



Europol and cybercrime: Europol's sharing decryption platform

Ethem Ilbiz & Christian Kاونert

To cite this article: Ethem Ilbiz & Christian Kاونert (2021): Europol and cybercrime: Europol's sharing decryption platform, Journal of Contemporary European Studies, DOI: [10.1080/14782804.2021.1995707](https://doi.org/10.1080/14782804.2021.1995707)

To link to this article: <https://doi.org/10.1080/14782804.2021.1995707>



© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.



Published online: 10 Nov 2021.



Submit your article to this journal [↗](#)



Article views: 332





View related articles [↗](#)



View Crossmark data [↗](#)

Europol and cybercrime: Europol's sharing decryption platform

Ethem Ilbiz ^a and Christian Kaunert ^{a,b}

^aInternational Centre for Policing and Security, University of South Wales, Rhondda Cynon Taf, UK; ^bSchool of Law and Government, Dublin City University as well as the University of South Wales, Dublin, Ireland

ABSTRACT

This article examines the resource sharing functionality of the decryption platform of Europol. The platform supports European law enforcement agencies (LEAs) that are having difficulties accessing legally obtained encrypted evidence due to the lack of human and technical resources. The article investigates Europol's resource transmission role with sharing economy variables such as transaction cost and trust-building. The core argument of the article is that Europol's sharing platform has a strong potential to reduce the transaction cost of outsourcing the decryption services and diminish trust-related problems for national policing agencies by replacing private sector actors. However, for a more sustainable cybercrime investigation strategy, the decryption platform needs a new market-oriented model supported with robust vetting and evidence security mechanisms to encourage more private company participation.

KEYWORDS

Europol; EC3; encryption; decryption; backdoor; computational power; sharing economy; cybercrime

Introduction

Unauthorised access to private or critical data is an increasing threat in cyberspace both for individuals and states. Encryption is a leading solution in preventing the intrusion of malicious actors attempting to obtain private and confidential data. In recent years, encryption has been promoted by the Council of the European Union to enhance the EU's ability to protect itself from cyber threats (The Council of the European Union 2020). However, encryption technology has a dark side as well as its benefits. As often referred with the 'Going Dark' metaphor (Comey 2014), encryption complicates access and analysis of the data linked with criminal activity. It can be extremely challenging for LEAs to collect digital evidence from encrypted devices and networks.

The investigation contradictions associated with encryption is not only limited to accessibility problems regarding encrypted evidence, but are also immense legal and ethical questions about whether LEAs should provide exceptional access to encrypted communication networks or under what conditions their access should be allowed (Abelson et al. 2015; Severson 2017; Monsees 2019). In the absence of automated and rapid access provided by the private sector, LEAs should be capable of decrypting password-protected evidence to tackle serious crimes like terrorism and online child sexual exploitation. They need to employ competent in-house experts for investigations and have enough financial resources to obtain powerful computational tools. In the absence of both, LEAs need trustworthy outsourcing partners qualified in decryption to acquire tacit knowledge. Otherwise, malicious actors would take the advantage of the weaknesses of LEAs and continue their illegal activities within encrypted networks without the fear of being caught.

CONTACT Christian Kaunert  Christian.kaunert@southwales.ac.uk  School of Law and Government, Dublin City University, Ireland

The financial and technical capacity EU member states have to investigate encrypted communications vary between member states. Many states lack human and financial resources to cope with encryption in criminal investigations (Koomen 2019). Others acquire decryption services either from private companies qualified in decryption or national forensic institutions that collaborate with LEAs (The Council of the European Union 2017). Therefore, an EU-level solution is favourable for all member states (The Council of the European Union 2016a). In this context, over the past few years, there has been a heated debate in the EU over how the LEAs should have access to encrypted communication for evidence collection. Two technological solutions stand in the forefront of this discussion. The first is to build backdoors in encrypted software that allows LEAs to bypass the normal authentication process and access encrypted data. The second is to break the encryption with computational force (Stupp 2016). Following several years of discussion between member states, the backdoor solution was shelved due to concerns about privacy rights and the potential risks regarding the weakening of the security of encryption (Stupp 2016). Instead, the EU member states agreed on enhancing Europol's decryption capabilities to support national authorities.

As a result of a joint agreement in December 2020, Europol announced the launch of an 'innovative decryption platform' under its mandate, which would be operated by European Cybercrime Centre (EC3) and developed in close cooperation with the European Commission's Joint Research Centre (JRC) (Europol 2020). According to EU Commissioner for Home Affairs Ylva Johansson and Europol's Executive Director Catherine De Bolle, the decryption platform aims to support national LEAs by decrypting their digital evidence (Europol 2020). Furthermore, Europol provides this service free of charge (Van Gemert 2019). Thus, the decryption platform established with altruistic motives intends to share EC3's and JRC's expertise and technological resources with European LEAs. The platform aims to provide a sustainable solution for LEAs to reach the technical and computational resources without ownership.

In broader literature on the EU's Area of Freedom, Security and Justice (AFSJ) concerned with EU cooperation on criminal justice matters (Fletcher, Lööf, and Gilmore 2008; Eckes and Theodore 2011) and EU police and judicial cooperation (Anderson and Joanna 2002; Occhipinti 2003; Guild and Geyer 2008), Europol has always received some attention (Lavranos 2003; Occhipinti 2003; Deflem 2006; Bures 2011). It has been identified as an international security actor mandated to develop cooperation agreements with third states and parties (Kaunert 2010). However, despite its remarkable role in AFSJ, autonomy of Europol in European security governance was found either limited (Busuioc and Groenleer 2013) or identified as a socialization platform of member states to influence EU security governance (Carrapiço and Trauner 2013).

The new digitalization trend in serious crimes and their cross-border nature have also shifted academic discussions in the AFSJ literature. The legal challenges of Europol with its external partners on finding a balance between security and liberty, such as interoperability of crime data and protecting fundamental rights, became the new focus of current AFSJ literature (Briere 2018, 2019; Coman-Kund 2018, 2020; Drewer and Miladinova 2017; Mitsilegas and Giuffrida 2017; Weyemergh, Armada, and Briere 2015). Within the increasing role of the private sector on EU cybersecurity governance (Carrapiço and Barrinha 2017; Carrapiço and Farrand 2017, 2020), Europol is also placed at the centre of these debates as an intermediary between public and private actors (Bossong and Wagner 2018). In this regard, a new public-private partnership (P3) model, 'Sharing Economy' also known as 'Uberization' has been promoted as a new collaboration model for Europol (Wainwright and Cilluffo 2017; TUECS 2020).

Considering the short history of Europol's decryption platform, the literature concerned with this area is still nascent. According to Europol's executives, the European policing agency is on the way to becoming a hub for innovation for policing solutions with these platforms (De Bolle 2020). Its former role of collecting data has shifted to that of a more integrated data management between public and private actors (Konig 2020). However, the absence of comprehensive international legal and practical framework is one of the common points highlighted in encryption debate (Pisarić 2020; Ryder 2016; Koomen 2019, 2021; Gutheil et al. 2017). Although these studies emphasized changing governance

trends in cyberspace and vulnerabilities that Europol must tackle, they lack to offer a critical analysis whether the current decryption platform of Europol is a functional solution to tackle the 'Going Dark' problem.

As part of the Special Issue 'European Transnationalism Between Successes and Shortcomings', this article aims explicitly to interject in this debate by focusing on Europol's new decrypting platform and its collaboration model based on sharing. The central question of this article is that 'To what extent is Europol's decryption platform a functional initiative in response to the problems associated with outsourcing needs of LEAs in order to access encrypted evidence?'. The article employs the sharing economy model and its variables; transaction cost and trust-building as a multi-disciplinary theoretical framework to answer research question. The sharing economy model (Uberization) adapted from economics has been endorsed by the Europol authorities as a new governance model for P3 (Wainwright and Cilluffo 2017). However, in broader AFSJ theorization, the sharing economy model has not attracted enough attention yet.

In light of the considerations above, this article argues that the Europol associated decryption platform has strong potential to reduce the transaction cost of outsourcing the decryption services and solve trust issues of LEAs by replacing private sector actors. However, the current platform should be developed further with a new market-oriented model, which is supported with robust vetting and evidence security mechanisms, to turn the platform into a more inclusive place for more private sector participation. The core argument of the article is examined by relying on qualitative data collected from semi-structured interviews with public and private actors, open-source Europol reports and official documents belonging to the European Commission and Parliament. The remainder of this article follows a section where the historical background of Europol's decryption platform is explained. It is followed by sharing economy conceptual framework and the implementation of its variables to examine the functionality of Europol's decryption platform. The conclusion section summarises the research findings and policy suggestions for the EU political actors and Europol executives.

From intermediary to active outsourcing partner – Background of Europol's decrypting platform

The Europol Convention was formally drawn up in July 1995, but Europol was unable to commence full activities until October 1998, when the Convention had been ratified by all EU member states (Deflem 2006; Kaunert 2010). As a result of its legal status as an international organization established under international law, national ratifications were required for all amendments to the Convention. The legal mandate included: (a) improving effective cooperation among police authorities of the member states to prevent and combat serious international organized crime; (b) investigating crimes such as drug trafficking and terrorism.

In those years, neither cybercrime nor P3 was a priority area for Europol. Both remained at the bottom of Europol's 'to do list' until the second half of 2010s. In line with increasing cyber threats targeting European companies and state institutions, the idea of creating a cybercrime unit elevated in the Justice and Home Affairs (JHA) Council agenda. The first initiative to establish a European Cyber Crime Centre (EC3) started with the JHA Council decision to invite Europol to build a European platform where cybercrime information could be shared and reported between European institutions (JHA Council 2008). The name of EC3 also first appeared in the Internal Security Strategy of the EU in 2010 as a focal point for Europe's fight against cybercrime (European Commission 2010; Neil, et al. 2012). In 2013, the EC3 was established as a subunit of Europol to support operational and analytical capacity for investigations and cooperation in cybercrime investigation between European LEAs. Since the beginning, it became a significant security actor with its involvement in serious cybercrime investigations and intense interaction with private partners (Bossong and Wagner 2018).

When EC3 was established, increasing terrorist attacks of the Islamic State of Iraq and Syria (ISIS) in European capitals initiated a new debate upon dealing with encrypted messages of members of terrorist organisations (Lomas 2016). On one hand, public authorities were voicing encryption as a crucial threat to investigate terrorist communication and defending backdoor solution for LEAs. On the other hand, civil society, academia and private companies were pushing back these arguments by highlighting dangers of backdoor solution against privacy and security of European citizens (Koomen 2019). As a result of this heated debate, the minister of interiors of member states agreed on a European Commission authorisation to find a bilateral solution that protects privacy of the EU citizens and enhances the technical capacity of the LEAs (The Council of the European Union 2016b).

Apart from the ISIS threat in 2013, the Working Party on General Matters, including Evaluations (GENVAL), decided to conduct mutual assessments in member states to see implementation and operation of the European policies against cybercrime (The Council of the European Union 2017). These mutual evaluations were based on Joint Action introduced by the European Commission in December 1997. According to Joint Action, member states and their relevant bodies combating organised crime are evaluated by experts whether they apply and implement national-level instruments and comply with standards proposed in the organised crime context (The Council of the European Union 1997). The evaluation missions were conducted in all member countries between October 2014 and September 2016. Evaluation reports emphasised the growing use of encryption as one of the biggest challenges for LEAs to tackle cybercrimes such as online child sexual abuse and online card fraud (The Council of the European Union 2017).

Before the final report of GENVAL was released, EC3 and JRC had already offered joint training programmes and technical workshops for LEAs showing best decrypting cases (Europol 2016c). In these workshops, LEAs, JRC and EC3 exchanged best practices and techniques that had already successfully proven effective outcomes in member state investigations (Europol 2016b). Besides, the spreading ransomware attacks during the 2010s also pushed Europol to be a co-founder of an initiative called 'No More Ransom' with Dutch National Police and private companies McAfee and Kaspersky Lab (Europol 2016d). The project provided open-source decryption tools for victims to recover their encrypted data. Europol invited other cybersecurity companies to join 'No More Ransom' to enlarge P3 network (Europol 2018). Different LEAs and private organisations took part in this network (Europol 2016a) in line with increasing media attention towards the project (Interview 4). The Europol's involvement in this project was to coordinate and exchange information between LEAs and private actors to develop solutions to diverse ransomware threats (Interview 1,2,3,4).

In 2017, the European Commission also announced its position on how to tackle the 'Going Dark' problem. The Commission decided to prioritize enhancing the decryption capabilities of Europol to support member state LEAs (European Commission 2017). Following the announcement, the European Commissioner responsible for security, Julian King, emphasised that the EU is shifting away from the backdoor solution and eliminating the disadvantages of LEAs (Stupp 2017). In 2018, five million Euros were allocated to strengthen the EC3's technical capabilities to tackle encryption cases and coordinating the research around the encryption (Morbin 2020; Interview 1).

In the first two years, Europol only reported the experiences of LEAs with encryption and mostly their difficulties with it (Interview 1). In the third year following the European Commission's decision, the decryption platform was launched in December 2020. The EC3 was tasked to operate the platform with in-house experts (Europol 2020) without any private sector involvement (Interview 1,2,3,4). Europol's intermediary role in the 'No More Ransom' project went beyond to a more active role by analysing encrypted digital evidence. With the launch of the platform, Europol has demonstrated that national LEAs no longer need to seek an outsourcing partner to acquire tacit knowledge for decryption. The EC3 became an alternative forensic institution to share its resources free with LEAs.

Sharing economy model

Sharing is defined as a prosocial behaviour that is the joint use of resources or space (Munger 2018; Cohen and Zehngbot 2014). It is based on an altruistic motive intended to benefit and support another (Sedkaoui and Khelfaoui 2020; Belk 2014). Sharing provides temporary access to a good or service without having its ownership (John 2013a). Therefore, it enables the use of resources that belong to others and diminishes the investment burden on knowledge and equipment.

The concept of sharing has been in transformation in recent years. Following the industrial revolution, consumption and ownership had been the prominent trend in customer behaviour (Bardhi and Eckhardt 2012). However, this trend began to change with globalisation, economic crisis, environmental concerns and exponential developments in digital technologies (Sedkaoui and Khelfaoui 2020). As a result of that, a new generation sharing economy model was born in recent years that had a disrupting impact on nearly all sectors, including transportation (Uber, Lyft), accommodation (Airbnb), freelancer services (Upwork, Fiverr) (Christensen, Raynor, and Rory 2015). The digitalised sharing economy model proved that many services could be acquired without ownership (O'Rourke and Lollo 2015; Bardhi and Eckhardt 2012; John 2013b; Hodkinson 2011).

According to Botsman and Rogers (2010), sharing economy model is an exchange of under-utilised assets between peers in a network or marketplace for money or non-material benefits. For the model's success, there should be a group of people or a community concerned with sustainability and the use of resources in a mutual and altruistic way (Albinsson and Yasanthi Perera 2012; Hamari, Sjöklint, and Ukkonen 2015). The unused or underused resources should be allocated to the people who need them. The feeling of being part of the community is identified as an important motivational factor for non-monetary sharing (Albinsson and Yasanthi Perera 2012). Being part of a community also creates specific synergies and enables community members to realise various benefits such as access to products without ownership, saving money and time (Botsman and Rogers 2010). There are many variations of sharing economy platforms such as peer to peer (p2p), customer to customer (c2c), business to business (b2b), business to customer (b2c) or government to government (g2g) (Sedkaoui and Khelfaoui 2020).

Given the scope of the encryption problem, there is a big cybersecurity community in the EU interested in encryption and seeking feasible solutions in accordance with privacy and security concerns of European society Figure 1. National LEAs, Europol and European Union Agency for Cybersecurity (ENISA) and private companies are key actors of this community. However, in legal means, only LEAs and Europol are authorised to carry out decrypting digital evidence unless they outsource decrypting services from the private sector.

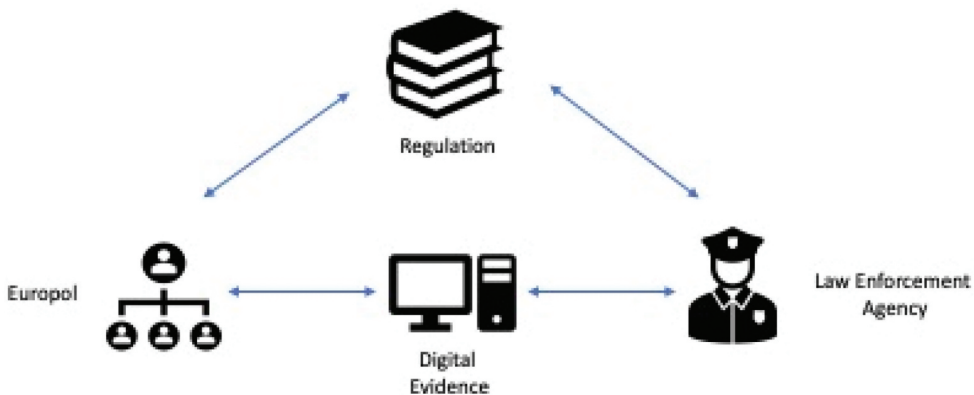


Figure 1. Current Sharing Decryption Platform Model.

Since 2016, EC3 and LEAs have been sharing their resources as peers for a noble cause to tackle cybercrime for the good of European citizens'. Exchange of their knowledge and resources is vital to investigate encrypted evidence because being unable to do so may turn into a security vulnerability. In the absence of talent and financial resources, the LEAs may not perform their duties. Their weaknesses can be exploited by crime groups and criminals can continue their modus operandi without fear of being caught. In that sense, knowledge and resource sharing between EC3 and national LEAs are well-suited with fundamental principles of sharing economy model such as being part of a community (cybersecurity) and sharing idle capacity (decrypting resources) for altruistic reasons (eradicating cybercrime). Therefore, the benefits of sharing economy platforms for peers should have a similar influence on LEAs who participated in the Europol's decrypting platform. In that regard, two significant variables of sharing economy model on peers, namely, 'reducing transaction cost' and 'trust building', will be discussed in the following two sections.

Reducing transaction cost

Reducing transaction cost is considered as one of the most significant advances in the sharing economy model for community members. Transaction cost deemed all costs between production and the customer's final price such as searching, contacting and contracting costs (Munger 2018; Aigrain and Aigrain 2012; Williamson 1985). The addition of each cost increases the market price of a product or service.

Sharing that allows temporary access to an asset is an alternative to ownership. Due to cost of sharing is generally lower than buying, it creates a consumer surplus which is the difference between the highest amount the customer is willing to pay and the actual amount paid (Sundararajan 2016). So, by sharing, all costs associated with the transaction remains in the pocket of the consumer. In this vein, sharing economy platforms allow the exchange of idle capacity of goods and services in a marketplace or a network. These platforms match supply and demand between people who have the idle capacity of assets and who need them. Hence, temporarily sharing goods or services in a community can be a more sustainable solution for those with limited resources (Jiang and Tian 2019). Community members can recover their resource gap by exchanging goods and services with each other without buying them. The lowering of transaction costs in that sense facilitates sharing goods and services and increases peers' commitment to the community (Chalmers Thomas, Price, and Schau 2012).

As often articulated by member states, most LEAs in the EU have lacked the human resources and technical infrastructure to cope with the encryption problem (The Council of the European Union 2016a). They need to acquire tacit knowledge from an outsourcing partner such as a private company with forensic expertise in decryption. However, outsourcing services from the private sector is an expensive procurement, contrary to popular belief.

Although no publicly available record was found during the research on how much the EU LEAs paid these private companies, payments made by the US and UK LEAs offer hints to how expensive these acquisitions have been (Hosenball 2016; Edwards 2016; Venkataramakrishnan 2020; Koepke et al. 2020). For instance, in the 2015 San Bernardino terrorist attack in the US, both the Federal Bureau of Investigation (FBI) and National Security Agency (NSA) were unable to decrypt the perpetrator's mobile phone, and as an investigator body, the FBI paid around \$1 million to an Israeli based company for decryption (Hosenball 2016; Edwards 2016). Similarly, UK policing agencies, including London Metropolitan Police and Police Scotland, paid a total of £4 million for two to three years contracts to their outsourcing partner specialised in decryption (Venkataramakrishnan 2020). A report prepared by a non-profit organisation, Upturn, also reveals widespread purchase of decryption tools by US LEAs ranging from a few thousand dollars to million-dollar contracts (Koepke et al. 2020). If the total amount paid by all US local LEAs is considered, it is clearer how sharing resources between LEAs is vital to reduce the

financial burden of substantial decryption costs. Especially for small LEAs, allocating their limited financial resources on decryption will impede their other operational capabilities and undermine their jurisdictional responsibilities. In the end, their impotence in decryption and weakness to outsource decryption service will turn into a public safety problem. The content of encrypted evidence will remain in mystery, and criminal cases will not be resolved.

In view of this, the five million Euros budget allocated for Europol to enhance its decryption capabilities is a modest investment compared to the purchases made by US and UK LEAs. If Europol can correspond to all member states expectations, Europol's decrypting platform will reduce transaction costs for national LEAs. National policing agencies will acquire decryption services from EC3 rather than private companies that are generally located out of the EU's borders. The money paid for these companies remains in the EU, which is another contribution to the digital sovereignty of the Union.¹ Moreover, the transaction cost of seeking an outsourcing partner and contracting costs will diminish for all member states.

Nevertheless, there is still an unanswered question of the efficiency of Europol's decryption platform. Considering 27 member states, including their national and local LEAs, the EC3's capabilities to respond all enquiries need to be monitored in the following years. According to a senior cybercrime unit representative of a European policing agency, Europol's decryption capacity may not be enough to respond all member states demands in the long run. This limitation would inevitably enforce Europol to prioritise critical cases rather than responding to all inquests (Interview_3). Furthermore, if Europol does not live up to the expectations of LEAs, European policing agencies continue investing in their domestic decryption capabilities rather than seeking help from Europol (Interviews 1 and 3).

Another critical point in this regard is the computational power that Europol's decryption platform has. According to a leading cybersecurity company expert, Europol has a strong decryption platform in terms of computational power. However, in the case of a using a random password, this platform might not work alone, and private sector's computational power might be needed to enhance Europol's decryption infrastructure. However, this resource sharing might still not work. For instance, to decrypt a twenty digits random password may take thousands of years even if all the computational power in the world is used (Interview 4). This time Europol might need the support of the private sector again to benefit from their quantum computer technology to tackle the decryption problem.

Building trust

Trusting a stranger is not easy for many people in cyberspace because of many uncertainties about the other side (Riles 2020; Bratianu 2018). Many clarifications are needed whether the person or entity in interaction is trustworthy or reliable while exchanging knowledge and assets. The trust became a more challenging issue between public and private partners in a cybersecurity context (Manley 2015). Lack of trust is listed as one of the top problems in P3s (Wall 2007; Carr 2016; Dunn-Cavelty and Suter 2009; Huey, Nhan, and Broll 2013). It is also a common problem in the EU not only between LEAs and private sector but also between Europol and LEAs, which has shown a considerable progress in recent years (Bossong and Wagner 2018).

Strong encryption is a big challenge for many LEAs, and the growing use of encryption by crime groups hinders police investigation capabilities. The LEAs cover their lack of expertise in purchasing different products and services from digital forensic companies' (Koepke et al. 2020). To unlock an encrypted device and extract data, digital evidence must be delivered to a private forensic expert. However, prior to that trust between LEAs and the private sector for evidence security must be ensured for a strong collaboration.

Digital evidence such as information stored in computers, other electronic devices or computer networks is ephemeral in nature. They can easily be altered, and traces of data manipulation cannot be detected (Chaikin 2006). Data alteration may also happen accidentally (Brown 2015). Therefore,

the forensic examination of digital evidence must be made with delicacy and sensitivity. It should be based on strict procedures. All forensic examination steps must be documented, and reliable forensic experts must conduct a forensic examination. Otherwise, during the criminal proceeding, it may not be considered valid evidence by the court. So, the chain-of-custody process is the crucial mechanism to prove the evidence is protected from tampering or alteration (Dubord 2008). The chain-of-custody process ensures digital data extract from an electronic device and is authentic data encoded on the device, and it is the same as it was initially discovered and sized (Sanett and Park 2000).

Considering private sector involvement in forensic examination of encrypted evidence, auditing the chain-of-custody process with private experts might not be easy for LEAs unless robust protocols and monitoring processes exist between public and private partners. Without a robust monitoring process, any alteration in digital evidence during the forensic examination cannot be proved by LEAs. The absence of a monitoring mechanism on evidence may undermine the fair trial principles of the criminal proceeding. In one of the examples provided in the Upturn report, a mobile phone seized by the Seattle Police Department has been shipped to Israel for forensic examination for a few weeks of forensic process (Koepke et al. 2020). As shown in this example, what kind of chain-of-custody procedures is followed between US-based policing agency and a private company in Israel is unknown during these weeks.

There are also uncertainties about whether any alteration happened during the evidence examination or what kind of safeguards ensured evidence security. Furthermore, in case of any legal violation linked with evidence security, which countries jurisdiction is prevailing and who will be liable for breaking the chain-of-custody procedures needs further clarification. In this respect, the European Commission's e-evidence proposal may improve legal certainty and clarity on processing digital evidence, rather than depending on the goodwill of private companies (Interview 1). However, the current e-evidence proposal regulates only obtaining digital evidence from online service providers inside and outside of the EU but does not cover private-sector responsibilities when they are assigned to examine digital evidence (European Commission 2021). Therefore, e-evidence proposal content needs to be broadened to include companies providing digital forensic examination to the LEAs and their liability to protect evidence from alterations.

Along with chain-of-custody concerns, choosing the right private company is another problem for LEAs that they must deal with. The LEAs have to collaborate with private experts qualified in decryption, have a clean, professional and criminal record, follow strict chain-of-custody procedure and offer reasonable pricing. The national authorities generally use vetting mechanisms to pick the right partner (Ilbiz 2019). However, due to the ephemeral nature of digital evidence and urgency of evidence processing, these long and detailed procurement processes may be skipped by LEAs and authorisation of private companies for the forensic examination can be determined without detailed scrutiny (Koepke et al. 2020; Gutheil et al. 2017).

Given these vulnerabilities in forensic examination of digital evidence, Europol's decryption platform has strong potential to eliminate the trust problem of national LEAs. The EC3 has already provided digital forensic services for member states under the EU jurisdiction and chain-of-custody procedures. Europol's decryption platform will be an addition to the existing services. Therefore, the trust-building initiatives essential for private companies is not relevant for Europol and EC3. In that sense, Europol's sharing platform will resolve the trust-building problem of LEAs while coping with the encryption problem in cyberspace.

Furthermore, the decryption platform of the EC3 is important for the EU's current shift towards digital sovereignty. Relying too much upon private sector has created fears of losing control of cybercrime data, and it may create inertia on European policing agencies of those who are unable to act independently while investigating cybercrime (Madiaga 2020). However, considering the dominance of the private sector in governing cyberspace, this sovereignty can be achieved only by sharing resources with the private sector to tackle cybercrime. Otherwise, digital sovereignty arguments might not go beyond a lofty ambition [Figure 2](#).

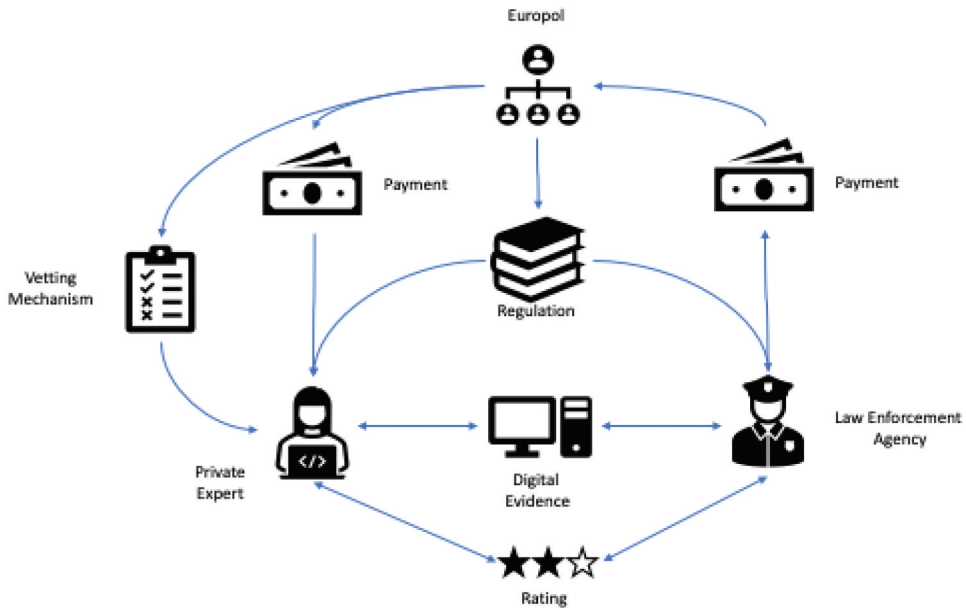


Figure 2. Proposed Sharing Decryption Platform Model.

Conclusion

Encryption is one of the most complex and politicized pieces of technology EU actors have dealt with in recent years. The Europol's decryption platform is one of the outcomes of heated discussions in the EU which is often centred between privacy and security. As argued in the sharing economy subsections, there are strong indications that the new platform will reduce transaction costs and trust problems for LEAs while outsourcing decryption services. However, functionality of the platform remains unclear whether the EC3 will be able to respond to all member countries enquiries. Considering the increasing number of people using encrypted communication networks and devices, the EC3 may not shoulder this responsibility alone in upcoming years and private sector participation might be inevitable. Similarly, the existing outsourcing model of LEAs for acquiring decryption service is also not sustainable for its high transaction costs and lack of trust towards their private partners. Therefore, Europol's existing decryption platform should draw inspiration from private sector examples. In this regard, one of the popular sharing economy platforms called 'Upwork' might be a good-fit to inspire Europol executives. Adopting Upwork model can enable a smooth private sector integration to Europol's decryption platform before the encryption becomes a more complicated and political technology for the LEAs.

According to proposed model, Upwork platform helps freelancers to share their information technology skills with customers who need them. The platform intermediates between two sides for transaction of payments, regulating interactions, resolving disputes and monitoring ratings. Furthermore, Upwork also tests the skills of freelancers to sustain a high quality service in the platform. In this model, Upwork only matches supply and demand without investing in assets or employees. The platform provides an entrepreneurial opportunity for people who have underused IT skills to reach a more significant customer network which might otherwise not be easy for them on their own. On the other hand, customers can hire talented IT professionals in a competitive market by getting a higher quality service with better price.

If this model can be adapted by Europol, decryption platform governed by EU policing agency can intermediate between LEAs and the private sector when they need to collaborate for decryption. Europol can create its own vetting mechanisms for private actors before they are accepted to the platform. The vetting procedure may include the background checks, security clearance procedures, verifying capabilities of private actors in chain-of-custody procedures and confidentiality mechanisms to protect digital evidence and seed information. Moreover, updating e-evidence rules that covers liabilities of private companies providing digital forensic services to the LEAs will also be helpful to regulate interoperability of digital data between LEAs and private actors those mostly located outside of the EU. Inclusion of a transparent pricing policy will also be in favour of the LEAs to compare different private actors and choose the best value service from high-rated service providers. The model inspired from Upwork thus can solve many P3 problems of Europol, LEAs and the private sector as discussed in this article.

In line with the general aim of the Special Issue, this article aimed to contribute to ongoing discussions in the EU about Europol's sharing decryption platform. It proposed a new P3 model based on sharing to cope with the changing landscape and nature of transnational digitalized threats across Europe. At the time of writing this article, Europol's decryption platform was nascent, and Europol was reluctant to share much information about this initiative. Based on insufficient empirical evidence, it is not easy to predict how the platform will evolve in the future. Its functionality will be tested in the following years when more empirical analysis will be available.

Interviews

Interview 1, Expert in Encryption and Democratic Governance for Europe.

Interview 2, Security Lead of a Major Cybersecurity Company.

Interview 3, Senior Member of a Cybercrime Unit in European Law Enforcement Agency.

Interview 4, Security Expert in a Leading Cybersecurity Company.

Note

1. Cellebrite (Israel), Magnet Forensics (Canada), Grayshift (US), BlackBag Technologies (US), AccessData (US), Oxygen Forensics (UK) and Belkasoft (US).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the European Commission [Jean Monnet Centre of Excellence, Jean Monnet Chair, Jean Monnet Network of EU Counterterrorism, and Marie Curie IEF].

ORCID

Ethem Ilbiz  <http://orcid.org/0000-0002-7205-9672>

Christian Kaunert  <http://orcid.org/0000-0002-4493-2235>

References

- Abelson, H., S. M. Ross Anerson, J. B. Bellovin, M. Blaze, W. Diffie, J. Gilmore, M. Green, et al. 2015. "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communication." *Journal of Cyber Security* 1 (1): 69–79.

- Aigrain, P., and S. Aigrain. 2012. *Sharing Culture and the Economy in the Internet Age*. Amsterdam: Amsterdam University Press.
- Albinsson, P. A., and B. Yasanthi Perera. 2012. "Alternative Marketplaces in the 21st Century: Building Community through Sharing Events." *Journal of Consumer Behaviour* 11 (4): 303–315. doi:10.1002/cb.1389.
- Anderson, M., and A. Joanna, eds. 2002. *Police and Justice Co-operation and the New European Borders*. The Hague: Kluwer Law International.
- Bardhi, F., and G. M. Eckhardt. 2012. "Access-Based Consumption: The Case of Car Sharing." *Journal of Consumer Research* 39 (4): 881–898. doi:10.1086/666376.
- Belk, R. 2014. "Sharing versus Pseudo-Sharing in Web 2.0." *The Anthropologist* 18 (1): 7–23. doi:10.1080/09720073.2014.11891518.
- Bossong, R., and B. Wagner. 2018. "A Typology of Cybersecurity and Public-private Partnership in the Context of the EU." In *Security Privatization*, edited by O. Bures and H. Carrapico, 219–247. Cham: Springer.
- Botsman, R., and R. Rogers. 2010. *What's Mine Is Yours: The Rise of Collaborative Consumption*. New York: Harper Business.
- Bratianu, C. 2018. "The Crazy New World of the Sharing Economy." In *Knowledge Management in the Sharing Economy: Cross-Sectoral Insights into the Future of Competitive Advantage*, edited by E.-M. Vătămănescu and F. M. Pînzaru, 3–18. Cham: Springer International Publishing.
- Briere, C. 2018. "Cooperation of Europol and Eurojust with External Partners in the Fight against Crime: What are the Challenges Ahead?" *Brexit Institute Working Paper* N.1.
- Briere, C. 2019. "Cooperation of Europol and Eurojust with External Partners in the Fight against Crime: A Legal Appraisal." In *The External Dimension of EU Agencies and Bodies*, edited by C. H. Herwig, E. V. Hofmann, and M. Chamon, 59–77. Cheltenham: Edward Elgar Publishing.
- Brown, C. S. D. 2015. "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice." *International Journal of Cyber Criminology* 9 (1): 55–119.
- Bures, O. 2011. *EU Counterterrorism Policy: A Paper Tiger?* Farnham: Ashgate.
- Busuoiuc, M., and M. Groenleer. 2013. "Beyond Design: The Evolution of Europol and Eurojust." *Perspectives on European Politics and Society* 14 (3): 285–304. doi:10.1080/15705854.2013.817803.
- Carr, M. 2016. "Public-private Partnerships in National Cyber-security Strategies." *International Affairs* 92 (1): 43–62. doi:10.1111/1468-2346.12504.
- Carrapiço, H., and A. Barrinha. 2017. "The EU as a Coherent (Cyber) Security Actor?" *Journal of Common Market Studies* 55 (6): 1254–1272. doi:10.1111/jcms.12575.
- Carrapiço, H., and B. Farrand. 2017. "Dialogue, Partnership and Empowerment for Network and Information Security: The Changing Role of the Private Sector from Objects of Regulation to Regulation Shapers." *Crime, Law, and Social Change* 67 (3): 245–263. doi:10.1007/s10611-016-9652-4.
- Carrapiço, H., and B. Farrand. 2020. "Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy." *Journal of European Integration* 42 (8): 1111–1126. doi:10.1080/07036337.2020.1853122.
- Carrapiço, H., and F. Trauner. 2013. "Europol and Its Influence on EU Policy-making on Organized Crime: Analyzing Governance Dynamics and Opportunities." 14 (3): 357–371.
- Chaikin, D. 2006. "Network Investigations of Cyber Attacks: The Limits of Digital Evidence." *Crime, Law, and Social Change* 46 (4): 239–256. doi:10.1007/s10611-007-9058-4.
- Chalmers Thomas, T., L. L. Price, and H. J. Schau. 2012. "When Differences Unite: Resource Dependence in Heterogeneous Consumption Communities." *Journal of Consumer Research* 39 (5): 1010–1033. doi:10.1086/666616.
- Christensen, C. M., M. E. Raynor, and M. Rory. 2015. "What Is Disruptive Innovation?" *Harvard Business Review*. December.
- Cohen, M., and C. Zehngebot. 2014. "What's Old Becomes New: Regulating the Sharing Economy." *Boston Bar Journal* 58: 6.
- Coman-Kund, F. 2018. "Europol's International Cooperation between 'Past Present' and 'Present Future': Reshaping the External Dimension of EU Police Cooperation." *Europe and the World* 2 (1): 1–37.
- Coman-Kund, F. 2020. "Europol's International Exchange of Data and Interoperability of AFSJ Databases." *European Public Law* 26 (1): 181–204.
- Comey, J. B. 2014. "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" Brookings Institution, Accessed 15 July 2021. <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>
- The Council of the European Union. 1997. Joint Action Adopted by the Council on the Basis of Article K.3 of the Treaty on European Union, Establishing a Mechanism for Evaluating the Application and Implementation at National Level of International Undertakings in the Fight against Organized Crime Brussels Official Journal of the European Communities
- The Council of the European Union. 2016a. Encryption of data: Mapping of the problem.
- The Council of the European Union. 2016b. Justice and Home Affairs: Outcome of the Council Meeting.

- The Council of the European Union. 2017. *The Practical Implementation and Operation of the European Policies on Prevention and Combating Cybercrime*. Brussels.
- The Council of the European Union. 2020. *Security through Encryption and Security despite Encryption*. Brussels.
- De Bolle, C. 2020. "The Role of Europol in International Interdisciplinary European Cooperation" *European Law Enforcement Research Bulletin* 19, 13–24.
- Deflem, M. 2006. "Europol and the Policing of International Terrorism: Counterterrorism in a Global Perspective." *Justice Quarterly* 23 (3): 336–359. doi:10.1080/07418820600869111.
- Drewer, D., and V. Miladinova. 2017. "The BIG DATA Challenge: Impact and Opportunity of Large Quantities of Information under the Europol Regulation." *Computer Law and Security Review* 33 (3): 298–308. doi:10.1016/j.clsr.2017.03.006.
- Dubord, P. 2008. "Investigating Cybercrime." In *Handbook of Digital and Multimedia Forensic Evidence*, edited by J. J. Barbara, 77–89. Totowa, NJ: Humana Press.
- Dunn-Cavelty, M., and M. Suter. 2009. "Public–Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection." *International Journal of Critical Infrastructure Protection* 2 (4): 179–187. doi:10.1016/j.ijcip.2009.08.006.
- Eckes, C., and K. Theodore, eds. 2011. *Crime within the Area of Freedom, Security and Justice: A European Public Order*. Cambridge: Cambridge University Press.
- Edwards, J. 2016. "FBI Paid More than \$1.3 Million to Break into San Bernardino iPhone." *Reuters*, Accessed 14 February 2021. <https://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB>.
- European Commission. 2017. Eleventh progress report towards an effective and genuine Security Union. Brussels.
- European Commission. 2020. *The EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe*. Brussels.
- European Commission. 2021. *E-evidence: Cross-border Access to Electronic Evidence*. Brussels.
- Europol, 2016a, "13 Countries Join the Global Fight against Ransomware," <https://www.europol.europa.eu/newsroom/news/13-countries-join-global-fight-against-ransomware-0>.
- Europol, 2016b, "EC3 and the EC Joint Research Centre Tackle the Challenge of Encrypted Material for Law Enforcement Investigations", <https://www.europol.europa.eu/newsroom/news/ec3-and-ec-joint-research-centre-tackle-challenge-of-encrypted-material-for-law-enforcement-investigations>.
- Europol. 2016c. "Forensics". Accessed 08 February 2021. <https://www.europol.europa.eu/activities-services/services-support/forensics>
- Europol, 2016d, "No More Ransom: Law Enforcement and IT Security Companies Join Forces to Fight Ransomware," <https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware>.
- Europol, 2018, "Join the Global 'No More Ransom' Initiative to Help More Victims Fight Back," <https://www.europol.europa.eu/newsroom/news/join-global-%E2%80%99no-more-ransom%E2%80%99-initiative-to-help-more-victims-fight-back>.
- Europol, 2020, "Europol and the European Commission Inaugurate New Decryption Platform to Tackle the Challenge of Encrypted Material for Law Enforcement Investigation," <https://www.europol.europa.eu/newsroom/news/europol-and-european-commission-inaugurate-new-decryption-platform-to-tackle-challenge-of-encrypted-material-for-law-enforcement>
- Fletcher, M., R. Lööf, and B. Gilmore. 2008. *EU Criminal Law and Justice*. Cheltenham: Edward Elgar.
- Gutheil, M., Q. Liger, A. Heetman, J. Eager, and M. Crawford. 2017. *Legal Framework for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*.
- Hamari, J., M. Sjöklint, and A. Ukkonen. 2015. "The Sharing Economy: Why People Participate in Collaborative Consumption." *Journal of the Association for Information Science and Technology* 67: 9.
- Hodkinson, P. 2011. *Media, Culture and Society: An Introduction*. London. Los Angeles: SAGE.
- Hosenball, M. 2016. "FBI Paid under \$1 Million to Unlock San Bernardino iPhone: Sources." *Reuters*, Accessed 14 February 2021. <https://www.reuters.com/article/us-apple-encryption/fbi-paid-under-1million-to-unlock-san-bernardino-iphone-sources-idUSKCN0XQ032>.
- Huey, L., J. Nhan, and R. Broll. 2013. "'Uppity Civilians' and 'Cyber-vigilantes': The Role of the General Public in Policing Cyber-crime." *Criminology & Criminal Justice* 13 (1): 81–97. doi:10.1177/1748895812448086.
- Ilbiz, E. 2019. "The Uberization of the United Nations' Regime to Prevent the Online Financing of Terrorism: Tackling the Problem of Obfuscation in Virtual Currencies." *Journal of Cyber Policy* 4 (3): 404–424. doi:10.1080/23738871.2019.1666892.
- JHA Council. 2008. Council Conclusions on a Concerted Work Strategy and Practical Measures against Cybercrime. (Brussels).

- Jiang, B., and L. Tian. 2019. "The Strategic and Economic Implications of Consumer-to-Consumer Product Sharing." In *Sharing Economy: Making Supply Meet Demand*, edited by H. Ming, 37–54. Cham: Springer International Publishing.
- John, N. A. 2013a. "Sharing and Web 2.0: The Emergence of a Keyword." *New Media & Society* 15 (2): 167–182. doi:10.1177/1461444812450684.
- 2013b. "The Social Logics of Sharing." *The Communication Review*. 16 (3)113–131. 10.1080/10714421.2013.807119
- Kaunert, C. 2010. "Europol and EU Counter-terrorism: International Security Actorness in the External Dimension?" *Studies in Conflict and Terrorism* 33 (7): 652–671. doi:10.1080/1057610X.2010.484041.
- Koepke, L., E. Weil, U. Janardan, T. Dada, and Y. Harlan. 2020. *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*. Upturn. <https://www.upturn.org/reports/2020/mass-extraction/>.
- Konig, F. 2020. *Big Data, 5G, and AI: How Europol could help von der Leyen achieve her goals* Hertie School Jaques Delors Centre Policy Paper (Berlin).
- Koomen, M. 2019. *The Encryption Debate in the European Union*. Carnegie Endowment for International Peace (Washington).
- Koomen, M. 2021. *The Encryption Debate in the European Union: 2021 Update*. Carnegie Endowment for International Peace (Washington).
- Lavranos, N. 2003. "Europol and the Fight against Terrorism." *European Foreign Affairs Review* 8: 259–275.
- Lomas, N. 2016. "Encryption under Fire in Europe as France and Germany Call for Decrypt Law." Accessed 13 February 2021. https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/?guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2x1LmNvbS58&guce_referrer_cs=sMnhNkTqBEB3VgCB0PgRA&gucounter=2.
- Madiaga, T. 2020. "Digital Sovereignty for Europe." *EPRS Ideas Paper* 651.992.
- Manley, M. 2015. "Cyberspace's Dynamic Duo Forging a Cybersecurity Public-Private Partnership." *Journal of Strategic Security* 8 (3): 85–98. doi:10.5038/1944-0472.8.3S.1478.
- Mitsilegas, V., and F. Giuffrida. 2017. "The Role of EU Agencies in Fighting Transnational Environmental Crime: New Challenges for Eurojust and Europol." *Transnational Crime* 1 (1): 1–150. doi:10.1163/24680931-12340001.
- Monsees, L. 2019. *Crypto-Politics: Encryption and Democratic Practices in the Digital Era*. London: Routledge.
- Morbin, T. 2020. "Strong Crypto and Policing: EU Again Debates Encryption." *Data Breach Today*, Accessed 11 February 2021. <https://www.databreachtoday.asia/strong-crypto-policing-eu-again-debates-encryption-a-15392>.
- Munger, M. C. 2018. *Tomorrow 3.0: Transaction Costs and the Sharing Economy*. Cambridge Studies in Economics, Choice, and Society. Cambridge: Cambridge University Press.
- Neil, R., E. Disley, D. Potoglou, A. Reding, D. M. Culley, M. Penny, M. Botterman, G. Carpenter, C. Blackman, and J. Millard. 2012. Feasibility Study for a European Cybercrime Centre: RAND Corporation.
- O'Rourke, D., and N. Lollo. 2015. "Transforming Consumption: From Decoupling, to Behavior Change, to System Changes for Sustainable Consumption." *Annual Review of Environment and Resources* 40 (1): 233–259. doi:10.1146/annurev-environ-102014-021224.
- Ochchipinti, J. D. 2003. *The Politics of EU Police Cooperation: Towards a European FBI?* Boulder, CO: Lynne Rienner.
- Pisarić, M. 2020. "Encryption As A Challenge For European Law Enforcement Agencies " Thematic Conference Proceedings of International Significance, Belgrade, 18-19 November 2020.
- Riles, A. 2020. "Building Platforms for Collaboration: A New Comparative Legal Challenge". In *Legal Tech and the New Sharing Economy*, edited by M. C. Compagnucci, N. Forgó, T. Kono, S. Teramoto, and E. P. M. Vermeulen, 15–20. Singapore: Springer Singapore.
- Ryder, S. 2016. "The End of Effective Law Enforcement in the Cloud? to Encrypt, or Not to Encrypt." IEEE 9th International Conference on Cloud Computing.
- Sanett, S., and E. Park. 2000. "Authenticity as a Requirement of Preserving Digital Data and Records." *IASSIST Quarterly* 24 (1): 15. doi:10.29173/iq578.
- Sedkaoui, S., and M. Khelfaoui. 2020. *Sharing Economy and Big Data Analytics*. *Sharing Economy and Big Data Analytics*. London: Wiley and Sons.
- Severson, D. 2017. "The Encryption Debate in Europe", *A Hoover Institution Essay*, Aegis Paper Series No. 1702.
- Stupp, C. 2016. "EU Cybersecurity and Police Chiefs Reach Breakthrough Agreement on Encryption." Accessed 12 February 2021. <https://www.euractiv.com/section/digital/news/eu-cybersecurity-and-police-chiefs-reach-breakthrough-agreement-on-encryption>.
- Stupp, C. 2017. "Brussels Promises More Police Access to Encrypted Data, but No Backdoors." Euractiv. Accessed 10 February 2020. <https://www.euractiv.com/section/data-protection/news/brussels-promises-more-police-access-to-encrypted-data-but-no-backdoors>.
- Sundararajan, A. 2016. *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism*. Massachusetts: MIT Press.
- TUECS. 2020. "The Uberization of Europol's Cybercrime Strategy: An Innovative Governance Model on Public-Private Partnership". Accessed 01 July 2021. <https://cordis.europa.eu/project/id/886141>

- Van Gemert, W., 2019, "Update on European Cybercrime Centre (EC3) Activities," http://www.parl2019ro.eu/eu/HTP_BLOB?id=4007&tip=pdf&blb=3.
- Venkataramakrishnan, S. 2020. "UK Police and Other Investigators Spend £4m on Phone Hacking Software." *Financial Times* 2020. Accessed 14 February 2021. <https://www.ft.com/content/309e83ac-76a0-49c1-bbd2-f4ebe04ce58c>.
- Wainwright, R., and F. J. Cilluffo. 2017. *Responding to Cybercrime at Scale: Operation Avalanche – A Case Study*. Center for Cyber and Homeland Security, Issue Brief 2017-03.
- Wall, D. S. 2007. "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace." *Police Practice and Research* 8 (2): 183–205. doi:10.1080/15614260701377729.
- Weyemergh, A., I. Armada, and C. Briere. 2015. "Competition or Cooperation: State of Play and Future Perspectives on the Relations between Europol, Eurojust and the European Judicial Network." *New Journal of European Criminal Law* 6 (2): 258–287. doi:10.1177/203228441500600207.
- Williamson, O. E. 1985. *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*. New York; London: Free Press; Collier Macmillan.