EXAMINING THE CHALLENGES OF POLICING ECONOMIC CYBERCRIME IN THE UK

Naci AKDEMİR[*] Bülent SUNGUR[**] Bürke Uğur BAŞARANEL[***]

Abstract

Cybercrime has received the 'Tier One' national security risk status in many countries due to the increased cyber threats. In response to this severe threat, governments have announced a substantial amount of investment in cybercrime prevention programmes. It is evident that tackling cybercrime requires expertise and cybersecurity skills as the networked global nature of the Internet pose significant challenges to policing cybercrime. Previous policing cybercrime studies illustrated that local police officers lack the technical skills, which obviously hampered the fight against cybercrime. Police forces continue enhancing their ability to tackle cybercrime through specialised cybercrime units. Nevertheless, there is a dearth of empirical research examining policing problems of economic cybercrime through the lenses of expert police officers working in cybercrime departments. This empirical research addresses this knowledge gap in the literature. A thematic analysis method was employed to analyse semi-structured interviews conducted with expert police officers working at cybercrime departments in the United Kingdom.

Lack of international cooperation, underreporting of economic cybercrime incidents and lack of victim awareness emerged as key challenges. Police officers' views regarding private sector involvement in policing economic cybercrime appear to be tentative due to ethical concerns. Public-private partnership in combatting cybercrime appears to be an effective solution to enhance the effectiveness of combatting cybercrime. European Union (EU)'s new Cybersecurity Act (Regulation 2019/881), which restructures the European Union Agency for Network and Information Security (ENISA) is the latest example of public-private partnership in combatting cybercrime. However, the results of this study suggest that the scope of this initiative should be extended to non-EU countries to maintain global cybersecurity.

Keywords: *Cybercrime, Cybersecurity, Policing, Public-Private Partnership, Economic Cybercrime*

[*] Dr., Öğretim Görevlisi, Jandarma ve Sahil Güvenlik Akademisi, naciakdemir@jandarma.gov.tr ORCID: https://orcid.org/0000-0002-4288-6482

[**] Öğretim Görevlisi, Jandarma ve Sahil Güvenlik Akademisi, bulentsunger@gmail.com ORCID: https://orcid.org/0000-0002-0705-0049

*** Dr., Öğretim Görevlisi, Jandarma ve Sahil Güvenlik Akademisi, bubasaranel@gmail.com ORCID: https://orcid.org/0000-0003-4760-2925

Makale Geliş Tarihi: 28.10.2019 Makale Kabul Tarihi: 09.01.2020

BİRLEŞİK KRALLIKTA SİBER EKONOMİK SUÇLARA YÖNELİK KOLLUK FAALİYETLERİ SORUNLARININ İNCELENMESİ

Öz

Artan siber tehditler nedeniyle siber suçlar pek çok ülke tarafından 'Birinci Öncelikli' ulusal güvenlik riski olarak nitelendirilmektedir. Bu ciddi riske tepki olarak hükümetler siber suçların önlenmesi programlarına ciddi yatırımlar yapmaktadır. Internetin ağlarla birbirine bağlı küresel karakterinin siber suçların kolluğuna ciddi zorluklar yaratması nedeniyle, siber suçlarla etkin mücadele için uzmanlığa ve teknik yeteneklere ihtiyaç duyulduğu aşikârdır. Siber suçların kolluğu hakkındaki önceki bilimsel araştırmalar yerel polisin uzmanlık eksikliğinin olduğunu ve bunun siber suçlarla mücadeleyi sekteye uğrattığını ortaya koymaktadır. Kolluk kuvvetleri siber suçlarla mücadele kapasitelerini arttırmak kapsamında uzman siber suçlarla mücadele birimlerini ihdas etmeye devam etmektedir. Fakat literatürde siber ekonomik suçlarla mücadele eden uzman birimlerin karşılaştığı sorunları uzman kolluk kuvvetlerinin gözünden ortaya koyan çalışma sayısının az olması dikkat çekicidir. Literatürdeki bu bilgi açığını gidermek maksadıyla Birleşik Krallık siber suçlarla mücadele birimlerinde görevli uzman polis memurları ile icra edilen yarı yapılandırılmış mülakatlardan elde edilen veriler tematik analiz yöntemi ile analiz edilmiştir.

Uluslararası işbirliği eksikliği, suç olaylarının kolluğa yeterince bildirilmemesi ve mağdurların siber suçlar farkındalık eksikliği en önemli sonuçlar olarak ortaya çıkmıştır. Özel firmaların siber ekonomik suçların kovuşturulmasına katılımı konusunda ise polis memurlarının etik kaygılar nedeniyle çekimser oldukları görülmüştür. Siber suçlarla mücadelede kamu-özel sektör işbirliğinin siber suçlarla mücadelenin etkinliğini arttıracak önemli bir çözüm olduğu değerlendirilmektedir. Avrupa Birliği (AB)'nin Ağ ve Bilgi Güvenliği Ajansı (ENISA)'nı yeniden yapılandıran yeni siber güvenlik yasası (Regulation 2019/881) siber suçlarla mücadelede kamu-özel sektör işbirliği kapsamda atılmış önemli bir adımdır. Fakat çalışmamızın sonuçları siber güvenliğin dünya çapında sağlanması için bu inisiyatifin AB üyesi olmayan ülkeleri de kapsaması gerekliliğini ortaya koymaktadır.

Anahtar Kelimeler: *Siber Suçlar, Siber Güvenlik, Suçların Kolluğu, Kamu-Özel Sektör İşbirliği, Siber Ekonomik Suçlar*

INTRODUCTION

The advent of the Internet and its commercial applications have significantly changed the way we socialise, shop or communicate. However, the widespread use of the Internet is not free from its problems. It is argued that the commercial application of the Internet has not only provided new opportunities for the commission of the traditional crime, but it has also given rise to new forms of crimes (Wall, 2007b; Lee, Holt, Burruss, and Bossler, 2019).

Recent research illustrates that cybercrime is the fastest grown crime in the world (Graham, 2017; Summerville, 2017). It is predicted that 23% of United States (US) population experienced cybercrime victimization in 2018 (Reinhart, 2018). Similarly, Action Fraud reported that Internet users lost £34.6m as a result of cybercrime between April and September 2018, which indicates a %24 rise when compared to the previous 6 months (BBC, 2019).

This increased cyber threat has caused public tension, which motivated national and international bodies to put cybercrime and cybersecurity on top of their agendas (Kshetri, 2013; Wall and Williams, 2014; Holt, Burruss, and Bossler, 2018). Hence, combatting and policing cybercrime have increasingly been stressed in many national and international documents (i.e. The Council of Europe Cybercrime Convention (ETS No. 185), The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (2000)).

Despite growing public concern fuelled by the increased number of cyber-attacks, adverse financial and psychological impacts of cybercrime, there is a dearth of empirical research examining policing problems of economic cybercrime through expert police officers' lenses. This empirical research aims to address this knowledge gap in the literature by discerning policing problems of economic cybercrime in the UK.

1. LITERATURE REVIEW

The first part of the literature review deals with two controversial issues in cybercrime literature: definition of cybercrime and the novelty of cybercrime. The second part of the review outlines previous empirical research related to the policing problems of cybercrime and perceptions of police officers.

1.1. Defining Cybercrime

It is generally considered that there is a lack of agreement around a standard definition of the cybercrime in the literature (Wall, 2008; Anderson, Barton, Böhme, Clayton, Van Eeten et al., 2013; Williams and Levi, 2015). The Council of Europe Cybercrime Convention (ETS No. 185), which is also known as Budapest Convention, is one of the first international initiatives to create a shared understanding of cybercrime (Wall, 2013a), though the convention caused significant discomfort regarding its imbalance between public liberties and power delegated to governments about surveillance, search and seizure of computers (Taylor, 2002). Rather than providing an umbrella definition, this convention

highlights the importance of deterrence. The Convention defines the scope of the deterrence as "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct" (The Council of Europe Convention on Cybercrime, 2001: 2), and presents sub-categories of cybercrime within four titles. A number of cybercrimes were defined within these four categories. However, this approach received criticism from the authors as it does not include some sorts of cybercrime like stalking, extortion (Brenner, 2007), online identity theft, and spamming (Clough, 2014).

Commission of the European Communities also published a communication to the European Parliament about combatting cybercrime in 2007. This report defines cybercrime as "criminal acts committed using electronic communications networks and information systems or against such networks and systems" (European Commission, 2007: 2). Contrary to the Council of Europe's broad definition, Commission perceives cybercrime in a narrow sense. This definition again excludes the cases related to illicit online activities.

United Nations is another international actor that dealt with cybercrime-related issues. The United Nations manual on the prevention and control of computer-related crime (1994) uses the terms, computer crime and computer-related crime interchangeably. This manual did not provide any definition. It emphasised the fact that traditional crimes such as theft, fraud and forgery can be associated with computer crime. The manual also stated establishing a distinction between illicit and unlawful activities was mandatory (UN Manual, 1994). The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders was another significant occasion where cybercrime-related issues were discussed. During the workshops two cybercrime definitions were formed:

a) "any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them."

b) "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network" (UN Congress, 2000: 5). While the former defines the cybercrime in a narrow sense as computer crime, the latter describes it in a broader sense as a computer-related crime.

A definition of the cybercrime can also be found in the Commonwealth of Independent States Agreement. The act without referring the term cybercrime defines[1] it as "a criminal act of which the target is computer information" (as cited in Akhgar, Choras, Brewster, Bosco, Veermeersch et al., 2016: 298). This definition focuses on crimes against computers and leaves out the occasions where computers or networked technologies are used to commit crimes online.

Shanghai Cooperation Organization (SCO) Agreement[2] provides a definition of cybercrime in its Annex as "the use of information resources and (or) the impact on them in the informational sphere for illegal purposes", however, agreement prefers the term information offences (as cited in Malby, Mace, Holterhof, Brown, Kascherus et al., 2013: 12). This definition also focuses on crimes related to information technologies and omits offences and illicit activities against individuals. The constant omission of the term cybercrime from these documents may be the sign of the political stances of participating countries.

With regards to academic efforts to define cybercrime, while some scholars (i.e. Thomas and Loader, 2000; Gordon and Ford, 2006; Koops, 2010; Kshetri, 2010a; Casey, 2011; Pathak, 2016) strived to create a definition of the cybercrime, some others (Gordon and Ford, 2006; Wall, 2007a; Brenner, 2010) preferred to provide a typology of cybercrime. The two most popular definitions of cybercrime will be examined below.

A search on academic databases such as Google Scholar and ProQuest was conducted to find out the most popular definition of cybercrime. The search result indicated that the definitions provided by Thomas and Loader (2000) and Gordon and Ford (2006) were the most frequently cited definitions in academic papers related to cybercrime. Thus, these two definitions will be juxtaposed to each other. Thomas and Loader (2000: 3) define cybercrime as *"computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks"* whereas Gordon and Ford (2006: 14) define it as *"any crime that is facilitated or committed using a computer, network, or hardware device"*. While the former definition involves illicit behaviours that are not defined as delinquent, the latter refers to only specific

[1] The original language of the Commonwealth of Independent States Agreement is Russian. Thus, it is cited from another source.

[2] Due to unavailability of the English version of the Shanghai Cooperation Organization (SCO) Agreement, it is cited from another source.

actions that are a crime. In this aspect, the description provided by Thomas and Loader (2000) covers a wide range of activities ranging from illicit ones like distributing Internet users' personal information (Gercke, 2012) or illegal ones such as spamming (Wall, 2005). Furthermore, the latter definition not only includes actions mediated through networked technologies but it also covers the crimes to be committed via hardware devices, though, the former does not include activities facilitated with devices like iPads or smartphones (Blanco Hache and Ryder, 2011; Dolliver and Poorman, 2018) or memory sticks containing malware (Gercke, 2012).

This section of the literature review has presented some common definitions of cybercrime. The next section aims to provide a synopsis of arguments regarding the novelty of cybercrime.

The argument that whether there is such a thing like cybercrime is one of the controversial issues in cybercrime literature. Whereas some scholars such as Grabosky (2001)) and (Brenner, 2001, 2004) argue that cybercrime is the continuum of the terrestrial crimes, others (Yar, 2005; Wall, 2007a; Sandywell, 2013) argue that cybercrime, which is driven by new Internet technologies, is a new form of crime.

1.2 The Novelty of Cybercrimes

Brenner (2001, 2004) evaluates the existence of cybercrime as a distinct type of crime from a law perspective. Brenner (2001) juxtaposed real-world crimes such as burglary, theft and fraud with their cyber counterparts. *"The mens rea"* (a culpable mental state)*, "the actus reus" (act or failure), "attendant circumstances" (conditions that lead crime) and "harm*" are the four criteria that Brenner (2001: 4) uses in her analysis. She contends that although the use of Internet technologies has slightly changed the nature of real-world crimes in cyberspace, they still cause the same harm (Brenner, 2001; 2004). It is asserted that each type of cybercrime has a correspondent crime in the real world. For instance, vandalism can be considered as the real world analogy of hacking (Petee, Corzine, Huff-Corzine, Clifford, and Weaver, 2010).

Furthermore, Grabosky (2001), who focuses on the use of the Internet technologies in the commission of the crimes, asserts that there is no qualitative distinction between real-world and cyberspace while both environments serve as a scene of the crime. He argues that Internet technologies are utilised as a tool to

commit terrestrial crimes in cyberspace; hence, cybercrimes cannot be considered as new types of crimes. They are just the continuation of real-world crimes (Grabosky and Smith, 2001).

However, Yar (2005) argues that there is a discontinuity between real-world crimes and virtual crimes. He argues that virtual space creates unique opportunities for the commission of the new genre of crimes, which cannot be committed in the real world. Phishing, malware infection or cyberstalking are examples of this kind of new types of online crimes (Yar, 2005). Wall (2007) argues that the Internet technologies have not only created new opportunities for the offenders, but they have also changed the nature of real-world crimes. Wall proposes a transformation test to distinguish between cybercrimes and real-world crimes. Based on this transformation test, he argues that there are certain types of new crimes, which are impossible to be committed in the absence of Internet technologies. He dubs these kinds of crimes as "true cybercrimes" (Wall, 2004, p.10; 2007, p.48). Malware infection or phishing would no longer be committed should the Internet, and networked technologies are removed from the content of these crimes. With his transformation test, Wall (2007) clearly shows that some forms of cybercrimes are unique to cyberspace and require special attention, as they can be the facilitator of the more severe crimes such as economic cybercrimes.

Overall, considering cybercrime as a new genre of crime has some significant implications for policymakers and law. As it will be highlighted in the following sections, the perspectives evaluating cybercrime as the continuation of terrestrial crimes hinder introduction of new laws and regulations addressing specifically to cybercrimes, which in turn pose challenges to policing cybercrime. The next section discusses the evolving concept of policing.

The concept of the policing has evolved, and it is no longer restricted to public police (Yar, 2013a; Button, 2019). Bayley and Shearing (1996: 588) argue that "police are no longer the primary crime-deterrent presence in society; they have been supplanted by more numerous private providers of security." As for policing cybercrime, the situation is no different. Several non-state actors such as Internet services providers, social network services (i.e. Facebook, Twitter) and NGOs (i.e. Internet Watch Foundation or The SANS Institute) may have several responsibilities in regulating and governing the Internet (Yar, 2013b). Wall (2010: 17) defines these bodies involved in the regulation and the governance of the Internet as "cybersecurity assemblage."

1.3. The Evolving Nature of Policing Cybercrime

Besides these non-profit organizations, the for-profit private sector has increasingly involved in the governance of the Internet. Reduced investment costs and availability of the external expertise are the rationales for the privatisation of policing cybercrime (Yar, 2013b; Boes and Leukfeldt, 2017; Finn, 2019). The increased volume of private companies providing security in cyberspace created an opportunity for governments to allocate the responsibility of providing protection for cybercrime threats through the public-private partnership. Responsibilization strategy, which Garland (1996: 452) defines as "central government seeking to act upon crime not in a direct fashion through state agencies (police, courts, prisons, social work, etc.) but instead by acting indirectly, seeking to activate action on the part of non-state agencies and organizations.", is at the heart of this approach. European Network and Information Security Agency (ENISA) and The National Cyber Security Centre of the UK are the examples of public-private partnership, which refers to the collaboration between governmental agencies and private sector, to prevent cybercrime and provide cybersecurity in Europe.

However, privatisation of law enforcement is not free from its problems. Research on the privatisation of policing of traditional crimes suggests the presence of the concerns around fair investigations, authority abuses and protecting companies' interests rather than public interest (Ruddell, Thomas, and Patten, 2011; Joh, 2019; Lam, 2019). Whether the same concerns are valid for the privatisation of policing cybercrime is vague. Identifying the advantages and the pitfalls of private policing of economic cybercrime through police officers' views in the case of the UK was another goal of this empirical study.

This section of the paper reviews the empirical research examining the challenges police officers experienced while policing cybercrime.

1.4. Challenges of Policing Cybercrime

Holt, Bossler, and Fitzgerald (2010) conducted survey-based research to investigate local law enforcement agencies' awareness of, preparedness for and perceptions of cybercrime. The result of this study suggested that a major of the police officer participants acknowledge the lack of expertise and need for expert agencies to conduct the investigations in cyberspace. Limited capacity and resources to combat cybercrime emerged to be another outcome of this study.

Bossler and Holt (2012) examined local police officers' views toward their perceived role in responding to cybercrime. Their research based on the dataset collected from the police officers working in two local police departments in the southeast part of the United States. The survey results suggested that local police officers had limited knowledge to respond to cybercrime incidents. Approximately 80% of police officers expressed a degree of reluctance to be involved in cybercrime cases. Regarding police response to cybercrime incidences, 63,5% of police officers acknowledged that most cybercrime incidents were not reported to the police.

Bond and Tyrrell (2018) analysed the national online survey of police understanding of revenge pornography UK 2017. The results of their analysis indicated that police officers lacked the knowledge pertaining to revenge pornography legislation. For example, 80,6% of respondents acknowledged that they would not know how to collect information while conducting revenge pornography cases. Moreover, while only 1,2% of police respondents reported having an excellent understanding of revenge pornography, 5,9% of the respondents acknowledged having no knowledge at all.

The findings of Hadlington, Lumsden, Black, and Ferra (2018) who interviewed sixteen frontline police officers suggested difficulties in keeping up with the pace of developments, ambiguity around the definition of cybercrime and inadequate training as the problems public police officers faced while conducting cybercrime investigations.

Holt, Lee, Liggett, Holt, and Bossler (2019) investigated police officers' views on online harassment and seriousness of the interpersonal crimes (harassment and cyberbullying) within the sample of 1,348 constables in England and Wales. Their research illustrated that most police participants perceived online harassment as a less severe crime. Constables' negative perceptions related to the seriousness of online harassment emerged to diminish their eagerness to handle online interpersonal crimes.

Lee et al. (2019) examined local police officers' attitudes toward cybercrime through a web-based survey conducted with 155 inspectors working at cybercrime departments in England and Wales. The result of this study illustrated that police officers working in cybercrime departments perceived interpersonal and online financial crimes as severe as traditional crimes. For instance, 42,6% of participants perceived stealing money from individuals' bank accounts equivalent to stealing

the same amount of money from their pockets. Additionally, 44,5% of responders agreed that online crime poses a significant threat to society. The results of this study demonstrated that experts' views significantly differed from those of local non-expert police officers' views. This difference suggests that police officers' skills related to cybercrime investigations impact their views and their willingness to conduct cyber investigations.

Nouh, Nurse, Webb, and Goldsmith (2019) conducted ten semi-structured interviews with experts from the government and private sector to examine the challenges law enforcement faces. Problems related to Action Fraud's procedures pertaining to data collection and recording the cases reported to them appeared to exacerbate reporting of problems of cybercrime. Lack of coordination between departments emerged to be another challenge faced by law enforcement bodies. Budged cuts related to Information Technologies (IT) infrastructure acknowledged as another significant challenge.

2.1. Data Collection

It is generally agreed that the networked global nature of the Internet poses significant challenges to policing cybercrime due to inherent technological complexities (Holt et al., 2019; Lee et al., 2019). Nevertheless, there is a dearth of empirical research examining policing problems of economic cybercrime through the lenses of police officers in the literature.

2. METHODOLOGY

In order to address this knowledge gap in the literature, ten semi-structured interviews were conducted with police officers working in cybercrime departments in the UK and three semi-structured interviews were done with experts working on IT departments of the local governments. The research was conducted according to the Declaration of Helsinki (World Medical Association, 2001). Interviewees were provided participant information sheets explaining interview and transcription processes prior to interviews. Participants were also asked to sign consent forms before the interviews. Interviews were conducted face-to-face at police departments. Interviews were recorded and transcribed verbatim by authors after the interviews.

2.2. Analytic Procedure

A thematic coding approach was employed to address the research question: *"What are the policing problems of cybercrime police units in the UK"*. The aims of this research were two-fold: documenting the problems experienced by police officers working in cybercrime departments and discerning police officers' perceptions related to the role of police in the wider policing assemblage.

Braun and Clarke (2006: 6) define thematic analysis as "a method for identifying, analysing, and reporting patterns (themes) within data." They categorise thematic analysis as inductive and theoretical. The former perspective is a bottom-up approach that aims to identify themes or concepts without relying on the pre-defined set of codes and themes. The latter is a top-down approach which utilises existing codes and themes informed by theory (Hayes, 1997; Maguire and Delahunt, 2017). This research applied an inductive analysis approach since the research questions and aims were explorative in nature. Initially, a single-authored coding process was applied with the help of QSR NVIVO qualitative analysis software. Codes and themes created in the first cycle of coding were revised by other authors to prevent single coder bias.

3. FINDINGS

Analysis of interviews conducted with police officers and cybercrime experts suggests that policing economic cybercrime is a multidimensional complex issue involving both national and international actors together with police forces. Participants' accounts are provided verbatim as evidence to maintain the validity and the reliability of the research.

Interviews with police officers revealed the lack of international cooperation as the key challenge to policing economic cybercrime. Participants acknowledged that non-European countries were reluctant to share information related to online perpetrators.

"The companies sit in Luxemburg, Panama or Gibraltar are reluctant to share information. So, you need to have a global agreement." (Participant 2).

"Sometimes, the suspect is out of the country. It is difficult to catch them and bring to the jurisdiction crime happened." (Participant 4).

This lack of international cooperation appears to be one of the reasons for low prosecution rates.

"Trying to find out who did it is the biggest challenge. Quite often the cybercrime extends to abroad, and obviously, we have problems with co-operating with other countries. Especially African countries are not very keen to work with us." (Participant 7).

"Cross-national nature of cybercrime is another challenge. Even if you find out the criminals, it is impossible to prosecute them due to residing out of the jurisdiction." (Participant 10).

Issues related to conducting digital forensics emerged as another explanation for failing to prosecute online perpetrators. Retrieving a large volume of data to find evidence and failures in protecting evidence appeared to exacerbate digital forensic.

"I think the difficulty is digital forensics. Naturally, we do not have the same sort of capability for digital forensics if we are to compare a theft from a shop or a burglary with a hacking case. The volume of digital evidence is huge. It requires hard work to retrieve the evidence and it also recognising the information, which could be used to support the prosecuting the offender is a very complex and time-consuming area of work." (Participant 8).

"A challenge can be that the people who are victims of cybercrime don't realise and fully understand how they had been a victim, and they got rid of the evidence. They delete it, wipe the computer because of viruses, which is good in relation to prevent further attacks, but that may stop us getting hold of some evidence." (Participant, 4).

"Victim companies are mostly concerned about getting their business back online, so they are not really concerned about preserving the evidence. Collecting evidence becomes problematic." (Participant 6).

Interviewees also reported that most of the cases were not prosecuted due to a large volume of cybercrime cases exceeding the capacity of cybercrime units located in major cities. It is evident the cases that caused significant financial harm received law enforcement attention.

"The level of response depends on the scale of the harm, which can be measured by financial and physical elements. A company having a huge economic loss because of their data being stolen will have a rapid response." (Participant 3).

Underreporting of economic cybercrime incidents appeared to be another key challenge of policing economic cybercrime. Victims' lack of knowledge about online threats appears to decrease reporting of the economic cybercrime cases.

"People's perception of what is cybercrime. People's inability to understand the differences between the crime, the threat the risk. %50 of crime we experience is cyber-enabled or cyber-dependent however, in most cases, people are not aware of it." (Participant 9).

"Sometimes, victims are not aware that they are subject to a ransomware attack, or they are exposed to malicious software. Sometimes small business run by families may not have expertise in IT issues. They have minimal technical experience. Sometimes victims find it difficult to explain what has happened." (Participant 5).

Victims' reluctance to report cases was cited as another possible reason for underreporting.

"In some cases, when the victim receives the refund, they are not willing to follow the case and go to the court, so victims' reluctance." (Participant 8).

"It happened in Northeast where a large public body had a ransomware attack. We know that they have not reported it because of reputational concerns." (Participant 4).

Interviewees were also asked about their perceptions related to the involvement of private companies in policing economic cybercrime cases. Most participants (n=7) considered public-private partnership fruitful to compensate skill gap between police officers and online perpetrators.

"I do understand why there is a need for private investigations because of their skills need private companies." (Participant 10).

"In technical aspects, most of the times, criminals are more equipped than us." (Participant 7).

However, interviewees also expressed their concerns related to the ethical issues and the extent of the privatisation of policing economic cybercrime.

"Private sectors' role should be limited to protecting. Robust security systems and educating individuals. The companies should co-operate with law enforcement

in partnership to be able to supply evidence that would help the successful prosecution of individuals." (Participant 4).

"The police should be operational independent. Therefore, when they investigate the type of evidence they secure, we look at what has motivated the offender, and the damage has been done to the victim, and we keep the balance between both sides. My concern is sometimes if you have a company doing a prosecution, they may sometimes be interested in protecting the rights of the company rather than looking at the human rights element." (Participant 9).

"As a police force, we should be doing the investigations. Private companies are more after their money, their costumers, their shareholders, but we are responsible to the public. Private companies may help digital investigations under our control". (Participant 6).

The United Kingdom's counter-terrorism strategy, CONTEST, known as the Four Ps Model, aimed to provide a strong response to the terrorist threat to the UK (Home Office, 2014, 2018) bears four components: prevent, pursue, protect and prepare. While pursue refers to prosecuting the offenders and disrupting their activities, prevent denotes safeguarding individuals from becoming an offender. Protect aims to shield the public and private sector from perpetrators by reducing vulnerabilities. Lastly, the goal of the prepare concept is to alleviate post-victimization impacts. Levi, Doig, Gundur, Wall, and Williams (2015) applied this model to policing economic cybercrime. Their research suggested that although this model needs revision to be successfully adapted to policing economic cybercrime, it still offers some valuable insight into tackling economic cybercrime. Participants were asked to evaluate the role of police on the broader cybersecurity assemblage in the light of this framework.

Most of the participants (n=8) reported protect as the primary strategy to be implemented. The belief that most of the cybercrime is preventable, protecting individuals' from experiencing harm and the investigation costs were cited as the rationale for viewing this strategy as the most vital one.

"The police should not just look at arresting people. We have responsibilities. We must look into protect and prepare people." (Participant 7).

"80% of cybercrime is preventable. So, the biggest part of our role is to protect." (Participant 2).

4. DISCUSSION

Despite the growing cyber threat and cybersecurity concerns among the public, there is a lack of empirical research on discerning the challenges of policing economic cybercrime. Previous empirical studies mostly dealt with non-expert police officers' perceptions related to policing cybercrime. The results of these studies demonstrated that local police officers lacked the technical skills to respond to cybercrime (Bossler and Holt, 2012; Bond and Tyrrell, 2018; Hadlington et al., 2018). The findings of this study that although police officers felt confident regarding their technical skills to investigate economic cybercrime cases, they still need external expertise due to the pace of developments in information technologies. This result is in line with (Lee et al., 2019) who found that expert police officers who felt confident were more willing to investigate cybercrime cases.

The lack of international cooperation in combatting cybercrime and providing cybersecurity echoed in this study replicating previous studies (Kshetri, 2010b; James and Gladyshev, 2015). This result which confirms the previous studies indicates that governments or international and transnational actors have failed to collaborate to combat cybercrime globally.

Deleting digital evidence emerged to be a reason for low prosecution. Police officers' accounts suggested Internet users' lack of knowledge as a significant reason for this problem. Some participants also acknowledged that Internet users sometimes even were not aware of their victimisation. This highlights the need for more educational programmes to improve awareness related to online threats.

Police officers' account revealed that most of the cybercrime cases happened in big cities could not be prosecuted. Thus, cybercrime units mostly focused on notorious cases that draw public attention or ended up with significant financial harm. Wall (2013b: 39) argues most of the financial loss can be characterised as "de minimis", which means that online perpetrators steal a small amount of money to evade prosecution. This strategy of online perpetrators appears to increase the workload of law enforcement, which in turn leads to escaping from law enforcement attention.

Regarding private companies' involvement to policing cybercrime, police officers were mostly concerned about private firms' attachment to ethical issues such as pursuing public interest and conducting a fair investigation. Participants

were in favour of outsourcing technical expertise when there is a need. Although outsourcing is always an option when there is lack of expertise in a specific area (Barthelemy, 2003), what combatting cybercrime requires is more than outsourcing. The European Unions' new Cybersecurity Act (Regulation 2019/881), which is in force since July 2019, redesigned ENISA to contribute to European cybersecurity and collaborate with stakeholders. To that end, the Advisory Group was established to cooperate with stakeholders. Cybersecurity certification is another novelty of this new act. ENISA will be responsible for preparing of European cybersecurity certification schemes (European Commission, 2019). The introduction of this new act is a clear indication of EU's commitment to sustain public-private partnership in combatting cybercrime.

CONCLUSION

National and international initiatives such as UK Cybercrime Strategy 2016/2021 place emphasis upon reducing disparities among national jurisdictions and creating strong coordination between policing bodies and other private and governmental actors of cybersecurity to alleviate policing problems of cybercrime (Ellis and Mohan, 2019). Despite these efforts, there is lack of empirical studies on this issue. This empirical research examining the challenges of policing economic cybercrime through police officers' lenses contributes to cybercrime/cybersecurity literature by documenting some challenges cybercrime units have experienced.

Police officers who were participated in this research highlighted the significance of the protect strategy of the Four Ps model for policing cybercrime. This emphasis indicates that police need to move beyond its predefined duties, which mainly focus on investigation and prosecution of the incidents. To that end, police forces need to collaborate with third parties more extensively. Hence, public police need to define its role in broader cybersecurity assemblage. New strategies expanding the responsibilities of police forces from the investigation of the cybercrimes to providing coordination and collaboration between cybersecurity actors, preventing cybercrime and protecting netizens should be devised. Although ENISA's new role will contribute to maintaining cybersecurity, the analysis of interviews suggests that the lack of cooperation with countries that are outside the EU jurisdiction posed a significant challenge. Hence, ENISA or another agency should actively seek to collaborate with non-EU countries.

REFERENCES

Akhgar, B., Choras, M., Brewster, B., Bosco, F., Veermeersch, E., Luda, V., Puchalski, D., and Wells, D. (2016) 'Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism', pp. 295-322 in B. Akhgar and B. Brewster (eds) Combatting cybercrime and cyberterrorism: challenges, trends and priorities: Springer.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., and Savage, S. (2013) 'Measuring the Cost of Cybercrime', pp. 265-300 in The economics of information security and privacy: Springer.

Barthelemy, J. (2003) 'The seven deadly sins of outsourcing', Academy of Management Perspectives 17(2): 87-98.

Bayley, D. H., and Shearing, C. D. (1996) 'The future of policing', Law Society Review 30: 585.

BBC (2019) UK cyber-crime victims lose £190,000 a day. Available at: https://www.bbc.co.uk/news/uk-47016671 (Accessed: 14/09/2019.

Blanco Hache, A. C., and Ryder, N. (2011) ''Tis The Season to (be Jolly?) Wise-Up to Online Fraudsters. Criminals on The Web Lurking to Scam Shoppers this Christmas: A Critical Analysis of the United Kingdom's Legislative Provisions and Policies to Tackle Online Fraud', Information & Communications Technology Law 20(1): 35-56.

Boes, S., and Leukfeldt, E. R. (2017) 'Fighting Cybercrime: A Joint Effort' in R. M. Clark and S. Hakim (eds) Cyber-physical security: protecting critical infrastructure at the state and local level: Springer.

Bond, E., and Tyrrell, K. (2018) 'Understanding revenge pornography: A national survey of police officers and staff in England and Wales', Journal of interpersonal violence: 0886260518760011.

Bossler, A. M., and Holt, T. J. (2012) 'Patrol officers' perceived role in responding to cybercrime', Policing: an international journal of police strategies & management 35(1): 165-181.

Braun, V., and Clarke, V. (2006) 'Using thematic analysis in psychology', Qualitative research in psychology 3(2): 77-101.

Brenner, S. W. (2001) 'Is There Such a Thing as' Virtual Crime'?'.

---. (2004) 'Cybercrime Metrics: Old Wine, New Bottles?', VA. JL & TECH. 9: 13.

---. (2007) 'The Council of Europe's Convention on Cybercrime', pp. 207-221 in J. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman and T. Zarsky (eds) Cybercrime: digital cops in a networked environment: NYU Press.

Brenner, S. W. (2010) Cybercrime: Criminal Threats from Cyberspace: USA: Prager.

Button, M. (2019) Private policing: Routledge.

Casey, E. (2011) 'Language of Computer Crime Investigation', pp. 35-48 in E. Casey (ed.), Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. London: Elsevier.

Clough, J. (2014) 'A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation', Monash UL Rev. 40: 698.

Dolliver, D. S., and Poorman, K. (2018) 'Understanding Cybercrime', pp. 139-160 in P. L. Reichel and R. Randa (eds) Transnational Crime and Global Security [2 volumes]: ABC-CLIO.

Ellis, R., and Mohan, V. (2019) Rewired: Cybersecurity Governance: John Wiley & Sons.

European Commission (2007) Towards a General Policy on the Fight Against Cyber Crime Available at: https://eur-lex.europa.eu/LexUriServ/ LexUriServ. do?uri= COM:2007:0267:FIN:EN:PDF.

--- (2019) The EU cybersecurity certification framework. Available at: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (Accessed: 17/08/2019.

Finn, B. M. (2019) 'Recommendations for a hybridized public private law enforcement approach'.

Garland, D. (1996) 'THE LIMITS OF THE SOVEREIGN STATEStrategies of Crime Control in Contemporary Society', The British journal of criminology 36(4): 445-471.

Gercke, M. (2012) Understanding Cybercrimes: Phenomena, Challenges and Legal Response: International Telecommunication Union.

Gordon, S., and Ford, R. (2006) 'On the Definition and Classification of Cybercrime', Journal in Computer Virology 2(1): 13-20.

Grabosky, P., and Smith, R. (2001) 'Telecommunications Fraud in the Digital Age: the Convergence of Technologies', pp. 23-43 in D. Wall (ed.), Crime and the Internet. London: Routledge.

Grabosky, P. N. (2001) 'Virtual criminality: Old wine in new bottles?', Social & Legal Studies 10(2): 243-249.

Graham, L. (2017) Cybercrime costs the global economy $450 billion: CEO. Available at: https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html (Accessed: 06/08/2019 2019).

Hadlington, L., Lumsden, K., Black, A., and Ferra, F. (2018) 'A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime', Policing: A Journal of Policy and Practice.

Hayes, N. (1997) 'Theory-led thematic analysis: Social identification in small companies'.

Holt, T. J., Bossler, A. M., and Fitzgerald, S. (2010) 'Examining state and local law enforcement perceptions of computer crime', *Crime on-line: Correlates, causes, and context*: 221-246.

Holt, T. J., Burruss, G. W., and Bossler, A. M. (2018) 'An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents', *Policing and Society*: 1-16.

Holt, T. J., Lee, J. R., Liggett, R., Holt, K. M., and Bossler, A. (2019) 'Examining perceptions of online harassment among constables in England and Wales', *International Journal of Cybersecurity Intelligence & Cybercrime* 2(1): 24-39.

Home Office (2014) *The Serious and Organised Crime Strategy*, London.

--- (2018) *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, London.

James, J. I., and Gladyshev, P. (2015) A Survey of International Cooperation in Digital Investigations, *International Conference on Digital Forensics and Cyber Crime* (pp. 103-114): Springer.

Joh, E. E. (2019) 'Policing the smart city', *International Journal of Law in Context* 15(2): 177-182.

Koops, B.-J. (2010) 'The internet and its opportunities for cybercrime'.

Kshetri, N. (2010a) 'The Global Cybercrime Industry and Its Structure: Relevant Actors, Motivations, Threats, and Countermeasures', pp. 1-34 in *The Global Cybercrime Industry*: Springer.

---. (2010b) 'Structure of Cybercrime in Developing Economies', pp. 165-188 in *The Global Cybercrime Industry*: Springer.

---. (2013) 'Cybercrime and cyber-security issues associated with China: some economic and institutional considerations', *Electronic Commerce Research* 13(1): 41-69.

Lam, P. T. (2019) 'Public–Private Partnerships for Fire, Police, and Ambulance Services', pp. 153-165 in *Public Private Partnerships*: Springer.

Lee, J. R., Holt, T. J., Burruss, G. W., and Bossler, A. M. (2019) 'Examining English and Welsh Detectives' Views of Online Crime', *International Criminal Justice Review*: 1057567719846224.

Levi, M., Doig, A., Gundur, R., Wall, D., and Williams, M. L. (2015) *The Implications of Economic Cybercrime for Policing*: City of London Corporation. Available at: https://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/Research-2015/Economic-Cybercrime-FullReport.pdf. (Accessed: 11 June 2017).

Maguire, M., and Delahunt, B. (2017) 'Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars', *AISHE-J: The All Ireland Journal of Teaching and Learning in Higher Education* 9(3).

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., and Ignatuschtschenko, E. (2013) 'Comprehensive Study on Cybercrime', *United Nations Office on Drugs and Crime, Tech. Rep*.

Nouh, M., Nurse, J. R., Webb, H., and Goldsmith, M. (2019) 'Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement', *arXiv preprint arXiv:1902.06961*.

Pathak, P. (2016) 'The Review of Terms and Concepts Used to Understand Cybercrime to Safeguard Ourselves from Cybercriminals', *International Journal of Advanced Research in Computer Science* 7(1).

Petee, T. A., Corzine, J., Huff-Corzine, L., Clifford, J., and Weaver, G. (2010) 'Defining" Cyber-crime": Issues in Determining the Nature and Scope of Computer-related Offenses,"', *Futures Working Group* 5: 6-11.

Reinhart, R. J. (2018) *One in Four Americans Have Experienced Cybercrime*. Available at: https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx (Accessed: 08/09/2019.

Ruddell, R., Thomas, M. O., and Patten, R. (2011) 'Examining the roles of the police and private security officers in urban social control', *International Journal of Police Science & Management* 13(1): 54-69.

Sandywell, B. (2013) 'On the Globalisation of Crime: the Internet and New Criminality', pp. 56-84 in *Handbook of internet crime*: Willan.

Summerville, A. (2017) *Protect against the fastest-growing crime: cyber attacks*. Available at: https://www.cnbc.com/2017/07/25/stay-protected-from-the-uss-fastest-growing-crime-cyber-attacks.html (Accessed: 06/08/2019 2019).

Taylor, G. (2002) 'The Council of Europe Cybercrime Convention a Civil Liberties Perspective', *Retrieved June* 13: 2006.

The Council of Europe Convention on Cybercrime. (2001) Convention on Cybercrime. In T. C. o. Europe (Ed.). Budapest: European Treaty Series - No. 185.

Thomas, D., and Loader, B. (2000) 'Cybercrime: Law Enforcement, Security and Surveillance in the Information Age' in D. Thomas and B. Loader (eds) *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge.

UN Congress. (2000) Crimes Related to Computer Networks, *10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders*. Vienna: United Nations.

UN Manual (1994) *United Nations Manual on the Prevention and Control of Computer-Related Crime*. Available at: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf (Accessed: 21/03/2017).

Wall, D. S. (2005) 'Digital Realism and the Governance of Spam as Cybercrime', *European journal on criminal policy and research* 10(4): 309-335.

---. (2007a) *Cybercrime: The transformation of crime in the information age*: Polity.

---. (2007b) *Cybercrime: The Transformation of Crime in the Information Age*: Cambridge: Polity Press.

---. (2008) 'Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime', *International Review of Law, Computers & Technology* 22(1-2): 45-63.

---. (2010) 'Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace (Revised May 2010)', *Police Practice and Research* 8(2): 183-205.

---. (2013a) 'Criminalising Cyberspace: The Rise of the Internet as a 'Crime Problem'', pp. 106-121 in *Handbook of Internet Crime*: Willan.

---. (2013b) 'Policing Identity Crimes', pp. 29-52 in D. S. Wall and M. L. Williams (eds) *Policing cybercrime: networked and social media technologies and the challenges for policing*: Taylor & Francis.

Wall, D. S., and Williams, M. (2014) *Policing cybercrime: networked and social media technologies and the challenges for policing*: Routledge.

Williams, M., and Levi, M. (2015) 'Perceptions of the ecrime Controllers: Modelling the Influence of Cooperation and Data Source Factors', *Security Journal* 28(3): 252-271.

World Medical Association. (2001) 'World Medical Association Declaration of Helsinki. Ethical principles for medical research involving human subjects', *Bulletin of the World Health Organization* 79(4): 373.

Yar, M. (2005) 'The Novelty of 'Cybercrime' an Assessment in Light of Routine Activity Theory', *European Journal of Criminology* 2(4): 407-427.

---. (2013a) *Cybercrime and Society*: Sage.

---. (2013b) 'The Private Policing of Internet Crime' in Y. Jewkes and M. Yar (eds) *Handbook of Internet crime*: Routledge.