Scientific Research Publishing

Journal of Data Analysis and Information Processing, 2023, 11, 121-143
https://www.scirp.org/journal/jdaip
ISSN Online: 2327-7203
ISSN Print: 2327-7211

Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool

Abdelkhalek Ibrahim Alastal, Ashraf Hassan Shaqfa

Geography and GIS Department, Arts College, Islamic University of Gaza, Gaza, Palestine
Email: Abdelkhalek.alastal@gmail.com, Ashaqfa@iugaza.edu.ps

How to cite this paper: Alastal, A.I. and Shaqfa, A.H. (2023) Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool. *Journal of Data Analysis and Information Processing*, **11**, 121-143.
https://doi.org/10.4236/jdaip.2023.112008

Received: January 12, 2023
Accepted: April 1, 2023
Published: April 4, 2023

Abstract

This paper addressed the current state of police officers' capabilities, skills, and their readiness to deal with the developments of cybercrime. This study discussed definition of cybercrime, cybercrime categories as well as comparison between traditional criminal techniques and cybercrime. As the abilities and skills required for detectives to investigate cybercrime have been discussed. Additionally, literature review and related work, was addressed challenges role of the police in combating cybercrime and facing cybercrime policing. We proposed the main tool in the study which is "Checklist of essential skills for a cybercrime investigator". Thus, to gain the ability to Identify technical and practical requirements in terms of skills, programs, and equipment to achieve effective and professional results in fight cybercrimes.

Keywords

Cybercrimes, Cyber Security, Digital Forensic, Police Officer, Skills, Checklist

1. Introduction

In today's digital era, using the internet for day-to-day transactions has become a daily routine for the majority of people, where the number of internet users has increased dramatically, as has cyber-crime [1].

Overall, there is no denying the fact that these technologies have created a cyberspace in which a criminal can commit his crimes in any part of the world while sitting at home in front of his personal computer screen which is connected to the Internet, and all that is required is some knowledge of computer science and networks.

Based on the preceding, now Cybercrime is a complex and ever changing phenomenon. Under such alarming scenario, cyber criminals are becoming more sophisticated and are targeting consumers as well as public and private organiza-

tions. Thus, cybercrime is a broad term encompassing acts committed or facilitated by the use of computer technology.

In recent decades, the developing of ICT has presented a formidable challenge to law enforcement and other security governance actors. In particular, cybercrime, a term that covers the offenses targeting both computers and/or networks and those assisted by computer technology [2] [3] [4], has become a major social issue over the past couple of decades. With the virtual environment offering myriad opportunities for illegal activities, new offenses such as hacking and malware attacks have emerged [4]. As well, traditional crimes are now committed by taking advantage of cyberspace's unique characteristics [2] [5] [6].

Considering cybercrimes negative impact on different sectors of society and resulting harm to a country's economic and social prosperity, to avoid falling into this scenario, appropriate strategic plans must be developed to face it.

Therefore, in this regard, it is imperative for security agencies to keep up with the threat of cybercrimes and plan ahead of time and effectively to combat them in order to prevent them from occurring, to seize them as soon as they occur, and to bring the criminals to justice. Whereas, this form of crime is characterized by its technical and legislative complexities.

This study contributes to deepening our understanding of the impact of the cybercrimes on different sectors of society, role of security agencies and policing In terms of knowledge and technical skills of police officers.

This study comes as an attempt to find out about this important issue "cybercrime" in its various renewable, evolving and continuous dimensions, and to study its characteristics, patterns and evidence and how to investigate it.

Due to the nature of the subject, we hope that this effort will contribute to shedding light on cybercrime, which differs significantly from traditional crimes, and the way to deal with it, as well as how to cope with it and a new sort of digital forensic evidence.

In this study, we aim to suggest prevention and response measures by examining criminal digital investigation real skills in computer and cybercrime which police officers have.

Research Problem:

In today's competitive world, with the exponential growth of the usage of computer and services of internet. Cybercrimes investigation needs skills of a special nature of the police officers to be capable of dealing with this kind of investigation, this topic leads us to identify the study's problem, which is related to the qualifications, knowledge, and technical skills required for police officers for investigate cybercrime, as well as the degree of availability and the measurability of these skills and qualifications.

Research Importance:

The study contributes to deepening our understanding of the impact of the real skills available that police officers have in the field of computer and internet crime investigation, and motivates employees in cyber security to the impor-

tance of following the new in this type of crime's fields. The outcomes could be a great importance for strategic planners and for the training programs of the cyber security departments and specially for the workers at the digital investigation field.

Research Questions:

It can be recalled here that the main purpose of this research was to study of cybercrime by answer the main question:

What are the qualification and technical skills essential of criminal investigation in cybercrimes must be available in the police officers?

Thus addressing the following items:

- Cybercrime definition, cybercrime categories.
- Comparison between Traditional Criminal Techniques and Cybercrime.
- The abilities and skills required for detectives to investigate cybercrime.
- Literature review and related work.
- Role of the police in combating cybercrime.
- Challenges facing cybercrime policing.
- Present checklist of essential skills for a digital forensics investigator.

Methodology:

Initially, we began by conducting a literature review on cybercrime and cyber security research. Due to the nature of the cyber security and cybercrime subject, we developed a checklist to help police recognize the qualifications and technical skills required for officers to investigate cybercrime. The questions were formulated based on typical needs assessment topics, critical areas from the literature review, for determining gaps between the status quo and the desires of those within a community. A police officer was targeted for the checklist to provide an objective and balanced viewpoint.

2. Cybercrime Definitions

To begin with, we can say that with the significant advances in ICT (Information and Communications Technology) in the twenty-first century, new concepts are being integrated into our life. Cybercrime is one of those notions that did not exist 30 years ago.

Overall, cybercrime is known as any criminal behavior carried out utilizing computers and the internet. In simple term, it can be said that Cybercrime is an illegal acts where the computer either a tool or target or both in this process.

According to the literature review, it can be said, that there is consensus that there is no single clear, exact, and globally acknowledged definition of cybercrime [7] [8]-[13], academics and organizations alike acknowledge this fact [8] [9] [12] [14]. As a result, the validity of working cybercrime definitions is still being disputed in academic literature. **Table 1** summarizes some various definitions of cybercrime presently utilized by key European and worldwide organizations, the table illustrates different utilization of terminology and cybercrime concepts.

Table 1. Cybercrime definitions used by organizations in selected years.

Definition of Cybercrime	Organization	Year
"any unlawful activity committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and providing or distributing information through a computer system or network" [15]	The Tenth United Nations Congress on Crime Prevention and Offender Treatment	2000
"activity directed against the confidentiality, integrity, and availability of computer systems, networks, and computer data, as well as the abuse of such systems, networks, and data by criminalizing such conduct" [16]	The Council of Europe Cybercrime Convention (often referred to as The Budapest Convention)	2001
"criminal acts committed using electronic communications networks and information systems or against such networks and systems" [17]	The Commission of European Communities	2007
"a large range of criminal acts in which computers and information systems are used as a major instrument or as a primary target" [18]	European Union Cyber security Strategy	2013
"a criminal act of which the target is computer information" [19]	Commonwealth of Independent States Agreement	2016

3. Cybercrime Categories [1]

In light the nature topic of cybercrime, on the basis of their goal and impact, the major categories of cybercrime may be generally divided into four groups as the following:

A) Individuals Crimes:

These types of offenses are committed in order to cause harm to specific people. These include hacking, forgery, cracking, harassment via emails, cyber-stalking, cyber bullying, defamation, dissemination of obscene material, email spoofing, SMS spoofing, carding, cheating and fraud, child pornography, assault by threat, and denial of service attack.

B) Property crimes:

There are cybercrimes committed to put a person's property at risk. They are categorized as intellectual property offenses, computer forgery, cyber-squatting, cyber vandalism, hacking computer system, transmitting viruses and malicious software to damage information, Trojan horses, cyber trespass, Internet time thefts, stealing money while money transfers, et cetera.

C) Crimes against organizations

By default, on one hand, we can observe that these kind of crimes are carried out against the government, organizations, company, and Group of individuals.

On other hand, these kind of offenses included the cyber terrorism, possession of unauthorized information, distribution of pirated software, salami attacks, web jacking, logic bombs, etc.

D) Crimes against society

All of the crimes stated above have an impact on society, either directly or indirectly. As a result, this includes all types of crimes such as pornography, online gambling, forgery, the selling of illegal goods, phishing, cyber terrorism, and so on.

Under such difficult and risky conditions for dealing with cybercrime development, ICT has evolved, become more advanced, accessible, and affordable than ever before. As a result, hacking technology is becoming more accessible to a wider range of people. For all of these reasons, police officers were under intense pressure to confront the issues of cybercrime. Where they must develop skills, knowledge, and talents in order to safeguard society from cybercrime, this is what will be addressed in this study.

4. Cybercrime Costs

In such a risky environment for the growth and expansion of cybercrime and with daily reports of cyber-attacks, cybercrime is posing increasingly serious threats to organizations and individuals around the world. It is obvious that cybercriminals do not differentiate between their victims; they just take advantage of every opportunity in order to steal money, information, or cause disruption.

Overall, studies after studies have shown that costs of cybercrime include data loss and destruction, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

The data below provide an indication of the costs of recent cybercrime inside the cybercrime ecosystem. In this regard, the numbers below come from a survey of enterprise organizations conducted by the Ponemon Institute (working in conjunction with Accenture). 48 The figures present descriptive data of "actual costs incurred either directly or indirectly as a result of cyber-attacks actually detected". 49 FY 2017 data was collected from respondents from 254 enterprise organizations in 15 sectors from seven countries—the United States, Germany, Japan, Australia, Italy, France and the United Kingdom. **Figure 1** presents the total average annualized costs of cybercrime (FY 2016 and FY 2017) in US dollars from enterprise organizations in seven countries.

Organizations from France and Italy did not participate in the Ponemon survey in FY 2016; hence, there is no data for them for FY 2016 (per the report, FY 2016 is presented as the FY 2017 total). As indicated in the figure, enterprise organizations in Australia report the lowest total average costs for FY 2017 at $5.41 million; they also reported the lowest in FY 2016 at $4.30 million. Conversely, organizations in the United States reported the total average annual costs of cybercrime for FY 2017 as $21.22 million and $17.36 million for FY 2016 [12].

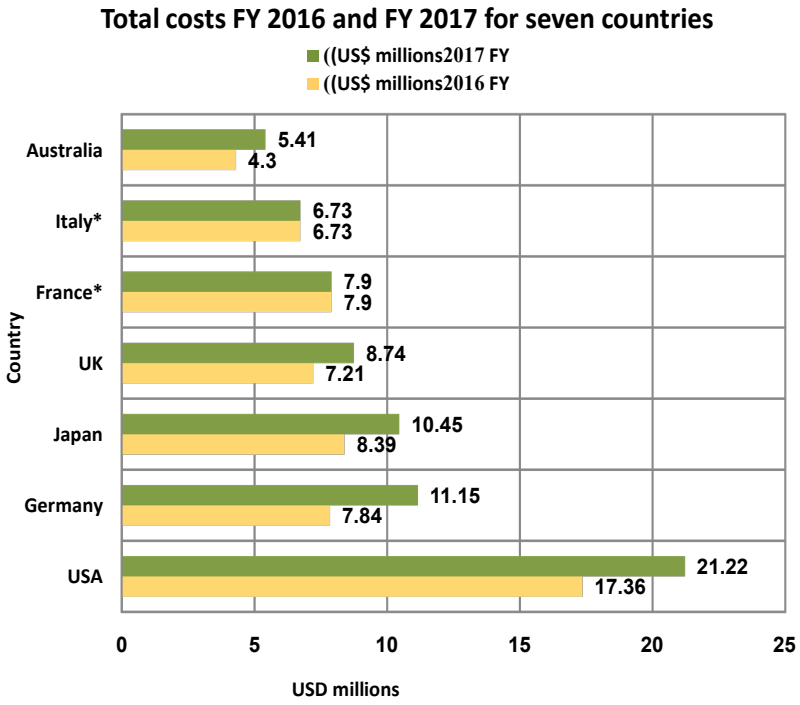

Figure 1. Cost of cybercrime for businesses—total costs FY 2016 and FY 2017 for seven countries. *Historical data does not exist for newly added country samples. Source: [12].

Cybercrime Characteristics

1) No temporal or geographic constraints: Synchronous and asynchronous exchanges that are not geographically limited.

2) No traceability: unless particular precautions to protect such data are adopted. Furthermore, even if the data is captured, it is simple to change, delete, encrypt, and obfuscate.

3) Damage in huge numbers: it is simple to affect a large number of individuals in a short amount of time.

4) Anonymity: the Internet may be used to conceal a person's actual identity in a variety of ways.

By discussing cybercrime costs and it's characteristics, it becomes clear the importance of confronting cybercrime through specific measures. The most significant of these measures is police officer training, as well as the availability of financial and technological resources as well as the required equipment to combat cybercrime.

5. Comparison between Traditional Criminal Techniques and Cybercrime

Recently, with the incredible growth and widespread usage of the Internet services, as well as the transfer of economic, social, political, and other activities to the cyberspace. Consequently, crime has relocated as a companion activity to these human activities, and cybercrime has emerged in the cyberspace. Cyber-

crimes, which differ significantly from conventional crimes in many dimensions, are frequently difficult to identify and prosecute. Technology is changing the environment every day, it affects the civilian and military infrastructure in all sectors. We can notes the effects of that through the cyber-attacks that the United States of America, Ukraine and other countries were exposed to, which were announced in various media.

However, because the existing systems for measuring crime were created decades ago and have not kept pace with new innovations, they only scratch the surface in measuring new crimes.

Thus, crime has been changing, and police agencies need to catch up. Where the world is experiencing a transformation in how criminals are using technology to invent new types of crime, and are developing new ways for carry out traditional crimes. Overall, to respond to these developments, police departments will need to make considerable modifications. First and foremost, police departments will need to employ individuals with new skills, provide new training to their officers and detectives, and in some cases restructure how they are organized.

In this context, many researchers have argued about the importance of the general duties officers responding to cybercrime in the same way they would to a traditional criminal activity. Likewise, an expanding collection of research examined police assessments about their preparedness to investigate reports of cybercrime. Figure 2 compares between electronic and traditional crime.

In plain terms, cybercrime is easier to access and execute than traditional crimes, and it is also easier to achieve powerful outcomes and avoid prosecution.

As previously stated, it is necessary to emphasize the importance of developing the police system and understanding how to deal with cybercrime. In order to protect the infrastructure of society.

6. The Abilities and Skills Required for Detectives to Investigate Cybercrime

Day after day, with the development, complexity and expansion of cybercrime, as well as the expansion of the scene in cyberspace.

As a result of the threat that cybercrime poses to various sectors of society, the need for trained investigators and prosecutors who are conversant with sources of electronic evidence is becoming increasingly critical, as criminal acts move from physical to digital domains. To efficiently handle the demands of a cybercrime investigation, investigators require a range of 'soft' and 'hard' skills, coupled with the experience to apply those skills in real and virtual environments (see Table 2).

7. Literature Review and Related Work

In order to better understand the impact of technology on policing, the HMIC (Her Majesty's Inspectorate of Constabulary) [22] published a report to study the current readiness of police services to effectively deal with cybercrimes and

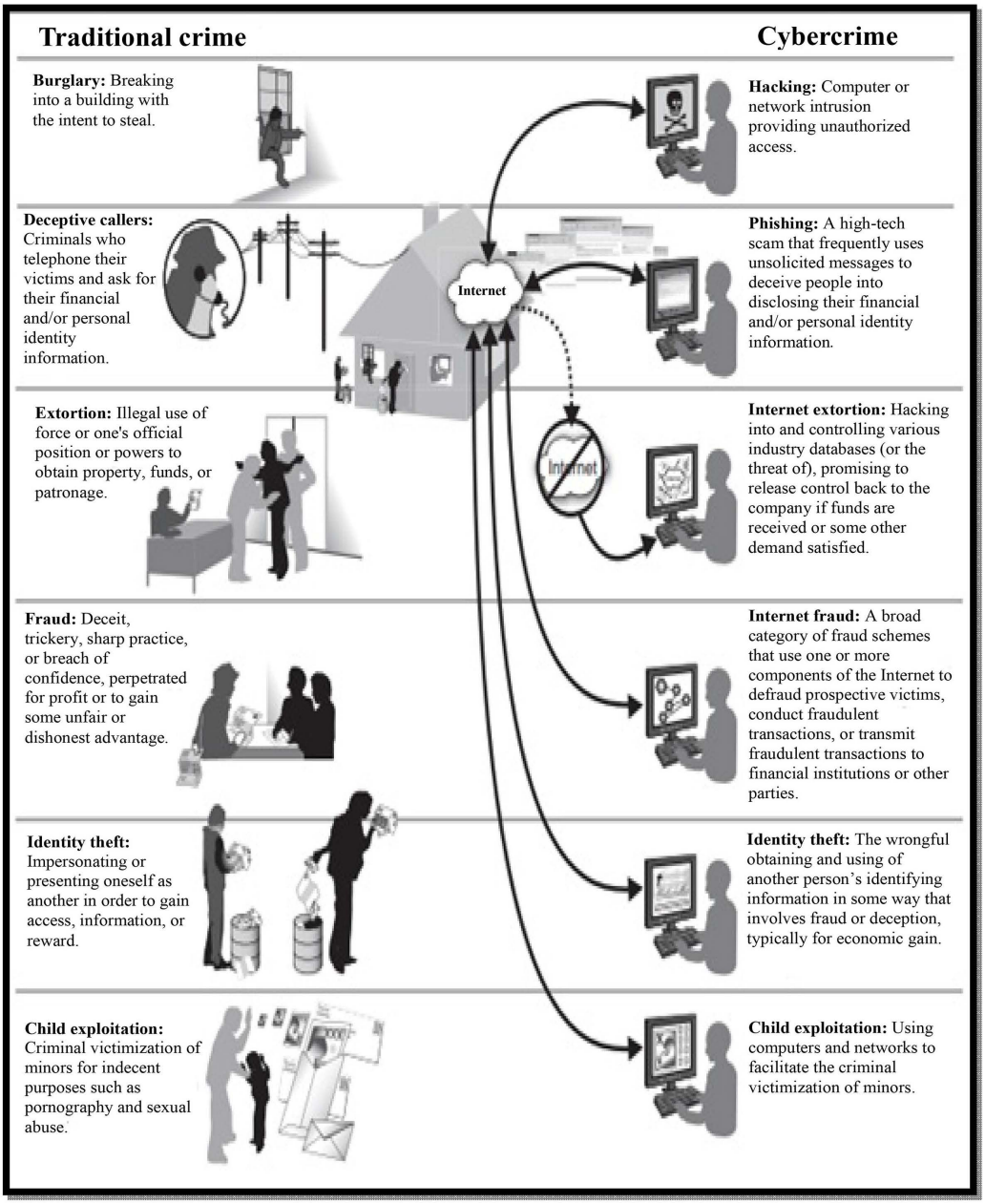

Figure 2. Comparison between traditional criminal techniques and cybercrime. Source: [20].

their victims. The study's key findings focused on giving training, knowledge, and direction to everyone engaged in policing cybercrime. Furthermore, they recommended for increased skills in digital forensics and digital device examination inside law enforcement.

Hunton *et al.* [23] conducted another study that focused on identifying distinct technical investigation responsibilities required for policing cybercrime. These positions include technical enquirer, network investigator, forensic technician, digital forensic examiner, and technical domain expert. They emphasize that as the complexity and risk of cybercrime rise, so should the degree of specialized technological skills and expertise.

Table 2. The set of digital forensic investigation skills required to investigate in cyber-crimes.

Skill	Details
Research	Expeditious retrieval of information in the public domain and reference material stored across the corporate network. Capacity to gain insights by triangulating information from disparate sources that are inaccessible via public search engines.
Awareness	Vigilance in maintaining awareness of developments in the field of information security. Applied knowledge of industry best practices for conducting digital forensics investigations.
Evidence Continuity	Strict compliance with established processes for demonstrating chain-of-custody when handling electronically stored information.
Forensic Imaging	Applied knowledge of data preservation techniques, which use both physical and logical methods to forensically acquire data and verify sources of information.
Networking Architecture	Practical understanding of the Open System Interconnection (OSI) model and the function of communication technologies in the storage and transmission of data, such as network protocols, media access control (MAC) addresses, firewalls, routers, proxy servers, data centers, online applications, cloud services, host-based applications, redundant array of independent disks (RAID), clusters, virtual servers, and modes of multifactor authentication.
Hardware	Applied knowledge of components and peripherals connected to information systems, including hard disk drives, random access memory (RAM), the basic input output system (BIOS), network interface cards (NICs), chipsets, and flash storage.
File Systems	Applied knowledge of diverse file system attributes such as FAT, FAT32, exFAT, NTFS, HFS+, XFS, Ext2, Ext3, Ext4, and UFS.
Structured Data Analysis	Retrieval and interpretation of universally formatted information, such as fixed field entries inside records, as well as embedded information associated with operating systems, relational databases, spreadsheets, registries, Internet history, security and system logs, and encrypted file systems.
Unstructured Data Analysis	Interpretation of values associated with detached files stored across various file systems such as digital photos, graphic images, videos, streaming data, web pages, PDF files, PowerPoint presentations, email data, blog entries, wikis, and word processing documents.

Continued

Semi-structured Data Analysis	Extraction of tags, metadata, or other types of identity markers subsisting within detached files, including information indicative of authorship, revision number, creator, sender, recipient, time and date particulars, GPS coordinates, keywords, and firmware version. This activity also extends to analysis of relational data within files that are associated with detached files, such as XML and other markup languages.
Reverse Engineering	Functional understanding of the mechanics of software development, remote administration, and malware proliferation.
Programming and Scripting	Knowledge of coding using languages such as C, C++, C#, Perl, Delphi, Html, .NET, ASP, Python, Java, JavaScript, Ruby, Bash Scripting, VBScript, PowerShell, Unix/Linux, EnScript.
Virtualization	Applied knowledge of building, configuring, and deploying virtual machines.
Technical Reporting	Experience in producing highly granular reports detailing the inner workings of information communication technologies, file integrity, authenticity of information, and movement of data.

Source: [21].

Moreover, another research by Harichandran *et al.* [24] focused on determining the demands of cyber forensic investigators. They performed a survey of participants from various vocations including cyber forensic students, professors, law enforcement, and practitioners. According to the poll results, participants said that the most pressing requirements are more financing, upgraded tools, improved communication, and amended legislation.

In the same context, several prior research [25] [26] [27] examined police officers' opinions of cybercrime. Whereas, Bossler *et al.* [25] studied how patrol officers evaluated their role in reacting to cybercrime and their existing abilities to respond to these offenses. According to the study, surveyed patrol officers in the United States believe that local law enforcement should not be primarily responsible for handling cybercrime cases.

While, Holt *et al.* [26] investigated determinants of patrol officer interest in cybercrime training and investigation in selected United States police agencies. They cite the officers' computer abilities as one element impacting their interest in cybercrime training and investigations.

Finally, Senjo [27] conducted an exploratory survey to collect police officers' perspectives on cybercrime. The results referenced that the majority of officers recognized cybercrime as a serious problem. However, the most prevalent sort of cybercrime was seen differently than what had been stated in the literature. Senjo indicates that media portrayals and stereotypes impact these perceptions.

Discussion of previous literature

Previous research has substantially contributed to putting light on several is-

sues confronting cybercrime investigators.

For example, source [22] concentrated on providing training, education, and guidance to everyone involved in cybercrime policing. Whereas research [23] focused on defining unique technical investigative duties necessary for policing cybercrime. They underline that as cybercrime complexity and danger increase, so should the level of specialized technology skills and experience. According to a source [24], the most immediate needs are greater funding, enhanced tools, increased communication, and changed laws. Source [25] investigated how patrol officers assessed their role in responding to cybercrime and their current capabilities to respond to these offenses. Source [26] studied the factors that influence patrol officer interest in cybercrime training and investigation in a sample of US police organizations. Source [27] performed an exploratory poll to gather police officers' thoughts on cybercrime.

Our study varies from past studies in that it focuses on developing a checklist for future usage in order to test and define the skills and abilities required for police officers to investigate cybercrime.

8. Role of the Police in Combating Cybercrime

Studies after studies have shown that law enforcement can play a central role in combatting cybercrimes as the main social control agent. In order the police to perform their duties effectively, understanding the nature and status of cybercrime is important, but estimating victimization is often difficult due to a lack of reporting by victims [28]. Moreover, current tools for detecting and investigating incidents, especially cybercrime, are inadequate and have not been tailored to technological evolution [29].

Significantly, it can be said that law enforcement responses to and perceptions of cybercrime are important research areas that can inform the control the spread of cybercrime in an era in which cyberspace is a medium for most business and personal activities.

Considering that the cybercrime used techniques such as hacking and malware attacks, understanding police officers' attitudes toward these offenses can lay a foundation for effective policing opposite cybercrime occurring in the virtual environment. Therefore, this study examines the factors related to the importance that police officers attribute to cybercrime control, As well, the knowledge and technical skills they have .

According to the Federal Bureau of Investigation (FBI), a total of 467,361 complaints with an estimated $3.5 billion losses were filed to the Internet Crime Complaint Center (IC3) in 2019 [30]. Considering the volume of unreported cybercrimes [31], the actual number of offenses committed in cyberspace is expected to be much higher. Based on the trend over the last five years, the number of crimes committed in cyberspace and the resulting financial losses will continue to rise.

Due to the nature of the cybercrimes and role of police officers, as the primary responders to crimes, law enforcement is expected to control illicit activities in

cyberspace. Because security governance in the virtual environment requires specialized knowledge and investigative skills [32], issues that make policing cybercrime challenging have been noted in the policing and cybercrime literature, including officers' lack of awareness and interest [25] [33]. Building on the existing evidence, we explore the factors that predict the importance that police officers attribute to cybercrime control. Since officers who acknowledge the problem's magnitude are more likely to be interested in resolving it [34], the results of this research can inform the practice of preventing and responding to cybercrimes.

9. Challenges Facing Cybercrime Policing

These days, we can observe that the number of Internet users continues to rise worldwide, with an estimated digital population of 4.6 billion in 2020 [35], constituting nearly 60% of the global population. Cybercrime investigators face numerous challenges when policing online crimes. In order to provide adequate support for cybercrime investigators, there needs to be a better understanding of the challenges they face at both technical and sociotechnical levels. Below we will discuss the most important of these challenges:

- The level of IT infrastructure available to police agencies and the cyber skills of investigators are major challenges in investigating cybercrime.
- The disparity between the rate at which cybercrime evolves and the speed of investigation in this type of crime.
- According to the Routine Activities Theory [36], Motivated criminals will find tempting chances in cyberspace because it allows them to conduct crimes without the necessity for spatiotemporal convergence with possible victims [37] [38]. This makes it more difficult for law enforcement to track down culprits, especially when they can remain anonymous [39].
- Furthermore, emerging offenses aimed against IoT devices that utilize advanced technology, such as driverless cars [40], have made identifying cybercrime more difficult.
- Another significant hindrance to successful cybercrime fighting is lack of available resources [41]. This is due to a lack of training and awareness about these growing crimes, as well as an inability to keep up with technology changes and criminals who have adapted to them [42] [43].
- Inadequate resources and competence have a negative impact on officers' willingness to participate in cybercrime control. Evidence reveals that cops are not skilled or experienced enough to conduct cybercrime investigations [44], and they are hesitant to participate in them [25].
- To tackle cybercrime, multi-agency cooperation comprising business and public sector entities are required [45]. To ensure the success of such programs, each element must provide a unique contribution [46].
- Businesses are unwilling to report incidences of victimization in order to safeguard brand values and shareholder assets [47]. The police cannot play a central role in combating cybercrime without active participation from the

private sector and businesses involved.

- According to many studies, police officers do not believe they should be the primary contact authority for cybercrime [25] [48]. This might be attributed to a lack of attention on cybercrime at the organizational level, or to a reduction of self-confidence and preparation to respond to cybercrime incidents [49] [50].
- It goes without saying that investigating "invisible" cybercrime is more difficult than traditional crime.

The challenges of cybercrime policing provide a collection of elements that contribute to the capacity to construct a checklist. For example, police officers' knowledge level with the tools and tactics used to perpetrate cybercrime, degree of awareness of various facets of cybercrime, understanding of cybercrime and the characteristics that distinguish each. Additionally, level of familiarity with some programs and tools used in the investigation of cybercrimes.

In this article, we propose a checklist for evaluating police officers' skill, knowledge and response to cybercrime, and experience related to how law enforcement officers perceive the importance of cybercrime control. Understanding officers' attitudes is an essential step for planning, establishing, and implementing programs to combat cybercrime.

10. Checklist to Identify the Technical Knowledge and Skills That Police Officers Must Have to Investigate Cybercrimes

Overall, it should be noted that the primary goal of this checklist (see **Table 3**) is to identify and assess the knowledge and technical skills that police officers must possess in order to investigate cybercrime. As a result, in simple terms, we can use the suggested "checklist" tool to determine the availability of technical criminal investigation skills in cybercrime among police officers and security agencies.

Furthermore, this checklist is intended to assist the security organization in determining whether the technical security team possesses the necessary skills to protect the organization from cyber-attacks, by measuring the main study variables represented in the study axes, and to identify the differences in the responses of the study community members according to personal variables.

Five-point Likert Scale was used for the of the responses of the study members to the statements of the basic study variables "axes", and its corresponding in the current study (excellent, very good, poor, very poor) respectively, and the values were given to them respectively (5, 4, 3, 2, 1).

11. Recommendations

In simple words, we can say that the proposed procedures will eventually assist the police in participate in cyberspace security governance and cybercrime control, even so, a more pressing issue that must be addressed is how officers view cybercrime. We can note that, considering the nature of the virtual environment

Table 3. Checklist for this study.

***Personal data**

Please read each of the paragraphs carefully and select only one of the available options, by check one box.

Age:
☐ under 30 years old ☐ 30 - less than 40 ☐ 40 - less than 50 ☐ 50 years and over

Gender:
☐ Male ☐ Female

Marital status:
☐ Married ☐ Unmarried ☐ Absolute ☐ Widower

Educational level:
☐ High School ☐ Bachelor ☐ Master ☐ PhD

City: ----------

Police Rank:
☐ Lieutenant ☐ First Lieutenant ☐ Captain ☐ Major ☐ Lieutenant-Colonel
☐ Colonel ☐ Brigadier General ☐ Other .....

Service length in years:
☐ Less than five years ☐ 5 - less than 10 ☐ 10 - less than 15
☐ 15 - less than 20 ☐ 20 years and over

Nature of the current job:
☐ Administrative ☐ Field ☐ Investigation ☐ Other .....

Investigate cyberspace issues:
☐ Did not investigate ☐ A case - less than five cases ☐ Five or more cases

The period of the training course on cybercrime per week:
☐ None ☐ Less than 5 weeks ☐ 5 - Less than 10 ☐ 10 or more weeks

Do you read print and electronic publications (cybercrime):
☐ Yes ☐ No

English reading proficiency:
☐ Yes ☐ No

Years computer use:
☐ None ☐ Less than 3 ☐ 3 - Less than 6
☐ 6 - less than 10 ☐ 10 or more

Computer hours using per week:
☐ None ☐ Less than 5 ☐ 5 - Less than 10
☐ 10 - less than 15 ☐ 15 - less than 20 ☐ 20 or more hours

Years of internet use:
☐ None ☐ Less than one year ☐ One year - less than three years
☐ Three years - less than four years ☐ years or more

Average weekly internet usage hours:
☐ None ☐ Less than 5 ☐ 5 - Less than 10
☐ 10 - less than 15 ☐ 15 - less than 20 ☐ 20 or more hours

Continued

*Checklist axes						
s.	Cyber crime	Responses (knowledge score)				
		Excellent (5)	Very Good (4)	Good (3)	Poor (2)	Very Poor (1)
First axis: the level of familiarity with the tools and methods used in committing cybercrime						
1	Computer virus					
2	Trajan Hoarse					
3	Password Crackers					
4	Network Scanners					
5	Email Flooders					
6	Key Loggers					
7	Packet Sniffers					
8	IP Spoofing					
9	War dialers					
10	Credit Card Numbers Generators					
11	Anonymity					
12	Social Engineering					
Second axis: level of awareness of some aspects related to cybercrime.						
1	Some of the famous cases of these crimes.					
2	Current reality of these crimes.					
3	Categories of perpetrators of these crimes and the distinguishing characteristics of each category.					
4	Future trends of these crimes.					
5	On-line sources of information on these crimes.					
6	Dimensions of international prosecution and joint cooperation to combat these crimes.					
7	Legislation and laws relating to these crimes					
Third axis: level of knowledge of cybercrime and the characteristics that distinguish each crime.						
s.	Cyber crime	Responses (knowledge score)				
		Excellent (5)	Very Good (4)	Good (3)	Poor (2)	Very Poor (1)
1	Spreading Computer Viruses and Trojans					
2	Denial of Service					
3	Distributed Denial of Service					
4	E-mail Hacking					

Continued

5	E-mail Flooding
6	E-mail Forgery
7	Unauthorized use of devices and networks
8	Hacking devices, networks and websites
9	Computer data sabotage
10	Publishing information that violates laws and regulations
11	Data Theft
12	Software Piracy
13	Intercepting and eavesdrop on computer communications
14	Fraud and Embezzlement
15	Manipulation of telecommunications network systems
16	Online Gambling
17	Cyber-Laundering
18	Identity Theft
19	Cyber Espionage
20	Cyber Terrorism
Fourth axis: level of familiarity with some programs and tools used in the investigation of cybercrimes.	
1	File compression/decoding applications include: (WinZip, WinRAR).
2	Video and image processing and analysis software
3	Digital forensic software such as: ProDiscover and CAINE (Computer Aided INvestigative Environment)
4	Command line forensic tools
5	Digital forensic hardware tools
6	Tasks performed by Digital forensic tools such as: - Acquisition - Validation and verification - Extraction - Reconstruction - Reporting
7	Evaluating digital forensic tool needs

Continued

s.	Cyber crime	Responses (knowledge score)				
		Excellent (5)	Very Good (4)	Good (3)	Poor (2)	Very Poor (1)
8	Digital forensic software tools					
9	Mobile device forensics					
10	Desktop forensics					
11	Email forensics					
12	Smartphone analysis					
13	Cloud analysis					
14	IoT forensics					
15	Triage and visualization					
16	File analysis tools					
17	Registry analysis tools					
18	Internet analysis tools					
19	Email analysis tools					
20	Mobile devices analysis tools					
21	Network forensics tools					
22	Database forensics tools					
23	Computer Forensics Methodology					
24	Applications of Computer Forensics					

that defies spatiotemporal limitations, solving cybercrime cases often necessitates interagency cooperation and involves officers performing varying duties at different levels.

As a result, all officers must be informed about the importance of controlling cybercrime in all sectors of society. This means that organizations must work to raise officers' awareness of cybercrime and prepare them to deal with it effectively by developing clear guidelines and providing adequate training [49] [50]. To suggest remedial measures to ensure effective prevention and control of the cybercrimes based on the study following suggestions are recommended:

1) Distributing of the checklist proposed in this study to police stations in order to check the current state of police officers' qualifications, skills, and experience in investigating cybercrime.

2) Front-line police officers as well as combating cybercrime specialists are carefully chosen, based on technical and scientific criteria, as well as the skills and expertise necessary to complete the required tasks professionally and effectively.

3) To combat cybercrime, local education authorities must have the resources to work with international partners.

4) The knowledge and technical skills' capabilities of cybercrime-fighting teams should be developed, as should effective and ongoing training.

5) The importance of training officials who investigate cybercrime on the most recent techniques for combating cybercrime.

6) Public education on cybercrime cases.

7) Raising cybercrime awareness and incorporating cyber law into high school curricula.

8) Every governorate should have a cybercrime research and development center.

9) Making it easier for victims of cybercrime to file complaints.

10) Legislative responses to cybercrime combat police are being reviewed and developed, which lack adequate tools to identify offenders or deploy technical capability to remove malicious software.

11) Support research beneficial to the fight against cybercrime.

12. Conclusions

This study contributes to a better understanding of police preparedness to investigate cybercrime. In the current scenario, with the exponential growth and spread of the usage of internet services, use of the cyberspace plays a very important role in the economic, social, political and various sectors of society. As a result of all of these changes, cybercrime has evolved and caused significant damage to all sectors of society.

On one hand, this study discussed definition of cybercrime, cybercrime categories as well as comparison between traditional criminal techniques and cybercrime. The study also focused on the abilities and skills required for detectives to investigate cybercrime. Additionally, literature review and related work, was addressed challenges role of the police in combating cybercrime and facing cybercrime policing.

On the other hand, it was proposed the main tool in the study which is "Checklist of essential skills for a digital forensics investigator", which includes two parts, first part cover personal data, second part addressed four axes: where first axis handle the level of familiarity with the tools and methods used in committing cybercrime. While second axis addressed level of awareness of some aspects related to cybercrime, whereas third axis processed level of knowledge of cybercrime and the characteristics that distinguish each crime. Finally, fourth axis treated level of familiarity with some programs and tools used in the investigation of cybercrimes.

Thus, the ability to identify technical and practical requirements in terms of skills, programs, and equipment to achieve effective and professional results in fight cybercrimes.

Suggested future studies

We propose the following topics for future research on cybercrime:

- Do the police officers recognize the impact of cybercrime on different society sectors?

- How the police should effectively respond to the needs of cybercrime victims?
- Do the police provide adequate support and advice to victims cybercrime?
- Are public aware of the threat of cybercrime?
- The level of knowledge and technical skills possessed by senior officers, as well as their impact on combating cybercrime.
- Frontline officers' level of knowledge and technical skills, as well as their impact on combating cybercrime.
- Investigating the university student community's awareness of cybercrime's dangers and students' role in combating it.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Kaur, A.M. (2017) A Study on Awareness of Cyber Crime and Security. *Research Journal of Humanities and Social Sciences*, **8**, 459-464. https://doi.org/10.5958/2321-5828.2017.00067.5

[2] Bossler, A.M. and Berenblum, T. (2019) Introduction: New Directions in Cybercrime Research. *Journal of Crime and Justice*, **42**, 495-499. https://doi.org/10.1080/0735648X.2019.1692426 https://www.tandfonline.com/doi/pdf/10.1080/0735648X.2019.1692426?needAccess=true

[3] Furnell, S. (2003) Cybercrime: Vandalizing the Information Society. *Proceedings of the International Conference on Web Engineering*, *ICWE* 2003, Oviedo, 14-18 July 2003, 8-16. https://link.springer.com/content/pdf/10.1007/3-540-45068-8_2.pdf

[4] McGuire, M. and Dowling, S. (2013) Cyber Crime: A Review of the Evidence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

[5] Brenner, S.W. (2001) Is There Such a Thing as 'Virtual Crime'? *California Criminal Law Review*, **4**, Article 1. https://www.researchgate.net/publication/228199325_Is_There_Such_a_Thing_as_%27Virtual_Crime%27

[6] Brenner, S.W. (2004) Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law & Technology*, **9**, 1-52.

[7] Black, A., Lumsden, K. and Hadlington, L. (2019) 'Why Don't You Block Them?' Police Officers' Constructions of the Ideal Victim when Responding to Reports of Interpersonal Cybercrime. http://shura.shu.ac.uk/27803/3/Black-WhyDon%27tYou%28AM%29.pdf

[8] Viano, E.C. (2017) Cybercrime: Definition, Typology, and Criminalization. In: Viano, E.C., Ed., *Cybercrime*, *Organized Crime* and *Societal Responses*, Springer International Publishing, Cham, 3-22. https://www.mdpi.com/2673-6756/2/2/28 https://doi.org/10.1007/978-3-319-44501-4_1

[9] Paoli, L., Visschers, J., Verstraete, C. and Van Hellemont, E. (2018) The Impact of Cybercrime on Belgian Businesses. Intersentia, Cambridge. https://doi.org/10.1017/9781780687742

https://intersentia.com/en/the-impact-of-cybercrime-on-belgian-businesses.html

[10] Sarre, R., Lau, L.Y.C. and Chang, L.Y. (2018) Responding to Cybercrime: Current Trends. *Police Practice and Research*, **19**, 515-518. https://doi.org/10.1080/15614263.2018.1507888

[11] Donalds, C. and Osei-Bryson, K.-M. (2019) Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach. *Computers in Human Behavior*, **92**, 403-418. https://doi.org/10.1016/j.chb.2018.11.039

[12] Broadhead, S. (2018) The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments. *Computer Law & Security Review*, **34**, 1180-1196. https://doi.org/10.1016/j.clsr.2018.08.005

[13] Akdemir, N., Sungur, B. and Başaranel, B.U. (2020) Examining the Challenges of Policing Economic Cybercrime in the UK. *Güvenlik Bilimleri Dergisi*, UGK Özel Sayısı, 113-134. http://fr.jsga.edu.tr/kurumlar/fr.jsga/IcSite/sciencesdesecurite/GuvenlikBilimleriDergisi/Arsiv/2020/Mayis/8makale-_6--_.pdf

[14] Gillespie, A.A. (2015) Cybercrime: Key Issues and Debates. Routledge, New York. https://doi.org/10.4324/9781315884202

[15] UN Congress Crimes Related to Computer Networks (2017) 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders; United Nations: Vienna, Austria, 2000. https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf

[16] Council of Europe (2001) Convention on Cybercrime. European Treaty Series-No. 185, Council of Europe, 1-22. https://rm.coe.int/1680081561

[17] Commission of the European Communities (2007) Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a General Policy on the Fight against Cyber Crime. Commission of the European Communities, Brussels. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

[18] European Commission (2013) Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, Brussels. https://edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en

[19] Akhgar, B., Choraś, M., Brewster, B., Bosco, F., Veermeersch, E., Luda, V., Puchalski, D. and Wells, D. (2016) Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism. In: Akhgar, B. and Brewster, B., Eds., *Combatting Cybercrime and Cyberterrorism*: *Challenges*, *Trends and Priorities*, *Advanced Sciences and Technologies for Security Applications*, Springer, Cham, 295-321. https://nottingham-repository.worktribe.com/output/3774756 https://doi.org/10.1007/978-3-319-38930-1_16

[20] US Government Accountability Office (2007) Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats. US Government Accountability Office, Washington, DC. https://www.gao.gov/new.items/d07705.pdf

[21] Perera, P. and Mahanamahewa, P. (2017) Analysis of Dependencies & Legal Barriers on Digital Forensic Investigations in Sri Lanka. http://ir.kdu.ac.lk/bitstream/handle/345/1733/028.pdf?sequence=1&isAllowed=y

[22] HMIC (2015) Real Lives, Real Crimes: A Study of Digital Crime and Policing. Technical Report, Her Majesty's Inspectorate of Constabulary, London. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

[23] Hunton, P. (2012) Managing the Technical Resource Capability of Cybercrime Investigation: A UK Law Enforcement Perspective. *Public Money & Management*, **32**, 225-232. https://www.tandfonline.com/doi/abs/10.1080/09540962.2012.676281 https://doi.org/10.1080/09540962.2012.676281

[24] Harichandran, V.S., Breitinger, F., Baggili, I. and Marrington, A. (2016) A Cyber Forensics Needs Analysis Survey: Revisiting the Domain's Needs a Decade Later. *Computers & Security*, **57**, 1-13. https://doi.org/10.1016/j.cose.2015.10.007 https://digitalcommons.newhaven.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1036&context=electricalcomputerengineering-facpubs

[25] Bossler, A.M. and Holt, T.J. (2012) Patrol Officers' Perceived Role in Responding to Cybercrime. *Policing*, **35**, 165-181. https://doi.org/10.1108/13639511211215504 https://www.emerald.com/insight/content/doi/10.1108/13639511211215504/full/html

[26] Holt, T.J. and Bossler, A.M. (2012) Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments. *Cyberpsychology, Behavior and Social Networking*, **15**, 464-472. https://pubmed.ncbi.nlm.nih.gov/22817769/ https://doi.org/10.1089/cyber.2011.0625

[27] Senjo, S.R. (2004) An Analysis of Computer-Related Crime: Comparing Police Officer Perceptions with Empirical Data. *Security Journal*, **17**, 55-71. https://doi.org/10.1057/palgrave.sj.8340168 https://www.ojp.gov/ncjrs/virtual-library/abstracts/analysis-computer-related-crime-comparing-police-officer

[28] Button, M. (2020) Editorial: Economic and Industrial Espionage. *Security Journal*, **33**, 1-5. https://link.springer.com/content/pdf/10.1057/s41284-019-00195-5.pdf https://doi.org/10.1057/s41284-019-00195-5

[29] Luciano, L., Baggili, I., Topor, M., Casey, P. and Breitinger, F. (2018) Digital Forensics in the Next Five Years. *Proceedings of the* 13*th International Conference on Availability, Reliability and Security*, Hamburg, 27-30 August 2018, 1-14. https://digitalcommons.newhaven.edu/cgi/viewcontent.cgi?article=1080&context=electricalcomputerengineering-facpubs https://doi.org/10.1145/3230833.3232813

[30] Federal Bureau of Investigation (2019) 2019 Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

[31] Tcherni-Buzzeo, M., Davies, A., Lopes, G. and Lizotte, A. (2016) The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly*, **33**, 890-911. https://doi.org/10.1080/07418825.2014.994658 https://digitalcommons.newhaven.edu/cgi/viewcontent.cgi?article=1045&context=criminaljustice-facpubs

[32] Hinduja, S. (2004) Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams. *Policing*, **27**, 341-357. https://doi.org/10.1108/13639510410553103 https://www.researchgate.net/profile/Sameer-Hinduja/publication/240602047_Percetions_of_local_and_state_law_enforcement_concerning_the_role_of_computer_crime_investigative_teams/links/55dddbcb08ae45e825d39208/Perceptions-of-local-and-state-law-enforcement-concerning-the-role-of-computer-crime-investigative-tea

ms.pdf

[33] Lee, J.R., Holt, T.J., Burruss, G.W. and Bossler, A.M. (2021) Examining English and Welsh Detectives' Views of Online Crime. *International Criminal Justice Review*, **31**, 20-39. https://doi.org/10.1177/1057567719846224 https://journals.sagepub.com/doi/epub/10.1177/1057567719846224

[34] Skogan, W.G. and Hartnett, S.M. (1997) Community Policing, Chicago Style. Oxford University Press, New York. https://www.ojp.gov/ncjrs/virtual-library/abstracts/community-policing-chicago-style.

[35] (2022) Global Digital Population as of October. https://www.statista.com/statistics/617136/digital-populationworldwide/

[36] Cohen, L.E. and Felson, M. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, **44**, 588-608. http://faculty.washington.edu/matsueda/courses/587/readings/Cohen%20and%20Felson%201979%20Routine%20Activities.pdf https://doi.org/10.2307/2094589

[37] Grabosky, P.N. (2001) Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, **10**, 243-249. https://journals.sagepub.com/doi/10.1177/a017405 https://doi.org/10.1177/a017405

[38] Wall, D.S. (1998) Policing and the Regulation of the Internet. In: Walker, C. and Ashworth, A., Eds., *Criminal Law Review*, Sweet & Maxwell, London, 79-91.

[39] Navarro, J.N. and Jasinski, J.L. (2012) Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences. *Sociology Spectrum*, **32**, 81-94. https://stars.library.ucf.edu/facultybib2010/3072/ https://doi.org/10.1080/02732173.2012.628560

[40] Kennedy, J., Holt, T. and Cheng, B. (2019) Automotive Cybersecurity: Assessing a New Platform for Cybercrime and Malicious Hacking. *Journal of Crime and Justice*, **42**, 632-645. https://www.tandfonline.com/doi/full/10.1080/0735648X.2019.1692425 https://doi.org/10.1080/0735648X.2019.1692425

[41] Goodman, M.D. (1997) Why the Police Don't Care About Computer Crime. *Harvard Journal of Law & Technology*, **10**, 465-494. http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech465.pdf

[42] Hadlington, L., Lumsden, K., Black, A. and Ferra, F. (2018) A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime. *Policing*, **15**, 34-43. https://doi.org/10.1093/police/pay090 https://shura.shu.ac.uk/23755/3/Black_qualitative_exploration_police_%28AM%29.pdf

[43] Holt, T.J., Blevins, K.R. and Burkert, N. (2010) Considering the Pedophile Subculture Online. *Sexual Abuse*, **22**, 3-24. https://doi.org/10.1177/1079063209344979 https://journals.sagepub.com/doi/10.1177/1079063209344979

[44] 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*, **36**, 2166-2181. https://doi.org/10.1177/0886260518760011 https://journals.sagepub.com/doi/abs/10.1177/0886260518760011

[45] Hou, T. and Wang, V. (2020) Industrial Espionage—A Systematic Literature Review (SLR). *Computers & Security*, **98**, Article ID: 102019. https://www.sciencedirect.com/science/article/pii/S0167404820302923 https://doi.org/10.1016/j.cose.2020.102019

[46] Dupont, B. (2004) Security in the Age of Networks. *Policing and Society*, **14**, 76-91.

https://www.tandfonline.com/doi/abs/10.1080/1043946042000181575
https://doi.org/10.1080/1043946042000181575

[47] Etzioni, A. (2011) Cybersecurity in the Private Sector. *Issues in Science and Technology*, **28**, 58-62.
https://cspri.seas.gwu.edu/sites/g/files/zaxdzs4106/f/downloads/etzioni_0.pdf

[48] Holt, T.J. and Bossler, A.M. (2012) Police Perceptions of Computer Crimes in Two Southeastern Cities: An Examination from the Viewpoint of Patrol Officers. *American Journal of Criminal Justice*, **37**, 396-412.
https://doi.org/10.1007/s12103-011-9131-5
https://www.academia.edu/23673247/Police_Perceptions_of_Computer_Crimes_in_Two_Southeastern_Cities_An_Examination_from_the_Viewpoint_of_Patrol_Officers

[49] Bossler, A.M., Holt, T.J., Cross, C. and Burruss, G.W. (2020) Policing Fraud in England and Wales: Examining Constables' and Sergeants' Online Fraud Preparedness. *Security Journal*, **33**, 311-328. https://doi.org/10.1057/s41284-019-00187-5
https://link.springer.com/article/10.1057/s41284-019-00187-5

[50] Burruss, G., Howell, C.J., Bossler, A. and Holt, T.J. (2019) Self-Perceptions of English and Welsh Constables and Sergeants Preparedness for Online Crime: A Latent Class Analysis. *Policing*, **43**, 105-119. https://ouci.dntb.gov.ua/works/9Go8QAx9/
https://doi.org/10.1108/PIJPSM-08-2019-0142