JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2022, 1–18
https://doi.org/10.1093/cybsec/tyac014
Review Article

Review Article

SoK: cross-border criminal investigations and digital evidence

Fran Casino [1,2,*], Claudia Pina [3], Pablo López-Aguilar [1,4], Edgar Batista [1], Agusti Solanas [1] and Constantinos Patsakis [2,5]

[1]Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Avinguda dels Països Catalans 26, 43007 Tarragona, Spain, [2]Information Management Systems Institute, Athena Research Center, Artemidos 6, Marousi 15125, Greece, [3]European Judicial Cybercrime Network, Eurojust, Johan de Wittlaan 9 2517 JR, The Hague, Netherlands, [4]Anti-Phishing Working Group - Europe, Av. Diagonal 621–629, 08028 Barcelona, Spain and [5]Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou str., 18534 Piraeus, Greece

*Correspondence address. Avinguda dels Països Catalans, 26, 43007 Tarragona, Spain. E-mail: franciscojose.casino@urv.cat

Received 25 May 2022; revised 15 July 2022; accepted 24 August 2022

Abstract

Digital evidence underpin the majority of crimes as their analysis is an integral part of almost every criminal investigation. Even if we temporarily disregard the numerous challenges in the collection and analysis of digital evidence, the exchange of the evidence among the different stakeholders has many thorny issues. Of specific interest are cross-border criminal investigations as the complexity is significantly high due to the heterogeneity of legal frameworks, which beyond time bottlenecks can also become prohibiting. The aim of this article is to analyse the current state of practice of cross-border investigations considering the efficacy of current collaboration protocols along with the challenges and drawbacks to be overcome. Further to performing a legally oriented research treatise, we recall all the challenges raised in the literature and discuss them from a more practical yet global perspective. Thus, this article paves the way to enabling practitioners and stakeholders to leverage horizontal strategies to fill in the identified gaps timely and accurately.

Key words: cybercrime, digital evidence, digital forensics, evidence exchange, international investigation, cross-border collaboration

Introduction

Understanding the evolution of information and communication technologies without cross-border data flows and ubiquitous systems is impossible. Nevertheless, the opportunities that such evolution brings to all levels of society come with unprecedented challenges in the context of criminal prosecution in cyberspace. Not only the amount of criminal investigations is increasing, but the border-less nature of the Internet adds humongous complexity to such procedures. In addition to the technical challenges of such investigations, the collaboration amongst different organizations is crucial, yet jurisdictional issues further impede it. Thus, the investigation and prosecution of crimes that extend beyond national boundaries is a problem that requires effective measures.

One of the main issues of cross-border investigations is the collection and exchange of electronic evidence, which is often located in multiple countries, requiring external access to it. While being a priority for most countries, there are many unsolved issues due to the different regulatory frameworks of each country, which hinder collaboration due to, e.g. ethical, legal, or even procedural differences. Moreover, since more than half of all criminal investigations require access to cross-border electronic evidence [1], most investigations require evidence requests to other jurisdictions. In addition to the procedural burden, judicial cooperation processes require weeks or even months to be fulfilled.

The EU and countries such as the USA have recently proposed initiatives to address the challenges related to gathering data in dif-

© The Author(s) 2022. Published by Oxford University Press. This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs licence (https://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial reproduction and distribution of the work, in any medium, provided the original work is not altered or transformed in any way, and that the work is properly cited. For commercial re-use, please contact journals.permissions@oup.com

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

ferent jurisdictions, intending to prevent and prosecute cybercrime in a timely manner. However, as discussed in the literature, these initiatives may pose additional challenges related with fundamental rights and the rule of law provided in the EU and the countries involved.

Contribution

This article analyses the current state of the art and practice of cross-border investigation initiatives and extracts the main challenges according to their nature, e.g. technological, procedural, legal, communication, and economic. It also contributes to the analysis of strategies to overcome them, and provides discussion of the road ahead in cross-border investigations, including research projects, and tools. Moreover, it analyses the impact of technologies such as blockchain that will require novel, adaptable regulations to deal with the dynamic nature of cybercrime. To the best of our knowledge, this is the first article providing such a thorough analysis of the topic, thus enabling a global perspective of the status of cross-border investigations.

The remainder of this work is organized as follows. 'Research Methodology' describes the research methodology, providing a descriptive analysis of the retrieved literature. 'Main Instruments for Cross-Border Investigations in Europe' presents a background on the main initiatives for cross-border data exchange. 'Literature Review and Challenge Extraction' describes the state of the art based on the literature analysed in 'Research Methodology', and discusses the current challenges of cross-border data exchange initiatives. Relevant open issues, trends, and further research lines are discussed in 'Discussion—Enhancing Cross-Border Collaboration'. Finally, the article concludes in 'Conclusions' with some final remarks.

Research Methodology

Our review protocol is based on the five features of Denyer and Tranfield [2] for a systematic literature review. More precisely, the steps are the following: (1) define the scope of the review, (2) define the research questions, (3) search literature databases, (4) apply inclusion and exclusion criteria, and (5) synthesize and report the results of the literature analysis.

Defining the scope of the review

A systematic literature review relies on standardized processes for searching, screening, analysing, and synthesizing the available literature in a systematic, transparent, and reproducible manner, thus assisting in the development of policy and decision-making [3]. Systematic reviews help building a reliable knowledge base by aggregating information from a wide range of relevant studies [3].

This article focuses on cross-border data exchange initiatives, protocols, and solutions, to extract and analyse the current state of practice and the existing challenges to provide a fruitful ground for discussion. Our approach relies on several research questions pertinent to cross-border co-operation, which are aligned to the specific objectives of our article (see Table 1). Based on these research questions, we perform a thorough analysis of the available literature and analyse the most well-known protocols and their challenges.

Search strategy

Since we aim to tackle recent challenges of current practice and the impact of novel frameworks in cross-border co-operations, we focused on the last 5 years, to give an up-to-date view of the current status of the matter. To this end, we performed a systematic literature search considering papers published between 2016 and 2022 (as of January). Scopus and Web of Science (WoS) were used to locate all scientific-related literature [4].

We queried Scopus and WoS using the following query:

> TITLE-ABS-KEY ((international OR cross-border OR cross AND border) AND investigation AND (crime OR criminal))

It is worth noting that the first bulk search query yielded 379 results. Database's refinement features were used (fine-tuning of results following the context of specific articles, papers, subject area, and so on). When a study's abstract was unavailable, the full article was retrieved and evaluated for relevance.

Due to the broad selection of articles, we discovered additional studies using the so-called backward and forward snowball effect, which involved searching the references of articles and reports for additional citations [5]. For instance, additional grey literature was discovered by manually searching the reference lists in several reports, since several relevant sources are only present in the form of, e.g. technical reports and guidelines in e.g. official Eurojust, Europol, and international cooperation websites. Following our methodology a total of 442 sources were initially selected (combining research and grey literature).

Inclusion and exclusion criteria

We evaluated the eligibility of the retrieved literature based on a set of inclusion/exclusion criteria. Initially, we excluded all non-English written papers. The next step was the screening of the retrieved papers (title and abstract reading). For the remaining articles, we performed a full reading. It is worth noting that a notable amount papers were excluded during the last two steps (title/abstract screening and full paper reading). Our exclusion criteria aimed at fulfilling the scope of the article, thus, we only included articles analysing current cross-border co-operation protocols and methods from a critical perspective, discussing challenges and/or ways to overcome them.

After collecting all the relevant sources and applying our methodology, 103 research articles passed the title and abstract screening. From these, 80 were discarded after a full review, leaving 23 research articles in the scope of our article, which were complemented with 13 sources selected from grey literature. Note that the main focus of the research methodology described in this section is to identify the current challenges of cross-border co-operation and thus, the extracted literature is analysed in 'Literature Review and Challenge Extraction'. A summary of the different steps of the bibliographic analysis is depicted in Fig. 1.

Analysis and reporting

The thematic content analysis enables the descriptive presentation of qualitative data and, therefore, helps researchers identifying, analysing, and interpreting patterns of meaning (or 'themes') within qualitative data [6]. We have adopted a thematic content analysis approach for deriving research areas and common themes from the eligible literature. Due to the nature of some of the reviewed literature (e.g. law-related articles, as well as articles not following well-

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

Table 1: Summary of research questions and the corresponding sections devoted to answer them

Research question	Objective	Section
Which are the current tools, procedures, and protocols for cross-border evidence exchange amongst European countries/jurisdictions?	The objective is to summarize the current instruments used between Europe and other countries to leverage cross-border investigations	Main Instruments for Cross-Border Investigations in Europe
Which are the main challenges related to cross-border investigations?	The purpose is to collect and summarize the main challenges found in the literature and discuss them	Literature Review and Challenge Extraction
Are current practices efficient enough to counter the sophistication of cybercrime?	The aim of this question is to understand whether current instruments and protocols are sufficient to efficiently fight cybercrime	Literature Review and Challenge Extraction and Discussion—Enhancing Cross-Border Collaboration
What technologies or strategies can be used to deal with the identified challenges?	According to the knowledge extracted from the literature, our plan is to identify the pain points of the actual state of practice to provide fruitful strategies against them.	Discussion—Enhancing Cross-Border Collaboration

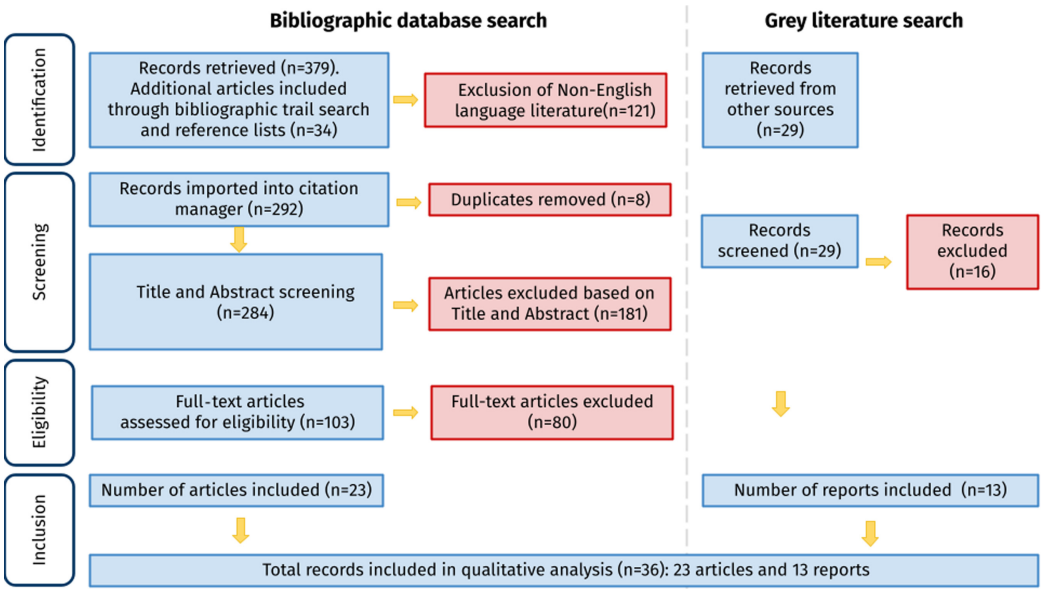

Figure 1: Flowchart of the search strategy.

established sectioning criteria) we combined a qualitative analysis software for the thematic content analysis of the selected literature (MAXQDA2020) with the classical screening and full text reading procedure. Moreover, findings were peer-reviewed by the authors. Next, we used various ways to synthesize the available literature to report the results of our study in a sound and comprehensive manner. For example, we present the main contributions of each article according to the subset of cross-border protocols analysed, and we extract their challenges in a global manner to derive further discussion.

Main Instruments for Cross-Border Investigations in Europe

Created to address, with due respect for human rights, the legal challenges in criminal justice that emerged from the evolution of technology and telecommunications, the Budapest Convention on Cybercrime of the Council of Europe is the most relevant international instrument on Cybercrime and Digital Evidence. Opened for signature in 2001, with currently 66 Parties spread around the world, its scope of application is not restricted to the borders of Europe. It aims to create a global framework on cybercrime and digital evidence among practitioners from a very diverse array of jurisdictions, facilitating international cooperation in criminal cases, with substantive and procedural provisions. This legal framework includes provisions for collecting digital evidence in emergencies, directly from service providers, with extra-territorial powers and on international cooperation. More than 20 years have passed since the drafting of the Budapest Convention, but its criminal substantive aspects, technology neutral in their provisions, remain fully updated. However, in relation to the provisions that support the operational work of Law Enforcement and Judicial Authorities, in view of new introduced technologies such as Cloud Computing and its impact in territoriality and jurisdiction, specific solutions were needed and brought forth by a second Additional Protocol to the Budapest Convention, approved in November 2021 [7].

In response to the identified challenges related to cross-border gathering and sharing of digital evidence, the recently approved second Additional Protocol [8] presents new provisions on disclosure of domain name registration information, direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

emergencies, and a specific provision on Joint Investigations Teams (JITs)[1]. The text was opened for signature in Strasbourg on the 12th May 2022. Other very relevant EU legal instruments for lawful collection of electronic information in cross-border investigations are the Mutual Legal Assistance Treaties (MLATs), and the European Investigation Order (EIO), which replaced MLATs in the context of a subset of participating EU members (EU members except for Denmark and Ireland [9]). These co-operation instruments rely on the independent judicial scrutiny of the competent authorities in the different countries to guarantee that the corresponding investigation requests and retrieved information are lawfully obtained during investigation processes.

The EIO aims to speed up the co-operation by extending the principle of mutual recognition in evidence gathering. Thus, EU participating member states and their corresponding judicial authorities are entrusted with the task of checking the legitimate grounds to either refuse or execute an EIO. An interesting feature of the EIO Directive is that, in conformity with the EU Charter on Human Rights art 47, allows for the Defence, as well as the victim's lawyer, to request a Court to issue an EIO to obtain digital evidence. This possibility enables lawyers, in equal arms with Prosecution Services, to seek access to the electronic data before it is deleted by requesting the issue of an EIO within the framework of applicable rights of suspects and victims. The latter exists in conformity with the national criminal procedure or directly in the competent court of the issuing state [10].

The MLAT process is the most used international co-operation protocol (i.e. MLAT also covers cases in which some of the EU members that want to co-operate are not bound by the EIO Directive). Thus, an MLAT is used to request data residing in countries such as Denmark, Ireland, as well as non-EU countries such as the USA or Japan. The main issue with the MLAT requests is that it may be stalled in many steps of the process. For instance, such a procedure was designed before the consolidation of the Cloud as the primary storage platform of most decentralized services on the Internet. Hence, due to this paradigm shift, the increase of cyberthreats that required cross-border co-operation hindered the efficacy of MLATs. As a consequence, the MLAT is currently regarded as an insufficient method to cope with actual needs due to its slowness and the resources that it requires.

To reduce the burden and speed up the acquisition of electronic data that law enforcement and judicial authorities need for investigating and successfully prosecuting criminals and serious crimes such as terrorism, the EU Commission created the E-evidence initiative, which consists of two main tools, the European Production Order (EPROD) and the European Preservation order (EPRES). The EPROD allows a judicial authority in one Member State to obtain electronic evidence directly from a service provider or its legal representative (thus, entails the creation of such a figure in each corresponding service provider) in another Member State [11]. The EPROD imposes a very strict response time (within 6 h in case of emergencies and to a maximum of 10 days, compared to 120 days in the case of EIO and an average of 10 months for MLAT). The EPRES allows a judicial authority in one Member State to request that a service provider or its legal representative in another Member State preserves specific data given a subsequent request to produce this data by using either an EPROD or an EIO. A parallel instrument with a similar aim was created in the USA, namely the Clarifying Lawful Overseas Use of Data (CLOUD) Act [2]. One of the most relevant aspects of the CLOUD Act and the E-evidence initiatives is their impact on the actual landscape since most technology corporations are based in the USA and EU. Therefore, since both initiatives deviate from the principle by which the physical location in which data are stored determines jurisdiction, and both determine that in specific cases, law enforcement officers should be able to directly access a provider's data under their corresponding jurisdiction without needing an MLAT [12]. Therefore, their application could change the cross-border investigation paradigm.

As noted in the literature, a series of questions are raised as to the E-evidence, and the CLOUD Act's compatibility with current legal frameworks in relation to privacy, human rights, and the necessity and proportionality principles of the requests made in the context of cross-border investigations [11, 13]. A clear example of the complexity of the challenges in relation to the E-evidence initiative is the still ongoing trialogue between the EU Commission, Council of the European Union, and European Parliament for the approval of the E-evidence Package. In the case of US–EU co-operation, the E-evidence initiative could require US-based online service providers (OSPs) to grant access to data in their possession. At the same time, the Stored Communications Act (SCA[3]) forbids the provision of such access, unless there is an executive agreement with the USA. On the other side, when US authorities request data stored in the EU, companies may risk breaching the EU General Data Protection Regulation (GDPR) under Article 48, since any judgment or decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable if it is based on an international agreement, such as an MLAT. Moreover, Article 46 of the GDPR also hinders the execution of data exchange procedures on the European side if there is no mechanism allowing European individuals to have the safeguards and legal remedies comparable to those resulting from the GDPR [11, 14].

Table 2 summarizes the main cross-border investigation instrument and their jurisdictional applicability. Moreover, Fig. 2 shows the different collaboration flows according to each instrument. For a profound analysis of the main co-operation instruments between different countries, we refer the reader to [10, 11, 14–16].

Beyond the current adopted measures described above, it should be highlighted that by acknowledging the pains and gaps of digital evidence exchange, the international community is making an attempt to harmonize these procedures. Therefore, the proposal for a United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes is currently being discussed. This discussion, currently being carried out by an Ad Hoc Committee[4] created in December 2019. The Convention, still at an early stage of development, has a focus on state sovereignty and non-intervention. In addition to criminal justice related topics, it aims to cover certain aspects related to Internet governance, cybersecurity, obligations to private sector, and involvement of the International Telecommunication Union (ITU). It is also introducing new computer-related or cyber-enabled offences such as digital data to mislead users, incitement to subversive activities, terrorism, extremism, drugs, and arms trafficking. The negotiations appear to be very complex to develop and no date is previewed for their conclusion.

1 JITs are a tool in international cooperation in criminal matters, created by a legal agreement between competent authorities of two or more States for the purpose of carrying out criminal investigations, established for a fixed period, usually 12–24 months, as needed to conclude the investigation.

2 https://www.justice.gov/dag/cloudact

3 (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712)

4 Resolution 74/247 adopted by the General Assembly on 27 December 2019.

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

Table 2: Main EU legal instruments for channelling cross-border requests for data gathering in criminal proceedings

Protocol/ co-operation tool	Description and applicability
CoE cybercrime convention[a]	66 countries[b]
EIO[c]	EU excluding Ireland and Denmark, since 2014.
MLAT within EU[d]	Member States of the European Union (special rules apply for Ireland, Norway, Luxembourg, and Iceland), 2000
MLAT between EU and third countries	For example, MLAT with Ireland[e] (2008), MLAT EU-Japan[f] (2009), and MLAT with US[g] (2003).

[a] Convention on Cybercrime of 2001 (ETS No. 185).
[b] https://www.coe.int/en/web/cybercrime/parties-observers.
[c] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014.
[d] Mutual Legal Assistance Convention (between Member States of EU) Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C.
[e] https://revisedacts.lawreform.ie/eli/2008/act/7/revised/en/html.
[f] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:22010A0212(01).
[g] EU–US Agreement on Mutual Legal Assistance (MLA) Agreement of 25 June 2003 on mutual legal assistance between the European Union and the USA.

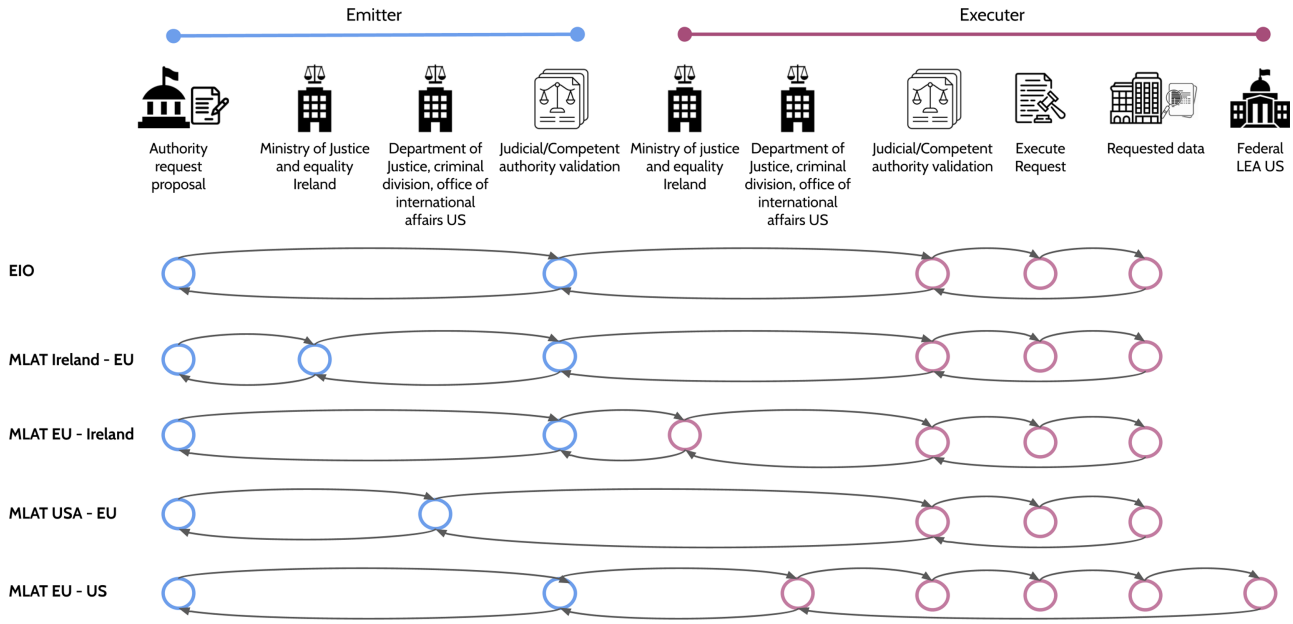

Figure 2: Main flow of each collaboration instrument and the corresponding institutions and authorities involved.

Literature Review and Challenge Extraction

In this section, we analyse the literature collected following the methodology described in 'Research Methodology'. For each article, we extract the challenges and group them in a higher level of abstraction, when possible, to provide a more comprehensive perspective of the current state of practice.

Several articles [11, 14, 16–19] recall the issues of MLAT and EIO systems and analyse recent initiatives designed to overcome most of them, namely the CLOUD Act and the E-evidence framework, and highlight the current constraints of this novel proposed legislation and the legal and ethical conflicts across EU and other countries such as the USA. In [20], the authors recall the inefficacy of actual protocols such as MLATs for distributed and highly volatile data in cross-border investigations and highlight the current challenges for collecting evidence from cloud service providers. Similarly, in [21], authors discuss the technical issues of cross-border investigations due to the decentralization of data and the conflicts between EU and US resulting from, e.g. GDPR, which prevents the indiscriminate data request from US to EU providers, recalling the case of Microsoft Ireland. In [22], the authors analyse current cross-border frameworks' issues from a technological and forensics perspective. In [23], the authors focus on the benefits and drawbacks of the E-evidence initiative. In [24], the authors highlight the current issues towards achieving harmonization and the difficulties for establishing an equivalent, fluent collaboration between parties using different legislation and definitions, which is crucial to guarantee an effective and timely prosecution. The article presented in [25] discussed the main issues of EIOs, including an analysis of incoherent definitions affecting the compatibility between legal systems of different countries.

Some articles focus on tools to complement or substitute the EIO. For instance, [26] compares the EIO with the Joint Investigation Team (JIT) as tools to ease cross-border investigations. Notably, JIT enables more flexibility to specific investigations regarding the number of authorities implied and their corresponding evidence exchange, yet it requires more coordination and the corresponding agreements between parties. The article presented in [27] discusses the issues of cross-border access to evidence from the EIO and the

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

E-evidence perspective. Moreover, the author analyses data collected from two surveys among practitioners, showcasing existing obstacles of current frameworks. In [28], the authors analyse two tools for judicial co-operation in criminal matters in the EU: the EIO and the proposed European Public Prosecutor's Office (EPPO) [29], showing the lack of standardized mechanisms of the EPPO. Thus, given the considerable differences between the national legal systems, the consistency of the EPPO investigations and their admissibility in court require complex rules for mutual admissibility of evidence that may not be realizable.

Other authors focus on specific parts of these frameworks. In [30], the authors analyse the different data categorization schemes of current evidence exchange frameworks, namely, EIO, E-evidence, and the CLOUD Act, highlighting the need for harmonizing and updating the different definitions and types of data. The latter is critical to ensure that the proper data requests are issued to fit the purpose of the investigation, being compliant with legislation. The authors propose a set of data categories to minimize the incoherence among such frameworks. Similarly, a review of the main challenges to adopting novel directives, especially in terms of data categorization and the related legal issues, is presented in [31]. The issue of data ownership in distributed systems is analysed in [32], where authors recall the power of disposal as a possible solution to ease and speed up the data collection procedures in distributed systems while recalling the current issues of the EIO in that regard. The article in [10] provides a guideline for the different actors participating in cross-border investigations by analysing the existing frameworks aiming to enable criminal justice co-operation. In [33], the authors discuss the difficulties and lack of harmonization in regards to the evidence categorization and classification necessary to establish standardized procedures and enhance collaboration between different organizations. In [34], the authors discuss the applicability of the speciality rule in the EIO that enables the use of evidence gathered in the context of an investigation to be used for other purposes. Notably, despite the ambiguities that could prevent the effective use of such evidence, the EIO does not provide strict prohibitive measures, thus aiming at a path of free movement of evidence in the EU. Since the E-evidence framework is far more restrictive at that level, the EIO is usually preferred, yet such "freedom" can be misused to circumvent legal prohibitions.

The work presented in [35] discusses the law updates of different EU countries to cope with new technologies. Moreover, it discusses several vague directives of the Cybercrime Convention Committee (T-CY) proposed in April 2013 [5] with particular attention to the exact location of the data to be seized. The authors discuss the desirability of a regulation that stipulates that access to stored computer data should be possible regardless of where the data are located if specific cumulative requirements are met (e.g. the exact location of data is not known, the evidence has to be retrieved in a lawful and proportionate manner, and for specific purposes) to solve ambiguous/uncertain situations, including the cases where anonymizing tools (e.g. The Onion Router—TOR) are used. In the context of financial crimes, [36] analyse the mutual recognition of freezing and confiscation orders, which work in conjunction with other EU mutual recognition instruments such as the European Arrest Warrants and the EIOs to speed up the enforcement of financial-related orders in all member states.

In [37], the authors use a sound methodology to create 10 use cases and collect the challenges related to knowledge sharing between organizations across international boundaries. The authors classify such challenges and provide some recommendations to overcome them.

Several articles discuss specific international collaborations and their impact on liaising with the EU. For instance, [38] analyses the benefits and challenges of the bilateral co-operation between Finland and Russia, which is based on the Treaty on Crime Prevention co-operation between the governments of Finland and the Russian Federation (1994). The authors highlight that the practical challenges in such bilateral agreements overlap with those observed in other multilateral agreements at the EU level. Recent Brexit-related issues are discussed in [39] along with current mutual recognition instruments, which will have to be redefined to maintain the EU–UK co-operation. In the US context, [40] analyses the extraterritorial enforcement to electronic evidence issues with a particular focus on the Microsoft Ireland case. In [41], the authors raise the concern of using dubious tools by the US government to collect evidence (with particular focus on the dark web) in foreign countries and their legal implications. In [42], the authors discuss the issues faced by the judiciary system, prosecution, and other actors involved in foreign and cross-border investigations from the US perspective. They provide some insights on how to overcome and/or minimize them. Similarly, the authors in [43] recall the issues regarding the applicability of the suspects' rights when there are conflicts between different jurisdictions, focusing on the US Fifth Amendment. In [13], the authors analyse the primary forms of cross-border data sharing with the USA, namely, letters rogatory, MLATs, and executive agreements authorized by the CLOUD Act, and highlight the benefits and limitations of the CLOUD Act compared with the other two previous protocols. Similarly, in [12] the authors examine the impact, the opportunities, and the adequacy of the US CLOUD Act concerning other international governments.

After collecting the challenges from the reviewed literature and comparing them with public information collected from judicial and law enforcement authorities [15], we have categorized them as seen in Table 3. Thereafter, we mapped each challenge with the corresponding articles where they are discussed in Table 4. We observe that one of the most recalled challenge is the timely collection and sharing of evidence in the context of MLATs and EIO, which is especially relevant in cases where data is highly volatile [15, 24, 46, 47]. In this regard, one strategy to enhance the efficiency of MLATs is to provide more descriptive definitions about data requests and to increase transparency of all parties involved in the whole procedure [14, 24]. Another strategy proposed in the literature is to deploy specialized personnel and national contact points to establish the necessary agreements between different legal systems [11]. The latter is related to another struggling challenge: the lack of resources for cross-border collaborations, which is critical since the proper training of personnel and the enhancement of their technical skills are crucial to guarantee quality and timely investigations. Notwithstanding, beyond finding qualified personnel, the budget devoted to this goal has to be enough to guarantee not only the engagement of professionals but also to provide them with the proper tools and equipment [11, 14, 37].

The lack of automated mechanisms to speed up cross-border investigations and the auditability of the interactions and collected evidence are two challenges that require the use of tools with verifiability and auditability capabilities [47–49]. Moreover, there is a need for defining standardized procedures, even if it is at a bi-lateral level so as to speed up the interactions and increase trust among organizations [14, 16]. There are some examples of tools aiming at easing cross-border collaboration, such as the e-CODEX [50] system, which enables both requests and evidence to be exchanged securely between judicial authorities. Similarly, the e-Evidence Digi-

5 Council of Europe Cybercrime Convention Committee (T-CY): (Draft) Elements of an additional protocol to the Budapest convention on cybercrime regarding cross-border access to data (9 April 2013).

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

Table 3: High level abstraction and description of the challenges identified in the literature

Challenge	Description
Data location and individuals' control over their own data	This challenge recalls the difficulty to establish the exact location(s) and existing copies of each individual's data, who has access to it, and on which grounds. For instance, proposals such as the E-evidence are not clear towards this aspect and introduce uncertainty.
Timely collection, analysis, and sharing of evidence	In this category, we include issues related to the fact that nowadays investigations may require the processing of vast amounts of data, along with its volatile nature. The latter is aggravated due to the inefficacy of MLAT and EIO frameworks, which may not accommodate the necessary speed or provisions to facilitate evidence collection.
Lack of harmonization in rules of admissibility of criminal evidence and prosecution	The lack of clear and common legislation regimes and standards across different states in relation to data retention, the gathering and validity of digital evidence versus the procedural rights of potential suspects, may hinder the applicability of the EIO directive due to jurisdictional constraints (especially in the case of protocols that do not require an independent judiciary validation). This situation, apart from the potential creation of inconsistent prosecution scenarios may be exploited by criminals using jurisdictional arbitrage tactics in cases of remarkable differences among states.
Lack of compatibility between different protocols regarding data categorization and definitions	This category includes the issues related to communication between different jurisdictions or states, in which potential incompatibilities regarding data categorization and related definitions may arise. The latter could create conflicts when applying the appropriate legal standards and procedures when requesting and processing new evidence, which could entail delays and even affect the validity of evidence in court if the proper procedures were not followed.
Direct cooperation with service providers and equality of opportunities	This category includes several issues related to the user's side and the equality of legal rights and opportunities. For instance, in the context of novel protocols such as E-evidence, the lack of information and procedural details hinders the refusal of a production or preservation order. More concretely, individuals and private companies' representatives may lack clear indications where and to whom to bring their claims or assess whether the petition satisfies law requirements regarding judicial independence.
Incompatibility conflicts between jurisdictions that may violate procedural rights and safeguards	Non-judiciary mediated orders (i.e. orders directly issued from police or prosecutors such as the ones foreseen in the case of E-evidence and CLOUD Act) lower the standards previously necessary to obtain evidence in cross-border criminal investigations and prosecutions. Note that the information obtained during investigations has to be specific to ensure defence rights in criminal proceedings, including the basis for the request, how the search was done, and how the data was analysed by investigating/prosecuting authorities. Moreover, specific bi-lateral incompatibilities arise between the CLOUD Act and EU (CLOUD Act breaches Article 48 of GDPR), and the E-evidence and US (the E-evidence may require data for which access is forbidden by the US Stored Communications Act). The latter issues are exacerbated by further incompatibilities between the legislation of different states, which may hinder international co-operation and its judicial robustness.
Lack of automated mechanisms to efficiently collect and report requests	Generally, EU member states do not have a unified system for collecting and reporting information related to issued/received cross-border data requests, channels/instruments used, and related outcomes. There are essential transparency deficits regarding how data requests are issued, transmitted, and executed by competent national authorities.
Auditability in data collection procedures	This category recalls data collection and management issues during investigations. In this sense, most current mechanisms lack standardized procedures to ensure that data gathering is consistent with national and/or fundamental international rights and the rule of law standards that apply to criminal investigations so that evidence is admissible in court. Moreover, post-investigation management of evidence is not properly tackled in approaches such as the EIO. For instance, EIOs do not deal with the use of outcomes obtained from shared evidence and the possibility to further share them with other parties or use them in other investigations.
Lack of resources related to equipment and training of law enforcement and judicial authorities to support direct co-operation between different jurisdictions	There is a lack of resources and efforts for training personnel to support the investigations both in the technical and the legal aspects, including information about the applicable rules and procedures considering the particularities of different legal systems.
Data retention issues	Considering the already mentioned needs for digital evidence in criminal investigations the availability of information is crucial to criminal investigations, however, quite often, the required digital evidence is in the possession of telecommunications service providers and therefore, retention of non-content communications data is a very relevant issue to be considered by public authorities.

tal Exchange System (eEDES) [51] aims to establish a secure and decentralized platform in Europe to ease communications and evidence exchange, particularly in the context of EIO and MLAT cross-border investigations. Another relevant measure at the international level is INTERPOL's e-MLA initiative [52], which aims to develop a platform for collaboration and Mutual Legal Assistance (MLA) exchanges. A nice addition to these tools could be to leverage the prosecution of criminal activities by using Eurojust's recommendations [53]. These recommendations offer the legal framework to decide, in the case of a criminal activity, i.e. being prosecuted in different member states, which of them is in a better position to undertake an investigation or prosecute specific acts, avoiding duplicated efforts and reducing the investigations overhead. Complementary to the tools, a more in-depth focus on the different modes of collabo-

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

Table 4: Relation of challenges discussed by each corresponding article

Challenge	Reference
Data location and individuals' control over their own data	[11, 19, 22, 32, 41]
Timely collection, analysis, and sharing of evidence	[10–14, 16, 17, 19–21, 23, 24, 26–28, 31, 36, 40, 41, 44]
Lack of harmonization in rules of admissibility of criminal evidence and prosecution	[16, 21, 22, 25, 35–37, 39, 42, 43, 45]
Lack of compatibility between different protocols regarding data categorization and definitions	[27, 30, 31, 33, 35, 37, 38, 42]
Direct cooperation with service providers and equality of opportunities	[10, 11, 14–16, 27, 41–43, 46]
Incompatibility conflicts between jurisdictions that may violate procedural rights and safeguards	[11–14, 16–19, 21, 23–25, 27, 32, 34, 37, 38, 40–45]
Lack of automated mechanisms to efficiently collect and report requests	[16, 20, 37]
Auditability in data collection procedures	[10, 11, 20, 25, 34]
Lack of resources related to equipment and training of law-enforcement and judicial authorities to support direct co-operation between different jurisdictions	[10, 16, 18, 24, 27, 31, 36–38]
Data retention issues	[10, 14, 15, 46]

ration among organizations is critical, since understanding organizational differences and establishing good relationships with policing organizations is critical to enhance the mutual trust [37]. In this regard, one of the current issues is the proper regulation and definition of data types and their possible categorization to facilitate the efficacy of MLATs, and cross-border co-operation [24,30]. The latter is crucial in financial crime investigations in which the need for more transparent monitoring of virtual assets (including the possible establishments of central bank account registries) and auditable data collection procedures are mandatory to enforce the corresponding required orders [36].

Although judicial cooperation instruments remain essential mechanisms to obtaining electronic evidence, especially when gathering content data, they are deemed too slow to share electronic evidence effectively. In order to obtain data more swiftly, keeping up with a constantly evolving digital landscape and a fragmented legal framework, public authorities seek direct cooperation with OSPs. Such a collaboration path is not without difficulties, due to a very diverse array of potentially applicable rules, the need for taking into account the internal procedures of OSPs and consequent uncertainty for public authorities, citizens, and the involved private entities. For instance, users, companies or industries may be forced to accept requests by default to avoid possible sanctions. In addition, defendant lawyers lack mechanisms to issue a data collection procedure (this is only foreseen in the EIO framework), so they do not possess the capabilities to request data that could be used as evidence to properly exercise the defendants' rights. Moreover, conflicts may arise in cases where the law provides suspects with specific rights which are not foreseen in other countries. Currently, the Eurojust/Europol supported SIRIUS Project helps judicial and law enforcement authorities in this pursue, by creating a repository of applicable procedures and publishing a yearly report [15] on the status of obtaining digital evidence from OSPs.

Several challenges have been highlighted in relation to the automation of communication and evidence sharing in the context of cross-border collaborations. Although a single tool that could enable the automation of all the required procedures would be desirable, the difficulties of building such a highly granular tool are daunting. Nevertheless, when approached individually, several technologies could ease the automation of such tasks. For instance, blockchain and smart contracts could provide enough guarantees to automate investigation requests, which would be digitally signed and audited. In the case of evidence collection, similar procedures could be used, exploiting the existing tools leveraged to collect evidence and enhancing them with the tamper-proof capabilities of blockchain, the use of hashes, and encryption. Furthermore, such tools could be linked with local jurisdictions systems through APIs. More details on the benefits of blockchain are given in 'Discussion—Enhancing Cross-Border Collaboration'.

Data localization policies have been extensively discussed in the literature as a strategy to reduce the burden of data acquisition both in terms of legal requests and the related technical issues [14, 17]. For example, it is often unclear which jurisdiction determines the applicable procedural framework that regulates the gathering and validity of digital evidence as well as to which jurisdiction EIOs or MLAs should be sent [15, 46]. However, data localization has several drawbacks, such as threatening the privacy of individuals should data be stored in jurisdictions under the control of governments with weak human rights protections. The latter could also cause conflicts of law and hinder the resolution of cross-border investigations. Moreover, modifying the decentralized nature of such systems would affect their security, resiliency, and performance. Last but not least, data localization has economic factors preventing its practical application, such as limiting the exploitation capabilities of the involved organizations, which results in the organizations' reluctance to adopt data localization policies [20].

The access to that data by JA/LEA, inevitably triggers discussions about balancing the right to privacy and secrecy of communications with the need for ensuring public security and effectively tackling serious crime. The Court of Justice of the European Union (CJEU) has taken the approach to set limits on data retention regimes and impose access conditions to retained data since 2014, when the CJEU declared the 2006 Data Retention Directive to be invalid. More recently, the Court has admitted exceptions to those rules [54–56] and the possibilities for OSPs to retain data and for public authorities to use that data in criminal processes are part of an increasingly complex framework.

Discussion—Enhancing Cross-Border Collaboration

Current activities and related projects

The European Commission has granted several projects aiming to provide solutions for cybercrime prevention and prosecution, and facilitate common procedures in the management of digital evidence. Thus, in this section we examine the extent to which the EU has promoted initiatives aimed at increas-

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

ing the security level of the actors involved in the fight against cybercrime.

With the aim to provide solid results of the above-mentioned topic, we used the EU's CORDIS [57] database to perform our search as it stores the information and public deliverables of all EU-funded projects. The two searches performed consisted in:

- Finding projects listed with fields 'criminology' or 'law enforcement'. Therefore, the search consisted in ((criminology OR law enforcement) AND status == SIGNED) in all projects' category with an all-years timespan from 1990 to 9th February 2022. The query, after eliminating duplicate entries, returned 72 projects. Projects not focused on digital crime, not providing frameworks to facilitate investigation procedures, or tools to empower law enforcement bodies were rejected by consensus. Thus, 23 references were accepted in the qualitative synthesis.
- Finding projects granted under the H2020 framework with call identifiers 'H2020-FCT-2014-2015', 'H2020-FCT-2016-2017', 'H2020-SU-SEC-2018', 'H2020-SU-SEC-2019', and 'H2020-SU-SEC-2020'. From the 132 obtained results, projects found in the previous search or not focused on digital crime, investigation procedures, or tools aiming to improve law enforcement capabilities against cybercriminals were rejected by consensus. Consequently, 16 projects were finally accepted in the qualitative synthesis.

The identified records, listed from the most recent starting date, are depicted in Table 5. The table provides the scientific field of the project, the project acronym, the starting, and the ending dates.

From the 39 projects included in the analysis after the screening, two main groups were identified: *Cross-Border Governance and Enforcement Services*, and *Tool-kits Development for Law Enforcement*. We discuss each category next.

Cross-border governance and enforcement services

The projects classified under this category aim to provide frameworks and procedures to address the lack of common regulations and the several disparities associated with criminal prosecution. Also, these projects bring new tools to empower law enforcement and judiciary bodies in their fight against all forms of digital crimes.

In an attempt to improve the protection of victims of human trafficking and child sexual abuse, HEROES and GRACE will provide technology to build bridges and facilitate cross-border coordination amongst law enforcement agencies, prosecutors, judges, and civil society organizations. In particular, GRACE will counter the spread of online child sexual exploitation material with the deployment of advanced analytical and investigative mechanisms. Results will be implemented by Europol and used by European LEAs. In this line, LOCARD will use machine learning (ML) algorithms to develop tools seeking for potential pedophile behaviours on social networks. Moreover, the platform provided by LOCARD aims to guarantee the integrity and transparency of the cross-jurisdictional chain of custody with blockchain technology. A similar objective is also shared by CREST that will implement the same technology to manage and deliver court-proof digital evidence. The project will deliver a platform to help LEAs fighting cybercrime in IoT ecosystems, autonomous systems, and targeted technologies. Not with blockchain but aiming to improve cross-border exchange of information, SHUTTLE will deploy a toolkit in accordance with the ISO17025 fostering, therefore, the use of a common methodology across European countries. Also, the increasing involvement of mobile phones in cybercrimes led the EU to invest in FORMOBILE and EXFILES projects. Whilst FORMOBILE will provide tools to facilitate investigations in mobile devices and develop a standard to homogenize forensic workflows, EXFILES will focus its efforts on the data extraction of encrypted files. Not focused on mobile devices but on providing a comprehensive picture of the presented evidence, the already ended project SPIRIT brought capabilities for LEAs across the investigation workflows and empowered them in criminal investigations. In particular, the project developed heterogeneous relationships on social graphs and provided privacy by design tools to enhance the acquisition and analysis phases of the investigation.

The improvement of law enforcement interactions using artificial intelligence (AI) tools represent a main objective for the EU project, pop AI. The project will increase trust in AI by building an ecosystem comprising several European LEAs. Similarly, ALIGNER and LAWGAME will allow relevant European actors to identify and discuss needs to develop AI tools aiming to support, train, and empower law enforcement bodies. From a different perspective but also aiming to foster dialogue amongst judiciary forces, and all actors involved in the investigation process, CYCLOPES and PROTAX will seek to connect with the most relevant European and international bodies, build bridges between industry and academia, and face the current challenges associated to fighting cybercrime (i.e. procedures, training, or standardization). Whilst CYCLOPES is focusing its efforts on building and maintaining a network of LEAs, PROTAX has also involved tax authorities to improve the prevention and prosecution of tax crimes. In this line, the EU projects I-LEAD and ILEAnet stand for building solid and sustainable LEA networks focused on research and seeking for innovative needs. Although I-LEAD will provide recommendations to improve standardization procedures, ILEAnet will establish a network of LEA practitioners to foster innovation and share best practices across the community. Also, the EU project COPKIT has developed a platform to address issues related to the investigative processes of LEAs (i.e. analysis, investigation, mitigation, and prevention). A panel of end users and stakeholders (led by EUROPOL) aim to ensure the coherence of the results. Similarly, ROXANNE will provide tools with shared intelligent and speech processing technologies to help LEAs make decisions in situations of high-levels of pressure. Moreover, the shared intelligent platform developed by INSPECTr will provide a novel process to help law enforcement in predicting, detecting, and managing crimes at national and supranational levels. Finally, ASGARD, a project ended in 2020, built a sustainable community (comprising LEAs and actors of the research industry) aiming to develop tools to extract, exchange and analyse large volumes of data for forensic investigations. Moreover, the project performed several actions to foster the interaction among stakeholders and enhance trust.

The disparities and complexity of new tools to enable a better management of digital investigations for LEAs, might increase the need for skilled experts to investigate cybercrime cases. Thus, the TUECS project will face this gap by providing stakeholders an innovative governance theory to foster public and private partnership while reducing their cooperation costs. Also, the high demand for security experts to fight cybercriminals has also been addressed by ESSENTIAL. With the implementation of a broad range of research topics, the project will provide effective security and interdisciplinary training campaigns to relevant experts and professionals.

The international nature of most criminal cases fosters the need for developing regulations led by authorities located around the globe. Although JustSites is not purely focused on digital crimes, this EU project will study the most relevant locations of international criminal authorities contributing, therefore, to a better understanding of their role and influence in criminal prosecutions.

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

Tool-kits development for law enforcement

The large number of tools used by LEAs and actors involved in judicial processes along with their technical limitations, frequently lead to inefficient investigation procedures. Thus, with the aim to build stronger, more resilient, and effective prosecutions, the development of tools to help LEAs must address the above mentioned challenges and provide the latest technology and innovative features. The previous section was focused on projects aiming to develop tools and foster standardization, participation, and coordination of European police forces across the Member States, whereas this section provides a summary of projects, granted by the EU Commission, seeking to undertake strong research programs and develop innovative tools with the most relevant technological advances and benefits for LEAs.

With the participation of ten different LEAs, practitioners and combining several fields of expertise (i.e. technology, sociology, psychology, linguistics, and data science), the PREVISION project provides a platform to face the most relevant cross-border security challenges. Likewise, the innovative research program, iCrime, will explore the different pathways of cybercrime offenders. The project aims to improve the understanding of cybercrime markets from social and economic perspectives. Using a different approach and after consulting the needs of several European LEAs, MAGNETO has developed sophisticated solutions and tools to address the lack of heterogeneity and other problems arising from the use of massive volumes of data.

Based on the fact that cybercriminals are improving data hiding methods (e.g. steganography) to perpetrate their malicious activities, UNCOVER seeks to provide LEAs with tools committed to bridge the gaps left open by commercial solutions (e.g. limited number of hiding methods, slow performance, or lack of confidence). The solution will consider users' operational needs, regulations, and chain of custody considerations. Similarly, the already ended project RAMSES combined scraping techniques of public and deep web to bring the latest advances in an intelligent steganalysis software platform to detect manipulation in images and videos. The platform could detect and track malware payments and extract and analyse malware samples using Big Data algorithms. In this line and aiming to enhance the collaboration amongst the many actors involved in the prosecution of a crime, APPRAISE will bring together representatives from a wide range of disciplines (i.e. technology, psychology, and sociology) and society to overcome the several complexities of fighting against cybercriminals. Also, aiming to foster data exchange and communication amongst LEAs, PROACTIVE will support the EU Action Plan for Chemical, Biological, Radiological, and Nuclear (CBRN) threats by providing innovative tools to improve the response capacities of policymakers, security professionals, and the civil society. Likewise, TRACE and AIDA will provide solutions to identify, track, and document all actions performed in investigation workflows. Whilst TRACE is focused on illicit financial flows (IFFs), AIDA addresses cybercrime with tools using data mining and analytics solutions. Similarly, by combining augmented reality and ML algorithms, DARLENE and INFINITY will provide solutions to improve LEAs decision-making preventing, therefore, criminal activities. In this line, the EU projects CounteR and INDEED will develop tools and capabilities to counter radicalization in Europe and encourage LEAs to undertake coordinated actions. Also, aiming to improve the understanding of the psychological dimension of cybercriminals, CC-Driver will perform a thorough research on human factors leading to all forms of cybercrime and will deliver tools to prevent, investigate, and mitigate cybercriminal behaviour. Results will maximize potential victims' protection and contribute to more effective training campaigns.

The identification of perpetrators using DNA analysis has several limitations in forensic investigations. With the aim to address these challenges, VISAGE provides a toolkit with intelligence information on appearance, age, and ancestry to construct composite sketches (of unknown trace donors) from traces recovered at crime scenes. A set of tools was also deployed by VICTORIA that developed a Video Analysis Platform (VAP) to address the lack of maturity related to video investigation tools.

'*51% of EU citizens feel not at all or not well informed about cyber threats and 86% of Europeans believe that the risk of becoming a victim of cybercrime is rapidly increasing*'. This conclusion was highlighted in RAYUELA [58], a project seeking to educate young people in the use of the Internet, therefore, preventing and mitigating cybercriminal behaviour.

Other relevant projects

Projects described in the previous section have been extracted from CORDIS. This database provides a comprehensive and structured public repository with all the information on projects whose funding, totally or partially, comes from the European Commission. However, there are other initiatives promoted by European institutions that, due to their relevance and potential impact, are worth mentioning.

With the participation of Europol, Eurojust, and the European Judicial Network, the SIRIUS project [59] aims to provide guidelines on specific OSPs along with investigative and analytical tools developed by Europol and the Member States. Moreover, the project would facilitate exchange of information and experience sharing amongst all parties involved in cybercrime prosecutions. In parallel, the Council of Europe is also playing a relevant role in the fight against cybercrime. Besides the already mentioned Cybercrime Convention, which the CoE has been developing and promoting through the Octopus Project [60] over the years, the institution is also promoting other initiatives like GLACY+, iPROCEEDS-2, CyberSouth, or CyberEast seeking to improve cybercrime investigations in the international arena.

Funded by the European Commission, the European Cybercrime Training Education Group (ECTEG) [61] provides training and education material to build law enforcement capacity on issues related to cybercrime. Amongst its most relevant projects, the Global Cybercrime Certification Project (GCC) seeks to create a common, international, and harmonized certification system for law enforcement agents and judiciary forces. Likewise, the DECRYPT project improves law enforcement continuous education by providing e-learning and classroom materials aimed at addressing encryption issues for decrypted materials to be admitted in a court of justice.

Finally, the already mentioned EVIDENCE2eCodex developed a useful instrument with legal validity to perform digital evidence exchanges related to EIO procedures. Likewise, the project developed a case aiming to show how electronic evidence could be shared through e-CODEX providing, thus, a secure and trusted environment to share information in criminal cases.

Commercial solutions—existing tools

Digital evidence management systems (DEMS) are the main commercial solutions to manage digital forensic investigations. In what follows, the most relevant DEMS available in the market are analysed and compared. To this end, several features of such DEMS have been considered, namely the mechanism to collect digital evidence, the reporting tools, the assurance of the chain of custody, the use of standards, and the compliance with regulations. Table 6 provides the relationship between the challenges and these features. The comparison

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

Table 5: Projects granted by the EU, ordered by most recently started

Fields of science	Project acronym	Start date	End date
Civil society; criminology; human trafficking; law enforcement	HEROES [62]	01/12/2021	30/11/2024
Ecosystems; civil society; artificial intelligence; ethical principles; law enforcement	pop AI [63]	01/10/2021	30/09/2023
Civil society; artificial intelligence; law enforcement	ALIGNER [64]	01/10/2021	30/09/2024
Public policies; law enforcement; ideologies	INDEED [65]	01/09/2021	31/08/2024
Virtual reality; law enforcement;	LAW-GAME [66]	01/09/2021	31/08/2024
Artificial intelligence; law enforcement; big data	APPRAISE [67]	01/09/2021	31/08/2023
Criminology; computer and information sciences; law enforcement	iCrime [68]	01/07/2021	30/06/2026
Monetary and finances; law enforcement	TRACE [69]	01/07/2021	30/06/2024
Criminology; law enforcement	UNCOVER [70]	01/05/2021	30/04/2024
Network security; law enforcement	CYCLOPES [71]	01/05/2021	30/04/2026
Data protection; social psychology; law enforcement; data mining	CounteR [72]	01/05/2021	30/04/2024
Ergonomics; law enforcement; Internet	RAYUELA [58]	01/10/2020	30/09/2023
Ecosystems; Internet of Things; law enforcement	DARLENE [73]	01/09/2020	31/08/2023
Law enforcement; data mining; terrorism; big data; deep learning	AIDA [74]	01/09/2020	28/02/2023
Software; criminology; mobile phones; law enforcement	EXFILES [75]	01/07/2020	30/06/2023
eCommerce	GRACE [76]	01/06/2020	30/11/2023
Artificial intelligence; law enforcement; big data	INFINITY [77]	01/06/2020	31/05/2023
Governance; forensic sciences; law enforcement	TUECS [78]	01/06/2020	31/08/2022
Ergonomics; criminology	CC-DRIVER [79]	01/05/2020	30/04/2023
Law enforcement; big data	INSPECTr [80]	01/09/2019	28/02/2023
Data protection; criminology; phonetics; law enforcement; natural language processing	ROXANNE [81]	01/09/2019	31/12/2022
Criminology; big data	PREVISION [82]	01/09/2019	31/12/2021
Ergonomics; ecosystems; law enforcement; terrorism	CREST [83]	01/09/2019	28/02/2023
Criminology; electrical engineering; mobile phones; forensic sciences; law enforcement	FORMOBILE [84]	01/05/2019	30/04/2022
Criminology;	LOCARD [85]	01/05/2019	31/07/2022
Civil society; law enforcement	PROACTIVE [86]	01/05/2019	30/04/2022
Planetary geology; criminology	JustSites [87]	01/01/2019	31/12/2023
Data protection; active learning; computational intelligence; law enforcement	SPIRIT [88]	01/08/2018	31/10/2021
Ecosystems; ethical principles	COPKIT [89]	01/06/2018	30/09/2021
Software; databases; bayesian statistics; colors	SHUTTLE [90]	01/05/2018	30/04/2022
Machine learning; virtual reality; criminology; ontology; law enforcement; data mining; terrorism	MAGNETO [91]	01/05/2018	30/04/2021
Data protection; ergonomics; taxation; criminology; law enforcement	PROTAX [92]	01/05/2018	31/07/2021
Law enforcement	I-LEAD [93]	01/09/2017	28/02/2023
Law enforcement	ILEAnet [94]	01/06/2017	31/05/2022
DNA; software; criminology; colors	VISAGE [95]	01/05/2017	31/10/2021
Data protection; mobile phones; optical sensors; computer vision; law enforcement	VICTORIA [96]	01/05/2017	30/11/2020
Law enforcement	ESSENTIAL [97]	01/01/2017	31/12/2021
Radio and television; law enforcement; data mining; big data	ASGARD [98]	01/09/2016	30/11/2020
Malicious software; criminology; forensic sciences; law enforcement; internet	RAMSES [99]	01/09/2016	30/11/2019

of 34 DEMS is summarized in Table 7. Concerning digital evidence collection, it is traditionally conducted manually by the investigator in charge of the criminal investigation. However, to shorten investigation times and optimize resources, further more automated procedures have already been considered, such as the use of public portals where citizens can upload potentially valuable resources for ongoing investigations, and the automatic collection of evidence by scanning the data stored in devices directly connected to the DEMS. Whereas manual procedures are implemented in all solutions, automated procedures are considered in only six (18%). The addition of automated mechanisms is a must in future solutions. Another popular feature of DEMS is the ability to create reports summarizing, among others, the insights acquired from the investigations to be presented in court, or the audit trails with the chronological set of records related to the investigations and their digital evidence. These tools are crucial to provide accountability for the entire investigation procedures, demonstrating that they have been conducted in a lawful, transparent and trustworthy way. Surprisingly, a fourth of the analysed DEMS do not provide any reporting functionality (9/34, 26%). 62% of the DEMS (21/34) enable audit trails reports, and 29% (10/34) enable exporting court-accepted reports as part of the documentation related to the digital investigations. With regards to these court reports, DEMS do not mention in which jurisdictions or courts of justice are these reports accepted, a very valuable information due to the disparity and discrepancies among jurisdictions. Standardizing and harmonizing court reports will gain significant relevance in the incoming years due to the increase of cross-border crimes.

Ensuring the chain of custody of digital evidence is another critical feature. To achieve successful prosecution, the integrity of evidence needs to be guaranteed and proved, from their initial gathering to their final presentation in court. Hence, tamper-proof solutions are required. In general, the cryptographic solutions to ensure the integrity of any file are one-way hashing functions. In case of tampering (intentionally or accidentally) a digital evidence, the resulting hash will be different and, in consequence, the chain of custody broken. Despite its importance, the majority of the analysed DEMS do not provide many details about this fundamental feature. For instance, 19 tools (56%) mention that the chain of custody is guaranteed, but no further details about how this is achieved are provided, whilst eight tools (23%) do not mention this feature at all. The other seven

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

Table 6: Relationship between the challenges and the DEMS' evaluated features

Challenge	Evidence collection	Reporting tools	Chain of custody assurance	Use of standards	Regulations compliance
Data location and individuals' control over their own data					✓
Timely collection and sharing of evidence	✓				
Lack of harmonization in rules of admissibility of criminal evidence and prosecution		✓	✓	✓	
Lack of compatibility between different protocols regarding data categorization and definitions				✓	
Direct cooperation with service providers and equality of opportunities					✓
Incompatibility conflicts between jurisdictions that may violate procedural laws and rights				✓	✓
Lack of automated mechanisms to efficiently collect and report requests	✓		✓		
Auditability in data collection procedures		✓		✓	✓
Lack of resources related to equipment and training of law enforcement and judicial authorities to support direct co-operation between different jurisdictions				✓	✓
Data retention issues	✓		✓		✓

Table 7: Analysis and comparison of commercial tools

Commercial solution	Evidence collection	Reporting tools	Chain of custody assurance	Use of standards	Regulations compliance
ADF [100]	Manual	Court reports	N/A	N/A	N/A
ARQ [101]	Manual, compatible devices	Audit trails	Hash (SHA-256)	N/A	N/A
AXO [102]	Manual	Audit trails, court reports	Yes*	N/A	CJIS
CEL [103]	Manual	No	Yes*	N/A	N/A
CCE [104]	Manual, compatible devices	No	Yes*	N/A	N/A
DET [105]	Manual	Audit trails	Yes*	N/A	N/A
DOT [106]	Manual	Audit trails	Yes*	N/A	N/A
DTQ [107]	Manual	Court reports	Hash*	N/A	N/A
DOQ [108]	Manual	Audit trails	Yes*	SWGIT	N/A
ECF [109]	Manual, compatible devices	Court reports	N/A	N/A	N/A
ERI [110]	Manual	Audit trails, court reports	Yes*	N/A	N/A
EVW [111]	Manual	No	Yes*	N/A	MoPI
FOR [112]	Manual	No	Yes*	FedRAMP	CJIS
GEN [113]	Manual	No	N/A	N/A	N/A
HIT [114]	Manual	Audit trails	Yes*	N/A	MoPI, GDPR
HYT [115]	Manual	No	N/A	N/A	N/A
INS [116]	Manual	Court reports	N/A	N/A	N/A
KIN [117]	Manual	Audit trails	Yes*	N/A	Yes*
LIM [118]	Manual	Audit trails	Yes	ISO	N/A
LIN [119]	Manual	No	Yes	N/A	N/A
NEW [120]	Manual	Audit trails	N/A	FIPS 140-2	CJIS
NIC [121]	Manual, public portal	Audit trails	Yes	N/A	CJIS
OMN [122]	Manual	Audit trails, court reports	Yes	N/A	Yes
ORA [123]	Manual	Audit trails, court reports	Yes	N/A	CJIS
PAT [124]	Manual	Audit trails	Yes	N/A	N/A
PWI [125]	Manual	Audit trails	N/A	N/A	N/A
SAF [126]	Manual	No	Yes	N/A	N/A
SFL [127]	Manual	Audit trails	Yes	N/A	CJIS
SPD [128]	Manual, public portal	No	Hash (SHA-256)	N/A	CJIS, CDR, IRS, DoD
UDE [129]	Manual, compatible devices	Audit trails, court reports	Hash*	N/A	N/A
VER [130]	Manual	Audit trails	Hash (patented)	FIPS	CJIS
VDZ [131]	Manual	Audit trails, court reports	Hash (SHA-256)	FedRAMP, FIPS 140-2	CJIS, HIPAA, GDPR, DoD, ITARM, EAR
WOL [132]	Manual	Audit trails	Hash (SHA-256)	N/A	CJIS
XWI [133]	Manual	Audit trails	N/A	N/A	N/A

*No further details provided online.

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

solutions explicitly mention the use of hashing mechanisms. More specifically, four of these solutions (ARQ, SPD, VDZ, and WOL) use the well-known SHA-256 algorithm, and the VER tool uses a US patented interlocking hashing. However, the management of these hashes to ensure the evidence chain of custody is not detailed. Future solutions should clearly describe the technologies and processes involved in the assurance of the chain of custody.

In order to bring digital evidence to the courts of law, it is necessary to follow the national standards, laws, and methodologies regarding the chain of custody. Unfortunately, international standards for digital investigations are not common, despite the many extant guidelines and documents from national organizations and LEAs. The lack of standards is reflected in the number of DEMS adopting them. Indeed, only six tools (18%) use some standard. More specifically, the US FIPS[6] standard is adopted by NEW, VER, and VDZ; the US FedRAMP[7] standard is adopted by FOR and VDZ; the SWGIT[8] standard is adopted by DOQ; and quality standards set by the ISO are adopted by LIM.

Assessing the impact of the DEMS in terms of social/ethical responsibility, fundamental rights, data protection, and privacy is mandatory to stand by the current regulations and legislations. Generally, the GDPR has harmonized the data protection laws across EU member states by strengthening data processing principles and granting citizens with extensive rights. Regulations intended for LEAs and national security/intelligence parties are, among others, the FBI's CJIS[9] in the USA, or the MoPI[10] in the UK. Surprisingly, only 14 DEMS (41%) recognize that they comply with some regulation. For instance, 10 tools comply with the CJIS regulation since their market is mostly located in the USA. However, only two DEMS (HIT and VDZ) are GDPR-compliant. Similarly, MoPI-compliant DEMS are only EVW and HIT. Other regulations implemented in DEMS are the US DoD[11] regulatory program in SPD and VDZ; and the US HIPAA[12], EAR[13], and ITARM[14] in VDZ.

The road ahead

Inevitably, due to the need for exchanging digital evidence there will appear more initiatives, beyond the aforementioned. One of the key elements in this discussion is the *chain of custody* as we are considering cases, which are initiated in a jurisdiction and are followed up in another with the control handed over from an entity to another, partially or as a whole. An obvious choice would be to determine whether the control might be centralized or decentralized. We sustain that the decentralized option is more appealing as it allows for more flexibility and control in each jurisdiction and prevents the issues of single points of failure. Moreover, with the introduction of blockchains and distributed ledgers there are several issues that can be inherently tackled, e.g. traceability, auditability, and, of course, immutability. Notably, the use of smart contracts can facilitate the automation of such exchanges and enable fine-grained control of who has access, when, what can be submitted and exchanged, by whom and so on. The latter introduces other practical issues as, for instance, existing legislation does not allow LEAs to use platforms and store evidence in public facing storage facilities or use infrastructure that common civilians use, let alone civilians from different countries.

The creation of dedicated platforms, such as the eEDES and others, based on blockchain technology must be streamlined in such a way that the role of national judicial and law enforcement authorities is correctly balanced with the intervention of supra national entities, such as Eurojust and Europol. The possibility for a central authority to intervene in such platforms should only be included if they are designed for cooperation with non EU States [134]. Technical and legal solutions designed to deal with digital evidence, often very volatile, need to find fast and direct routes for information gathering and sharing and not shy away from the inclusion of public/private cooperation, as direct cooperation among two sectors is often a necessary strategy to fight crime in the digital age. In this direction goes the latest decision to empower Europol [135], with the appropriate supervision, and allow it to process large datasets and receive data from private companies.

Setting aside issues such as identity management and access rights, which are more technical, an important aspect that has to be considered is the admissibility of digital evidence in court. The questions that emerge are primarily related to the collection of digital evidence. For instance, the collection of digital evidence by involving specific methods might be admissible in one country but not in another. Thus, the exchange of digital evidence would be legal, but the evidence would not be admissible. This is rather important especially in the eye of authoritarian regimes, lawful interception, deception during interrogations, and use of AI and ML against use of, e.g. decentralized platforms and end-to-end encryption. All the above, individually, may punch holes in the admissibility of evidence in court while raising ethical issues. The case of using the notorious Pegasus spyware [136] while exceptional, clearly illustrates how different countries consider lawful interception and surveillance. Moreover, the legality of using specific tools, methods, and the overall practice of the judicial system is questionable in many authoritarian regimes and may result in further violations of human rights.

Of particular interest is the recurring discussion on encryption and access to the underlying data from the LEAs. Clearly, the abuse of encryption by criminals, not only cyber criminals, introduces many additional burdens for LEAs and digital forensics experts. This is something that troubles law and policy makers [137] regardless of the laws that have been adopted [138, 139] or plan to be adopted by some countries [140], especially targeting end-to-end encryption. The red line between excessive surveillance capabilities and providing LEAs with the necessary access can be very thin. Even more, measures to prevent unintended negative side effects might not be enforceable as the integration of a backdoor in an encryption algorithm practically renders encryption useless and jeopardizes the protection of fundamental rights and citizens' data. The above introduces more questions regarding who is collecting the digital evidence, how, and whether this collection is acceptable to the rest of the parties in the chain of custody of a case.

We sustain that once the legal and ethical aspects are tackled, standardization activities should allow for the technical development of such solutions in an operational manner. Standardization should cover the definition of entities, roles, underlying ontologies, and the allowed interactions among entities. In this regard, while several standards define they way to manage and store data during forensic investigations (e.g. several standards in the ISO 27000 series), standardized ways to preserve the chain of custody during digital investigations, ensuring its authenticity for later admissibility in court are a necessary step towards cross-border harmonization [8].

6 Federal Information Processing Standard.
7 Federal Risk and Authorization Management Program.
8 Scientific Working Group on Imaging Technology.
9 Criminal Justice Information Services.
10 Management of Police Information.
11 Department of Defence.
12 Health Insurance Portability and Accountability Act.
13 Export Administration Regulations.
14 International Traffic in Arms Regulations.

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

There is still a long road ahead to achieve the proper alignment between the required protocols enabling cross-border prosecution, the underlying evidence management systems from a practical perspective, and other legal, ethical and procedural aspects that are continuously evolving to be on track with the current state of practice. In this regard, we sustain that novel directives and initiatives, such as the AI Act [141] should take into account the challenges and views discussed in this article to avoid introducing more burden to current challenges while trying to solve others. The latter is crucial, especially in the case of AI and ML, since they are continuously being integrated into many software solutions and are used by LEAs and digital investigators. While the European Commission devotes substantial efforts to fund initiatives to fight cybercrime (see 'Current activities and related projects'), most of them require further efforts to achieve an effective exploitation of their results, and to finally reach the status of an actual product/solution. Eventually, as in every funding scheme, not all projects manage to reach their full potential. Therefore, this 'valley of death' that all projects have to cross after their funding period is a big challenge and further mechanisms are currently being pushed by the EU to facilitate this passage.

Therefore, we think that more communication and collaboration is needed between policy makers, LEAs, digital investigators, academic and legal experts, as well as representatives of the general public, to reach to solutions conforming to the current ethical values and respecting the freedoms and rights of individuals to fight against next-generation cybercrime. In this regard, novel initiatives such as CSAE (i.e, Collect, Store, Analyse, and Engage) [142] are promoting the necessity of harmonization and effective collaboration through comprehensive frameworks.

Conclusions

The sophistication of criminal activities paired with ICT evolution hinder current investigations and require continuous cross-border collaboration between different entities. The latter is not an easy task since several challenges arise, e.g. in the legal, technical, and ethical dimensions. The research questions posed in 'Research Methodology' summarize the main aim of our research, namely providing a comprehensive state of knowledge of the different mechanisms to leverage cross-border investigations, their challenges, and a fruitful discussion of the road ahead of this particular matter. We discuss them in order next:

Q1: *Which are the current tools, procedures, and protocols for cross-border evidence exchange amongst European countries/jurisdictions?*

In order to provide enough background to discuss the rest of the research questions, we have summarized the main mechanisms and protocols enabling cross-border collaboration. In 'Main Instruments for Cross-Border Investigations in Europe' we have provided this information in the context of Europe, along with other well-known international procedures. According to our analysis, each mechanism has a different scope, and the application of the proper one is required in each case, especially to minimize the investigation's overhead.

Q2: *Which are the main challenges related to cross-border investigations?*

A profound analysis of the literature was required to extract all the challenges of this particular matter, as described in 'Research Methodology'. The selection of articles and reports that discussed the current challenges of cross-border investigations allowed us to conclude that the same issues are identified by different authors regardless of their background. We have summarized and abstracted these challenges to provide a clear overview of the state of practice, and we have discussed them along with some possible countermeasures in 'Literature Review and Challenge Extraction'.

Q3: *Are current practices efficient enough to counter the sophistication of cybercrime?*

To answer this research question, we need to combine the information from the two previous ones. In a nutshell, the current mechanisms used for cross-border collaboration are solving partial issues and challenges, but there is no panacea. Moreover, some recent mechanisms and protocols solve some of the identified challenges while introducing new ones, despite the efforts of the actors involved in the process. Thus, the outcome of this analysis is that a profound discussion is required amongst all stakeholders, followed by fast and efficient actions, since cybercriminals seem to be ahead of current legislation.

Q4: *What technologies or strategies can be used to deal with the identified challenges?*

As summarized in 'Discussion—Enhancing Cross-Border Collaboration', continuous efforts are being made to ease cross-border investigations in terms of tools, technologies, research projects, and legislation updates. However, there is still a long road ahead as current solutions are not sufficient to solve the existing challenges. With this aim, we set the ground for the next steps that should be tackled, along with some strategies highlighting the most urgent issues to be solved, which are creating bottlenecks and preventing efficient and robust prosecution. Moreover, we have discussed other possible issues that may arise in the near future, either standalone or due to a combination of challenges, so that prevention mechanisms can be put in place accordingly.

We think that the information analysed and the research questions answered in this article reflect the current state of practice with high fidelity. Therefore, this article provides a fruitful and interdisciplinary ground of research and a clear overview of the measures that may need to be considered in the years to come.

As a final note, we sustain that enabling technologies such as blockchain could enhance the auditability and transparency of several procedures performed during investigations. Several proposals that prove the capabilities of such a technology in the context of forensic investigations have been provided in the literature [143–146]. Moreover, blockchain could be used to automate several of the previously discussed procedures (e.g. evidence exchange). The latter could improve trust in legal systems and reduce the delays in investigations [20]. Of course, storing the evidence on the blockchain would not be the best option, e.g. consider the case of the evidence being a hard drive of some terabytes, however, off-chain mechanisms such as the IPFS [147] could efficiently fill in this gap.

Acknowledgments

This work was supported by the European Commission under the Horizon 2020 Programme (H2020), as part of the projects *LOCARD* (https://locard.eu) (grant agreement number 832735) and HEROES (https://heroes-fct.eu/; grant agreement number 101021801). F.C. was supported by the Beatriu de Pinós programme of the Government of Catalonia (grant number 2020 BP 00035).

Conflict of interest

The authors reported no potential conflict of interest.

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

References

1. European Commission. Commission staff working document impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN. (8 March 2022, date last accessed).
2. Denyer D, Tranfield D. Producing a systematic review. In: *The Sage Handbook of Organizational Research Methods*. Thousand Oaks: SAGE Publications Ltd, 2009,671–89.
3. Tranfield D, Denyer D, Smart P. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *Br J Manag* 2003;**14**:207–22.
4. Pranckutė R. Web of Science (WoS) and Scopus: the Titans of bibliographic information in today's academic world. *Publications* 2021;**9**:12.
5. Vom Brocke J, Simons A, Riemer K,. *et al.* Standing on the shoulders of giants: challenges and recommendations of literature search in information systems research. *Commun Assoc Inf Syst* 2015;**37**:9.
6. Elo S, Kyngäs H. The qualitative content analysis process. *J Adv Nurs* 2008;**62**:107–15.
7. Cybercrime Convention Committee (T-CY). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b. (2 March 2022, date last accessed).
8. Council of Europe. Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). 2022. https://www.coe.int/en/web/cybercrime/second-additional-protocol. (29 April 2022, date last accessed).
9. European Judicial Network. 2014/41/EU: Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters. https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120.
10. Stefan M. JUD-IT Handbook: CEPS Papers in Liberty and Security No 2020-03. Archive of European Integration, 2020.
11. Stefan M, González Fuster G. *Cross-Border Access to Electronic Data Through Judicial Cooperation in Criminal Matters*. CEPS Paper in Liberty and Security in Europe. Brussels: CEPS Publications, 2018.
12. Abraha HH. Regulating law enforcement access to electronic evidence across borders: the United States approach. *Inf Commun Technol Law* 2020;**29**:324–53.
13. Mulligan SP. Cross-border data sharing under the CLOUD Act. Washington: Congressional Research Service, 2018.
14. Mirko HSB. Improving cross-border access to electronic evidence. 2019. https://www.gppi.net/media/GPPi_2018_Hohmann_Barnett_System_Upgrade.pdf. (1 March 2022, date last accessed)
15. Europol. Sirius eu digital evidence situation report-3rd annual report, 2021. 2021.
16. Mitsilegas V, Carrera S, Stefan M. Cross-border data access in criminal proceedings and the future of digital justice. 2020. https://www.ceps.eu/download/publication/?id=30689&pdf=TFR-Cross-Border-Data-Access.pdf. (1 March 2022, date last accessed)
17. Abraha HH. Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. *Int J Law Inf Technol* 2021;**29**:118–53.
18. Jerman Blažič B, Klobučar T. Advancement in cybercrime investigation–the new European legal instruments for collecting cross-border e-evidence. In: *International Conference on Information Technology & Systems*. Berlin: Springer, 2019, 858–867.
19. Siry L. Cloudy days ahead: cross-border evidence collection and its impact on the rights of EU citizens. *New J Eur Crim Law* 2019;**10**:227–50.
20. Chauhan P, Bansal P. Enhancing trust and immutability in cloud forensics. In: *ICT Systems and Sustainability*. Berlin: Springer, 2021, 771–778.
21. Kahvedžić D. Cybercrime investigations of mobile phone devices and the cloud in the light of EU safe harbour rulings. In: *Era Forum*. Vol. **17**. Berlin: Springer, 2016, 355–367.
22. Shalaginov A, Shalaginova M, Jevremovic A,. *et al.* Modern cybercrime investigation: technological advancement of smart devices and legal aspects of corresponding digital transformation. In: *EEE International Conference on Big Data (Big Data)*. Atlanta, GA, IEEE, 2020, 2328–2332.
23. Fuster GG, Maymir SV. Cross-border access to e-evidence: Framing the evidence. CEPS in Liberty and Security in Europe No 2020-02. Brussels: CEPS, 2020.
24. Kleijssen J, Perri P. Cybercrime, evidence and territoriality: Issues and options. In: *Netherlands Yearbook of International Law 2016*. Berlin: Springer, 2017, 147–173.
25. Karas Ž, Đipić SP. Evaluation of the results of the european investigation order. *EU Comp Law Iss Chall Ser* 2019;**3**:492–506.
26. Zaharieva R. The European investigation order and the joint investigation team—which road to take: a practitioner's perspective. *ERA Forum* 2017;**18**:397–408.
27. Blažič BJ, Klobučar T. Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society. *Inf Commun Technol Law* 2020;**29**:66–81.
28. Csúri A. Towards an inconsistent european regime of cross-border evidence: the EPPO and the european investigation order. In: *Shifting Perspectives on the European Public Prosecutor's Office*. Berlin: Springer, 2018, 141–153.
29. European Commission. Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office. https://ec.europa.eu/transparency/documents-register/api/files/COM(2013)534_0/de00000000479750?rendition=false. (2 March 2022, date last accessed).
30. Warken C, van Zwieten L, Svantesson D. Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence. *Int Rev Law Comput Technol* 2020;**34**:44–64.
31. Blažič BJ, Klobučar T. Investigating crime in an interconnected society: will the new and updated EU judicial environment remove the barriers to justice?. *Int Rev Law Comput Technol* 2020;**34**:87–107.
32. Karagiannis C, Vergidis K. Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. *Information* 2021;**12**:181.
33. Biasiotti MA, Conti S, Turchi F. Electronic evidence semantic structure: exchanging evidence across europe in a coherent and consistent way. In: *AI Approaches to the Complexity of Legal Systems*. Berlin: Springer, 2015, 556–573.
34. Barbosa e Silva J. The speciality rule in cross-border evidence gathering and in the European Investigation Order'let's clear the air. In: *Era Forum*. Vol. **19**. Berlin: Springer, 2019, 485–504.
35. Ortiz-Pradillo JC. The new regulation of technology-related investigative measures in Spain. *ERA For* 2017;**18**:425–35.
36. Pavlidis G. Asset recovery in the European Union: implementing a "no safe haven" strategy for illicit proceeds. *J Money Laund Cont* 2021;**25**:109–17.
37. Birdi K,. *et al.* Factors influencing cross-border knowledge sharing by police organisations: an integration of ten European case studies. *Pol Pract Res* 2021;**22**:3–22.
38. Heusala A, Koistinen J. "Rules of the game" in cross-border cooperation: legal-administrative differences in Finnish–Russian crime prevention. *Int Rev Admin Sci* 2018;**84**:354–70.
39. Loik R,. *et al.* European internal security interests and Brexit. Legal and operational aspects of the post–Brexit cooperation model. *Roman J Eur Aff* 2020;**20**:5–17.
40. Currie RJ. Cross-border evidence gathering in transnational criminal investigation: is the Microsoft Ireland case the "next frontier"?. *Canad Yearbook Int Law* 2017;**54**:63–97.
41. Ghappour A. Searching places unknown: law enforcement jurisdiction on the dark web. *Stanford Law Rev* 2017;**69**:1197–236.

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

42. Arrigg Koh S. Foreign affairs prosecutions. *New York Univ Law Rev* 2019;**94**:340–401.
43. Modi N. Toward an international right against self-incrimination: expanding the fifth amendment's" compelled" to foreign compulsion. *Virg Law Rev* 2017;**103**:961–1015.
44. Mitsilegas V, Giuffrida F. The European public prosecutor's office and human rights. In: *Shifting Perspectives on the European Public Prosecutor's Office*. Berlin: Springer, 2018, 59–98.
45. Van Den Berge Y. Transposition of the directive on the protection of the financial interests of the european union into national legislation: experiences with tools and powers. *ERA For* 2021;**22**: 351–60.
46. Europol. Common challenges in combating cybercrime. https://www.europol.europa.eu/publications-events/publications/common-challenges-in-combating-cybercrime. (8 March 2022, date last accessed).
47. Casino F,. *et al.* Research trends, challenges, and emerging topics in digital forensics: a review of reviews. *IEEE Access* 2022;**10**: 25464–93.
48. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telemat Inf* 2019;**36**:55–81.
49. Javed AR, Ahmed W, Alazab M,. *et al.* A comprehensive survey on computer forensics: state-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access* 2022;**10**:11065–89.
50. European Commission. EVIDENCE2E-CODEX linking evidence into e-CODEX for EIO and MLA procedures in Europe. Conclusion report and feedback from the Joint WP4/EXEC, Workshop on Merging Views Meeting technical and legal community to cross-fertilise views. Deliverable D4.3. https://evidence2e-codex.eu/p/e/v/evidence2e-codex-deliverable-d4-3-summary-734.pdf. (10 April 2022, date last accessed).
51. European Commission. e-Evidence Digital Exchange System (eEDES). https://evidence2e-codex.eu/p/j/o/jointmergingworkshop-florence-2019-09-04-eedesintroduction-578.pdf. (10 April 2022, date last accessed).
52. Interpol. e-MLA. https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2018/INTERPOL-s-e-MLA-initiative-focus-of-EU-expert-meeting. (10 April 2022, date last accessed).
53. Eurojust. Eurojust written recommendations on jurisdiction: follow-up at the national level. https://www.eurojust.europa.eu/publication/eurojust-written-recommendations-jurisdiction-follow-up-national-level. (10 April 2022, date last accessed).
54. European Union Agency for Criminal Justice Cooperation. Detailed description in Cybercrime Judicial Monitor n.6. https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/cybercrime_judicial_monitor_issue_6_2021.pdf. (10 April 2022, date last accessed).
55. The Court of Justice of the European Union. Judgment of 5 Apr 2022, C-140/20 (Commissioner of the Garda Síochána and Others). https://www.dpcuria.eu/case?reference=C-140/20. (10 April 2022, date last accessed).
56. The Court of Justice of the European Union. La Quadrature du Net and Others (Oct. 2020). https://curia.europa.eu/juris/document/document.jsf?docid=232084&doclang=en. (10 April 2022, date last accessed).
57. CORDIS. Community Research and Development Information Service. https://cordis.europa.eu/. (10 April 2022, date last accessed).
58. RAYUELA. Empowering and educating young people for the internet by playing. https://cordis.europa.eu/project/id/882828. (10 April 2022, date last accessed).
59. SIRIUS. Cross-border access to electronic evidence. https://www.europol.europa.eu/operations-services-innovation/sirius-project. (10 April 2022, date last accessed).
60. Council of Europe. Octopus project. https://www.coe.int/en/web/cybercrime/octopus-project. (10 April 2022, date last accessed).
61. ECTEG. European Cybercrime Training Education Group. https://www.ecteg.eu/. (10 April 2022, date last accessed).
62. HEROES. Novel strategies to fight child sexual exploitation and human trafficking crimes and protect their victims. https://cordis.europa.eu/project/id/101021801. (10 April 2022, date last accessed).
63. POP AI. A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights. https://cordis.europa.eu/project/id/101022001. (10 April 2022, date last accessed).
64. ALIGNER. Artificial Intelligence Roadmap for Policing and Law Enforcement. https://cordis.europa.eu/project/id/101020574. (10 April 2022, date last accessed).
65. INDEED. Strengthening a comprehensive approach to preventing and counteracting radicalisation based on a universal evIdeNce-based moDEl for Evaluation of raDicalisation prevention and mitigation. https://cordis.europa.eu/project/id/101021701. (10 April 2022, date last accessed).
66. LAW-GAME. An interactive, collaborative digital gamification approach to effective experiential training and prediction of criminal actions. https://cordis.europa.eu/project/id/101021714. (10 April 2022, date last accessed).
67. APPRAISE. fAcilitating Public & Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts. https://cordis.europa.eu/project/id/101021981. (10 April 2022, date last accessed).
68. iCrime. Interdisciplinary Cybercrime Project. https://cordis.europa.eu/project/id/949127. (10 April 2022, date last accessed).
69. TRACE. Tracking illicit money flows. https://cordis.europa.eu/project/id/101022004. (10 April 2022, date last accessed).
70. UNCOVER. Development of an efficient steganalysis framework for uncovering hidden data in digital media. https://cordis.europa.eu/project/id/101021687. (10 April 2022, date last accessed).
71. CYCLOPES. Fighting Cybercrime – Law Enforcement Practitioners' Network. https://cordis.europa.eu/project/id/101021669. (10 April 2022, date last accessed).
72. CounteR. Fighting Cybercrime – Law Enforcement Practitioners' Network. https://cordis.europa.eu/project/id/101021607. (10 April 2022, date last accessed).
73. DARLENE. Deep AR Law Enforcement Ecosystem. https://cordis.europa.eu/project/id/883297. (10 April 2022, date last accessed).
74. AIDA. Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies. https://cordis.europa.eu/project/id/883596. (10 April 2022, date last accessed).
75. EXFILES. Extract Forensic Information for LEAs from Encrypted SmartPhones. https://cordis.europa.eu/project/id/883156. (10 April 2022, date last accessed).
76. GRACE. Global Response Against Child Exploitation. https://cordis.europa.eu/project/id/883341. (10 April 2022, date last accessed).
77. INFINITY. IMMERSE. INTERACT. INVESTIGATE. https://cordis.europa.eu/project/id/883293. (10 April 2022, date last accessed).
78. TUECS. The uberization of Europol's cybercrime strategy: an innovative governance model on public-private partnership. https://cordis.europa.eu/project/id/886141. (10 April 2022, date last accessed).
79. CC-DRIVER. The uberization of Europol's cybercrime strategy: an innovative governance model on public-private partnership. https://cordis.europa.eu/project/id/883543. (10 April 2022, date last accessed).
80. INSPECTr. Intelligence Network and Secure Platform for Evidence Correlation and Transfer. https://cordis.europa.eu/project/id/833276. (10 April 2022, date last accessed).
81. ROXANNE. Real time network, text, and speaker analytics for combating organized crime. https://cordis.europa.eu/project/id/833635. (10 April 2022, date last accessed).
82. PREVISION. Prediction and Visual Intelligence for Security Information. https://cordis.europa.eu/project/id/833115. (10 April 2022, date last accessed).
83. CREST. Fighting Crime and TerroRism with an IoT-enabled autonomous platform based on an ecosystem of Advanced IntelligEnce, Operations, and InveStigation Technologies. https://cordis.europa.eu/project/id/833464. (10 April 2022, date last accessed).
84. FORMOBILE. From mobile phones to court – a complete FORensic investigation chain targeting MOBILE devices. https://cordis.europa.eu/project/id/832800. (10 April 2022, date last accessed).

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

85. LOCARD. Lawful evidence collecting and continuity platform development. https://cordis.europa.eu/project/id/832735. (10 April 2022, date last accessed).
86. PROACTIVE. PReparedness against CBRNE threats through cOmmon Approaches between security praCTItioners and the VulnerablE civil society. https://cordis.europa.eu/project/id/832981. (10 April 2022, date last accessed).
87. JustSites. The Global Sites of International Criminal Justice. https://cordis.europa.eu/project/id/802053. (10 April 2022, date last accessed).
88. SPIRIT. Scalable privacy preserving intelligence analysis for resolving identities. https://cordis.europa.eu/project/id/786993. (10 April 2022, date last accessed).
89. COPKIT. Early-action led policing in fighting organised crime and terrorism. https://cordis.europa.eu/project/id/786687. (10 April 2022, date last accessed).
90. SHUTTLE. Scientific High-throughput and Unified Toolkit for Trace analysis by forensic Laboratories in Europe. https://cordis.europa.eu/project/id/786913. (10 April 2022, date last accessed).
91. MAGNETO. Multimedia Analysis and Correlation Engine for Organised Crime Prevention and Investigation. https://cordis.europa.eu/project/id/786629. (10 April 2022, date last accessed).
92. PROTAX. New methods to PRevent, Investigate and Mitigate COrruption and TAX Crimes in the EU. https://cordis.europa.eu/project/id/787098. (10 April 2022, date last accessed).
93. I-LEAD. Innovation - Law Enforcement Agencies Dialogue. https://cordis.europa.eu/project/id/740685. (10 April 2022, date last accessed).
94. ILEAnet. Innovation by Law Enforcement Agencies networking. https://cordis.europa.eu/project/id/740714. (10 April 2022, date last accessed).
95. VISAGE. Visible attributes through genomics: broadened forensic use of DNA for constructing composite sketches from traces. https://cordis.europa.eu/project/id/740580. (10 April 2022, date last accessed).
96. VICTORIA. Video analysis for Investigation of Criminal and TerrORIst Activities. https://cordis.europa.eu/project/id/740754. (10 April 2022, date last accessed).
97. ESSENTIAL. Evolving Security SciencE through Networked Technologies, Information policy And Law. https://cordis.europa.eu/project/id/722482. (10 April 2022, date last accessed).
98. ASGARD. Analysis System for Gathered Raw Data. https://cordis.europa.eu/project/id/700381. (10 April 2022, date last accessed).
99. RAMSES. Internet forensic platform for tracking the money flow of financially-motivated malware. https://cordis.europa.eu/project/id/700326. (10 April 2022, date last accessed).
100. ADF Solutions. Digital evidence investigator. https://www.adfsolutions.com/dei. (10 April 2022, date last accessed).
101. StorMagic. ARQvault digital evidence management. https://stormagic.com/arqvault/solutions/digital-evidence-management/. (10 April 2022, date last accessed).
102. Axon. Axon evidence. https://global.axon.com/products/evidence. (10 April 2022, date last accessed).
103. Cellebrite. Cellebrite digital intelligence. https://cellebrite.com/en/criminal-investigations/. (10 April 2022, date last accessed).
104. Motorola Solutions. CommandCentral evidence. https://www.motorolasolutions.com/en_us/products/command-center-software/records-and-evidence-management/commandcentral-evidence.html. (10 April 2022, date last accessed).
105. MCM Solutions. Detego case manager. https://www.mcmsolutions.co.uk/solutions/workflow-management-system/. (10 April 2022, date last accessed).
106. Otec Solutions. Digital evidence management suite. http://www.otecsolutions.com/index.php/dems-our-solution-for-managing-digital-evidence/. (10 April 2022, date last accessed).
107. QueTel Corporation. Digital TraQ. https://www.quetel.com/products/digital-evidence-management-system. (10 April 2022, date last accessed).
108. EvidenceOnQ Evidence Software. DigitalOnQ. https://www.evidenceonq.com/products/digitalonq.html. (10 April 2022, date last accessed).
109. OpenText. EnCase forensic. https://www.opentext.com/products-and-solutions/products/security/digital-forensics. (10 April 2022, date last accessed).
110. Erin Technology. ERIN7. https://erintechnology.com/evidence-tracker/. (10 April 2022, date last accessed).
111. Capita. EvidenceWorks digital evidence management. https://www.capita.com/expertise/industry-specific-services/public-safety/digital-evidence-management/evidence-management-technology. (10 April 2022, date last accessed).
112. Blue Line Innovations. Fortify. https://www.bli360.com/fortify-2/. (10 April 2022, date last accessed).
113. Genetec. Genetec clearance. https://www.genetec.com/products/operations/clearance. (10 April 2022, date last accessed).
114. Hitachi Vantara. Hitachi digital evidence management. https://www.hitachivantara.com/en-us/pdf/solution-profile/digital-evidence-management-solution-profile.pdf. (10 April 2022, date last accessed).
115. Hytera Communications. Hytera evidence management. https://hytera-europe.com/communication-applications/evidence-management. (10 April 2022, date last accessed).
116. Altia Solutions Ltd. Insight. https://www.altiaintel.com/evidence-and-records-management/. (10 April 2022, date last accessed).
117. Kinesense Ltd. Kinesense digital evidence and asset management. https://www.kinesense-vca.com/product/kinesense-dem/. (10 April 2022, date last accessed).
118. IntaForensics. Lima forensic case management. https://www.intaforensics.com/lima/. (10 April 2022, date last accessed).
119. Linear Systems. Digital evidence management. https://www.linearlawenforcement.com/dims-overview.
120. Tyler Technologies. New world digital evidence. https://www.tylertech.com/products/new-world-public-safety/digital-evidence. (10 April 2022, date last accessed).
121. NICE. Investigation and digital evidence management software. https://www.nicepublicsafety.com/nice-investigate/. (10 April 2022, date last accessed).
122. Omnigo. Evidence management. https://www.omnigo.com/solutions/evidence-management. (10 April 2022, date last accessed).
123. Oracle. Digital evidence management solution for police. https://www.oracle.com/assets/ds-digital-evidence-management-3864416.pdf. (10 April 2022, date last accessed).
124. PatrolEyes. PatrolEyes enterprise digital evidence management software. https://patroleyes.com/products/enterprise-digital-evidence-management. (10 April 2022, date last accessed).
125. Pwithe. Digital evidence management system. https://en.pwithe.com/product-category/digital-evidence-management-system/. (10 April 2022, date last accessed).
126. Tracker Products. SAFE evidence management. https://trackerproducts.com/. (10 April 2022, date last accessed).
127. Safe Fleet. Digital evidence management. https://www.safefleet.net/products/fleet-video-systems/law-enforcement-video-evidence-systems/digital-evidence-management/. (10 April 2022, date last accessed).
128. Scout PD. Evidence management. https://scout-pd.com/product. (10 April 2022, date last accessed).
129. Panasonic i-PRO. Unified digital evidence. https://i-pro.com/us/en/publicsafety/products/unified-digital-evidence/. (10 April 2022, date last accessed).
130. VeriPic. Digital evidence management. https://www.veripic.com/. (10 April 2022, date last accessed).
131. VIDIZMO. Digital evidence management. https://www.vidizmo.com/digital-evidence-management/. (10 April 2022, date last accessed).
132. WOLFCOM. WOLFCOM Evidence management system. https://wolfcomusa.com/evidence-management-software/. (10 April 2022, date last accessed).
133. X-Ways. X-Ways investigator. https://www.x-ways.net/investigator/index-m.html. (10 April 2022, date last accessed).
134. Ramos JAE, Ettenhofer J, Falletti F, Weyembergh A. *Institutional Framework for EU Criminal Justice Cooperation*. Oxford: Oxford University Press, 2020. doi: 10.30709/eucrim-2020-019.
135. European Parlament. Strengthening Europol's mandate: cooperation with private parties, processing of personal data, and support for research and innovation. https://oeil.secure.europarl.europa.eu/oeil/po

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023

pups/ficheprocedure.do?reference=2020/0349(COD)&l=en. (14 April 2022, date last accessed).
136. Amnesty International. Forensic methodology report: How to catch NSO Group's Pegasus. 2021. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/. (14 April 2022, date last accessed).
137. Council of Europe. Council resolution on encryption - security through encryption and security despite encryption. 2020. https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf. (14 April 2022, date last accessed).
138. Australia Government. Telecommunications and Other Legislation Amendment (Assistance and Access) Act. 2018. https://www.legislation.gov.au/Details/C2018A00148. (15 April 2022, date last accessed).
139. UK Government. Investigatory Powers Act. 2016. https://www.legislation.gov.au/Details/C2018A00148. (15 April 2022, date last accessed).
140. UK Government. Draft Online Safety Bill. 2022. https://www.gov.uk/government/publications/draft-online-safety-bill. (15 April 2022, date last accessed).
141. European Commission. Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206. (17 April 2022, date last accessed).
142. Sandt E, van Bunningen A, van Lenthe J,. *et al*., Towards data scientific investigations: a comprehensive data science framework and case study for investigating organized crime and serving the public interest. In: *White paper presented at the third INTERPOL-UNICRI global meeting on AI for law enforcement on November*. Vol. **25**. 2021, 2020.
143. Dasaklis TK, Casino F, Patsakis C. Sok: blockchain solutions for forensics. In: *Technology Development for Security Practitioners*. Berlin: Springer, 2021, 21–40.
144. Kumar G, Saha R, Lal C,. *et al*. Internet-of-Forensic (IoF): a blockchain based digital forensics framework for IoT applications. *Fut Gen Comput Syst* 2021;**120**:13–25.
145. Lone AH, Mir RN. Forensic-chain: blockchain based digital forensics chain of custody with PoC in hyperledger composer. *Digit Invest* 2019;**28**:44–55.
146. Zarpala L, Casino F. A blockchain-based forensic model for financial crime investigation: the embezzlement scenario. *Digit Finance* 2021;**3**:1–32.
147. Benet J. IPFS-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561. 2014.

Downloaded from https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060 by guest on 23 February 2023