

4.5. Overcoming jurisdictional limitations with practical results

The CC-DRIVER consortium has taken several initiatives to address the challenge of timely, cross-border co-operation in addressing cybercrimes that don't respect national boundaries. The initiatives bring together different stakeholders, especially LEAs, from different countries. The CC-DRIVER consortium and project themselves are good examples of how different partners from different countries can come together in common cause to address the cybercrime challenges that affect them all.

The consortium has created a relatively large Stakeholder Board (SB) with 24 members, 11 of whom are LEAs. There are also six academics and representatives from an association, two companies, two CERTs, one military and one NGO. The SB members come from 16 different countries. The consortium convenes quarterly meetings with the SB, so that stakeholders have an opportunity to exchange views, not only in regard to the project but also related cybersecurity issues and raising public awareness.

In another initiative, the consortium has created a working group of LEAs from across the EU to discuss their common challenges and different approaches to addressing them and identifying good practices. The working group consists of the four LEA partners from the CC-DRIVER consortium as well as six LEAs from the project's SB. The consortium justifies the disproportionate number of LEAs on the SB because the project is targeted at LEAs, helping them understand the drivers of cybercrime and giving them tools they need to counter cybercrime.

As another initiative and as co-ordinator of the CC-DRIVER project, Trilateral contacted eight other projects funded under the EU's Horizon 2020 security work programme to suggest that they form a cluster since all of the projects include LEAs as partners and are focused on improving the tools at the disposition of LEAs in combatting organised crime and terrorism. All responded positively. The LEA cluster meets quarterly and have begun inviting each other's partners to webinars that might be of interest. In this way, the projects leverage the results their projects, discuss issues of mutual interest and formulate coherent recommendations.

4.6. A comparative analysis of cybercrime legislation in eight countries

Eurojust and Europol (2017) have said that the challenges to LEAs "could further benefit from more extensive (and broader) research and a closer comparison of existing legislation at national and international levels" (p. 2).

The CC-DRIVER project is undertaking a comparative analysis of cybersecurity legislation and policy in eight European countries, namely UK, Spain, Germany, Romania, France, Italy, Sweden, Netherlands. We chose eight countries to provide us with a dataset that can be extrapolated to understand similar legislative and regulatory gaps in other contexts. The consortium is examining to what extent such policies include provision for (1) assessing risks, threats and vulnerabilities – human and technical, youth and adult (2) identifying and deploying relevant security measures, (3) taking into account legal and ethical rules of operation, (4) cost-benefit considerations, (5) fundamental rights such as the rights to privacy, protection of personal data and the free movement of persons. The CC-DRIVER partner Information Security Forum (ISF) is sending a questionnaire to its 450 members regarding the provisions that should be included in a comprehensive cybersecurity framework addressing crime as a service and young people. The partners will host workshops with LEAs and ISF member organisations in each of the eight Member States on examples of good cybersecurity practice and how we can turn off young people from cybercriminal pursuits. The partners are also interviewing members of national cyber security and cybercrime organisations on their key recommendations to SMEs and CSOs on measures they can take to reduce the impact of cybercriminality.

Based on their analysis, the partners will identify a set of good cybersecurity policy practices, especially concerning young people and cybercriminality for inclusion in our policy toolkit. We will also develop a cybersecurity policy framework, which we will commend to policymakers in Member States.

4.7. Finding the right degree of reliance on new technologies

LEAs are, in some sense, fortunate that they are being offered a range of new tools, technologies, applications and platforms from EU-funded projects, such as CC-DRIVER. Any ethical, data protection and societal issues that might arise from the development and use of these new technologies can be considered through the conduct of an impact assessment. The CC-DRIVER consortium is carrying out an ethical, data protection and societal impact assessment to identify potential impacts that could arise in each of the project's work packages and tasks. It is then discussing those potential impacts with the WP and task leaders and reaching agreement on which issues need to be addressed and how. Trilateral will next outline the proposed solutions to those impacts to the project's ethical advisory board, which comprises four external ethics experts, as well as the project's Stakeholder Board.

Thus, the impact assessment can help uncover the ethical and other issues that can arise from new technologies like predictive policing, facial recognition and such surveillance systems. An ongoing impact assessment, from the beginning to the end of a project, is useful also in raising the awareness of all partners in a consortium about the various issues that could arise from project developments and how best to solve those issues.

4.8. Gaining public trust and raising awareness

To best meet their challenges, LEAs should understand the importance of earning the public's trust as well as raising the public's awareness of the different types of cybercrimes and how they can avoid becoming victims.

The CC-DRIVER partners are undertaking various efforts to raise public awareness about the drivers of cybercrime, particularly as they come into play with young people, and the various measures CC-DRIVER is taking to counter those drivers.

An important way of gaining public trust depends on engaging stakeholders. To that end, CC-DRIVER is engaging stakeholders in several ways. It has created a large Stakeholder Board and an ethics advisory board, as mentioned above. It also has a Security Advisory Board which reviews project deliverables for whether they raise any national security issues. The project has created an LEA working group, comprising 10 LEAs, some partners and some from the Stakeholder Board, to discuss issues of mutual concern, good practices and sharing information about cybercrimes and cybercriminals. There is also the cluster of eight other EU-funded projects, also as mentioned above. All of the boards and working groups will help substantially in stakeholder engagement and improving trust.

The project also undertakes various dissemination activities to raise awareness via the project website[15], press releases, workshop presentations, social media accounts, etc.

5 Conclusion

One of the key conclusions we can draw from the challenges facing law enforcement agencies in Europe is the importance of co-operation and collaboration between different stakeholder groups, including LEAs, CERTs, CSIRTs, the private sector, academics, agencies such as Europol and ENISA, among others. The EC is stimulating such collaboration in various ways, not least of which is funding security projects that bring together several different types of partners, as is the case of CC-DRIVER.

15 https://www.ccdriver-h2020.com/

A second conclusion (or observation) we can draw is the need to resolve jurisdictional issues and expedite information exchange. Criminals and terrorists can hide their data anywhere in cyberspace, which complicates questions of jurisdiction. The loss of location results in competing claims to prosecution, underlining the need for early involvement of judicial authorities through Eurojust, direct police-to-police channels for co-operation and communication facilitated by Europol, and continuous innovation in the process of operational collaboration.

CC-DRIVER is bridging jurisdictional issues in various ways, particularly through its creation of a working group of 10 different LEAs. The project is contributing towards the alignment of legal frameworks through its comparative analysis of legislation and policy combatting cybercrime in eight European countries. Its gap analysis will identify benchmarks for good and comprehensive legislation and create a policy brief, which it will discuss with LEAs and policymakers across the EU.

We will only begin to turn the tide on cyber-attacks when we increase the chances of getting caught and sanctioned for committing them as well as diverting our youth towards non-criminal cyber activities. Cyber-attacks should be promptly investigated and perpetrators brought to justice, or action taken to allow an appropriate political or diplomatic response. The tools and applications being developed in CC-DRIVER will help achieve that, but we need to agree that cybersecurity is everyone's responsibility.

Acknowledgement

CC-DRIVER has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883543. The views expressed in this article are those of the authors and are in no way intended to reflect those of the European Commission.

References

- Algan, Y., & Cahuc, P. (2010) Inherited trust and growth. *The American Economic Review*. 100(5), Dec 2010, 2060-2092.
- Campbell, Z. & Jones, C. (2020) Leaked Reports Show EU Police Are Planning a Pan-European Network of Facial Recognition Databases. *The Intercept*. 21 Feb.
- Court of Justice of the European Union, Opinion 2/13 of the Court (Full Court) 18 December 2014, clause 191, p. 36.
  https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62013CV0002&from=EN
- Cowley, S., & Perlroth, N. (2019) Capital One Breach Shows a Bank Hacker Needs Just One Gap to Wreak Havoc. *The New York Times*. 30 July.
- Dalins, J., Wilson, C. and Carman, M. (2018) Criminal motivation on the dark web: A categorisation model for law enforcement. *Digital Investigation, 24*.
- European Commission & the High Representative of the Union for Foreign Affairs and Security Policy (2017) Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Joint Communication to the European Parliament and the Council. JOIN (2017) 450 final. Brussels, 13 Sept.
- Europol (2015) Internet Organised Crime Threat Assessment (IOCTA).
- Europol (2018) Internet Organised Crime Threat Assessment (IOCTA).
- Europol (2019) Internet Organised Crime Threat Assessment (IOCTA).
- Eurojust & Europol (2017) Common challenges in combating cybercrime. Council of the European Union. Brussels, 13 March.
- European Court of Justice, Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources.*
- Heaven, W.D. (2020) Predictive policing algorithms are racist. They need to be dismantled. *MIT Technology Review*. 17 July.
- Hill, K. (2020) The Secretive Company That Might End Privacy as We Know It. *The New York Times* 18 Jan 2020.
- McGuire, M. (2018) *Into the Web of Profit – Understanding the Growth of Cybercrime Economy.* Bromium Inc, p. 15. [Bromium is a subsidiary of HP.]
- McLean, R. (2019) A hacker gained access to 100 million Capital One credit card applications and accounts. *CNN Business.* 30 July.
- Miller, M. (2020) FBI sees spike in cyber crime reports during coronavirus pandemic. *The Hill*. 16 Apr.
- National Crime Agency (2019) National Strategic Assessment of Serious and Organised Crime 2020.
- Osborne, C. (2017) Shadow Brokers launch subscription service for stolen exploits, zero-day leaks. ZDNet. 31 May.

- Rozmus, M., Topa, I. and Walczak, M. (2010) Harmonisation of Criminal Law in the EU legislation– The current status and the impact of the Treaty of Lisbon.
  Online: http://www.ejtn.eu/Documents/Themis/THEMIS% 20written% 20paper.
- Sallavaci, O. (2020) Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters. In: Jahankhani, H., Akhgar, B., Cochrane, P. & Dastbaz, M. (eds.), Policing in the Era of AI and Smart Societies. Cham, Switzerland, Springer Nature, 1-58.
- Schroeder, W. (2020) Limits to European harmonisation of criminal law. *Eucrim: the European Criminal Law Associations' forum 2*.
- Toby, J. (1962) Criminal motivation: a sociocultural analysis. *The British Journal of Criminology 2.4*.
- Turvey, B.E. (2011) Criminal profiling: An introduction to behavioral evidence analysis. Ed. *Academic press*.