Design and Implementation of an Electronic Communication Portal Modules to Mitigate Cybercrimes Through International Cooperation

Shadi Younis and Mahmoud Jazzar

Faculty of Graduate Studies
Palestine Technical University – Kadoorie
Tulkarm, P. O. Box 7, Palestine

Abstract— *Most of the countries enact cybercrime laws and specialized law-enforcement agencies to investigate cybercrimes. Many challenges are facing the law and the law-enforcement agencies due to different reasons classified as legal, technical, and operational challenges. One of the main challenges facing combating cybercrime is international cooperation complexity. Another important challenge facing cybercrime, whether transnational or domestic is the technical and legal capabilities and expertise in investigating cybercrime, as well as people's knowledge of cybercrime and information security. These challenges have been determined and classified in terms of legal, technical, and operational challenges by reviewing and summarizing the local, regional, international laws, and agreements. The technical and research reports of different worldwide agencies and researchers have been used in the evaluation of these challenges. As such, the Palestinian law enforcement agency was interviewed to classifying international cybercrime challenges and solution evaluation as a point of view by legal experts. Afterward, international cooperation challenges have been determined and evaluated. An essential technical frame of requirements to improve international cooperation was prepared in terms of modules as an international cooperation electronic portal. The proposed solution will contribute to the mitigation of international communication complexity, law enforcement agencies staff capacity building, and improve people's knowledge of cybercrime topics and issues by using an electronic cooperation portal. The solution has an additional aim to improve the cooperation between the public and private sectors. At this stage, a demo of law enforcement agencies' communication module was implemented.*

Keywords— Cybercrime, International Cooperation, Domestic Laws, Communication Portal, Cybercrime Portal

1. INTRODUCTION

In recent decades, the development of information and communication technology has become large and fast, which has contributed to making technology in all aspects of social, government, and business life. As a result, communication technology has formed an important infrastructure for digitizing governments, business, and social life [1]. Therefore, governmental and business sectors are moving rapidly towards the full digitization of their services, which has an impact on making the world more vulnerable to cyberattacks. This rapid development and widespread technology and communications provide the cybercriminals new motives and modern trends to commit a cybercrime [2]. These motives and trends present new challenges for law enforcement agencies in investigating and combating cybercrime. Besides, the development and spread of the Internet causes the absence of borders between countries that makes a cybercrime a cross-border crime. Generally, this is great challenge in combating cybercrime especially with the development and spread of encryption and anonymity tools that make cybercriminals commit their crimes safely [3], [4].

Cybercrime is an illegal activity that involves a computer, computer networks, or telecommunication where a computer is a tool, a target, or a place to commit or facilitate crime [5]. Cybercrimes are usually committed for personal fund gain, commercial competition, theft of intellectual property, personal theft, bullying, harassment, money laundering, terrorism, and so on [6]. Cybercriminals can be categorized based on their behavior and objectives that lead to committing cybercrime. The categories include individuals with goals such as exploring new technologies and fund gain. Criminal organizations who are trying to increase their financial gain and profits. Plus, the terrorist organizations or states who aim to destroy information, infrastructure, and cause harm to societies and states [7]. On the other hand, there are laws and law enforcement agencies for combating cybercrime. However, the Internet and modern technology have facilitated the commission of cybercrime enabling remote access to victims. As well as the low cost of committing the crime because of the availability of freeware or low-cost tools and software to commit a cybercrime. Besides, anonymity and encryption tools became easily available and used. Putting all together, many legal, technical, and operational challenges are facing the law enforcement agencies in investigating and gathering evidence to combat cybercrime [8].

Different agencies and organizations in the world produced specialized reports about Internet use and cybercrimes statistics. These reports describe the current and future status in the world. Besides, these reports specify the relationship between the increases of Internet users around the world with the increase of cybercrimes. The International Telecommunication Union (ITU) [9] issued a statistical report in 2019 on measuring digital development facts and figures. The ITU report shows a rapid increase of Internet users around the world. While the Internet users in 2010 were 1.772 billion users, they were 3.924 billion users in 2018. However, the estimated users in 2019 were 4.131 billion as indicated in (ITU Estimate, n.d.) [9]. On the other hand, the Internet Crime Complaint Center (IC3), the department in the Federal Bureau of Investigation (FBI) issued its annual report on Internet Crime [10]. The report shows the growth of cybercrime yearly in the states. As such, in 2015, there were 288,012 complaints with $1.1 billion losses. While there were 467,361 complaints with $3.5 billion losses in 2019.

In parallel to the significant increase in cybercrime, new trends are appearing due to the development of modern communications technologies. As a result, the challenges facing laws and law enforcement agencies are greatly increased [1]. Different reasons are making challenges for the laws and agencies like the nature of cybercrimes as borderless crimes, people's knowledge, law-enforcement staff capabilities, loss of data, and the relationship between the public sector and the private sector (service providers, private investigators) Challenges in the age of cyberspace [11]. Generally, these challenges are classified as legal, technical, and operational challenges.

Mostly, the cross-border cybercrimes threaten countries and cause the greatest harm to the world in terms of large monetary losses, damage to societies. This type of cybercrime targets communications infrastructure in addition to targeting the individuals on a large scale. Therefore, international cooperation is the greatest challenge in combating this type of cybercrime. As a result of the limits of state jurisdiction, the capabilities of law enforcement agencies and their powers to investigate outside borders are limited. A well, a unified and comprehensive international law to combat cybercrime is absent. Besides, there are intricacies of cooperation between countries in the investigation and their impact on the time-sensitivity of the digital evidence. Additionally, the absence of a comprehensive and unified international agency specialized in cybercrimes complicates investigations and prosecutions [12].

Various international and regional efforts are being made to combat cybercrime through the work of international conventions and treaties, Combatting Cybercrime [13]. For example, The Budapest convention of 2001 was developed by the Council of Europe (COE) with participants with other states that are not members of COE [14]. Despite the accession to this convention is not limited to geographical boundaries. However, the accession is conditional upon the agreement of all member states of the agreement. Another convention is the Commonwealth of Independent States (CIS) Agreement of 2001. The participant of all twelve-member states developed the CIS agreement. In addition, accession to this agreement is not limited to geographical boundaries and membership to the CIS. However, it is conditional upon the agreement of all CIS members. Likewise, the country wishing to join the convention must adopt legislation and regulations to implement the convention as well as amend the laws on cybercrime to comply with the convention as stated on Combatting Cybercrime: Tools and Capacity Building for ... (n.d.) [13].

The Shanghai Cooperation Organization (SCO) Agreement of 2009 was developed by the SCO members to enhance their capabilities to meet global challenges and threats in light of the development of information and communication technology and the accompanying developments in cybercrime. Also, the accession to the SCO agreement is not limited to the geographical area or the membership to the SCO, Combatting Cybercrime: Tools and Capacity Building for ... (n.d.) [13]. There are other regional cybercrime agreements. The League of Arab States Convention on Combating Information Technology Offences of 2010 was developed by the League of Arab States members, the accession of this convention is limited to the league of Arab states members only. In this agreement, the parties must adopt and implement procedural policies and legislation related to cybercrime that facilitate the investigation and prosecution of cybercrime.

African Union (AU) Convention on Cyber Security and Personal Data Protection of 2014 is another regional agreement example. This convention was developed by AU member states, only these members have the right to access it. This agreement requires the ratification of fifteen instruments to enter into implementation [13].

The state of Palestine as many other countries issued a cybercrime law by Decree No. 10 [15]. This law defines activities, tools, and terminology related to cybercrime. It has also determined the law enforcement agencies that are responsible for the investigation and prosecution of cybercrime at Palestinian National Authority. While this law is new in Palestine, the Police department in Palestine received complaints before the issuance date of this law. As a result of the increase in cybercrime and complaints submitted to Palestinian police, this law has been issued to regulate the required legislation to combat and prosecute cybercrimes. Through Palestinian police statistics, the number of complaints in the year 2015 was 502 complaints. While, in 2016 it was 1327 complaints, 2025 complaints in 2017, and 2568 complaints in 2018. In the year 2017, A cybercrime unit was established in the Palestinian Public Prosecution Office, this unit includes a team of information technology specialists, who are trained and specialized in the investigation of cybercrime, in addition to allocating specialized prosecutors to prosecute cybercrimes in the Palestinian judiciary public prosecution, Palestine, P. P. (n.d.) [16].

Upon the above basic illustration, cybercrime challenges can be classified into legal, technical, and operational challenges. Table 1 below give an idea about the international challenges associated with combating cybercrimes.

Table 1. List of international cooperation challenges in combating cybercrime

Challenges	**Classification**		
	Legal	**Technical**	**Operational**
Loss of location because of Anonymity.		x	
Loss of Data because of encryption.		x	
Loss of data of private sector (service providers).		x	
Peoples' knowledge.	x		x
Law-enforcement staff capabilities.		x	
Public sector and the private sector cooperation.			x
Limits of state jurisdiction.	x		
The capabilities of law enforcement agencies and their powers to investigate outside borders.	x	x	x
The absence of unified and comprehensive international cybercrime law.	x		
The absence of a comprehensive and unified international agency specialized in cybercrimes complicates the investigations and prosecutions.	x		x
The Complexity of communication between countries in the investigation and their impact on the time-sensitivity of the digital evidence.	x		x

Different websites and online resources about cybercrime are currently used. As such, the United Nations Office on Drugs and Crime (UNODC) website includes a cybercrime module. While the UNODC contains a cybercrime unit to work on technical assistance in capacity building, awareness, international cooperation, and researches in cybercrime, UNODC [17]. However, their online module focuses on capacity building by online training and learning material and cybercrime research. INTERPOL website contains a module of cybercrime, this module contains information about INTERPOL responsibilities on cybercrime, training, and awareness material INTERPOL [18]. Council of Europe Website contains training and learning materials that are about Budapest convention, reports, and studies about cybercrime, Council of Europe [COE] [14]. As such, a unified portal is required to enhance the efficiency and the process of cybercrime combating with consideration of local, bilateral, regional, and international laws and agreements.

The challenges, shown in Table 1, significantly affect the combating of cybercrime. Many challenges are resulting from the current reality of international cooperation such as the capabilities of law-enforcement agencies and their staff. Also, the complexity of cooperation between countries impacts the time-sensitivity of digital evidence. To mitigate these challenges, the design and implementation of Electronic Portal have to be applied to facilitate and speed up the communication between agencies, enhance information sharing, and improve law-enforcement agencies and their staff capabilities by online training and experience exchange. The portal should be internationally administered. The communication between local and international agencies is subjected to regulations and rules depending on the laws and agreements. In this way, the complexity of the diplomatic communication process and the local bureaucracies through different departments and agencies procedures can be avoided.

2. ANALYSIS, DESIGN AND IMPLEMENTATION

Cross-border cybercrimes are serious and complicated challenge faced by domestic law enforcement agencies around the world. The study originated from the significant need to mitigate the international cooperation challenges that face cybercrime laws and law enforcement agencies around the world. This study used a qualitative method to explore and classify cybercrime challenges based on previous studies, research, current regional and international conventions, and agreements. As such, the Palestine law enforcement agency was used as example for determining challenges and solution evaluation.

There is a strong increase in cross border cybercrime due to the international communication infrastructure Challenges in the age of cyberspace [19]. In addition, the use of anonymity tools provide cybercriminal the ability to commit cybercrime against victims in different locations and countries and enables the cybercriminal to appear in a third geographical location. Law enforcement agencies investigators face the inability to investigate across borders due to legislation and laws as well as the limits of jurisdiction [2]. The investigation of these crimes requires international cooperation to investigate and collect digital evidence in more than one country. Besides, seeking technical assistance in the investigation of domestic or cross border new cybercrime types and trends because of weak experience or lack of resources. International communications and diplomatic channels usually take a long time to reach the stage of cooperation in the technical investigation. This negatively affects the collection of digital evidence because of the sensitivity of digital evidence to time. In addition to the ability to alter or delete digital evidence [20]. Moreover, the period for which service providers maintain data that assists investigators in gathering evidence, 2019 Internet Crime Report Released (2020) [21]. In many cases, this leads to the suspension of the investigation and the dropping of the case. An electronic communication module proposed to facilitate and speed up the communication process between law enforcement agencies to the investigation or technical assistance needs.

The spread of different and strong encryption techniques and tools, and using these tools in communications and data transfer result in common challenges in combating cybercrime. In addition, the spread of anonymization tools that help the cybercriminal to keep themselves away from law enforcement Comprehensive Study on Cybercrime, UNODC [17]. Besides, the continuous changing of cybercrime threatens nature and motivations. The law enforcement investigators face the lack of capabilities in their expertise and the investigation tools and resources to investigate these cybercrimes; also, the lack of prosecutors and judge's knowledge about the digital evidence nature and types [22]. Continuous training and learning for law enforcement agencies staff must be maintained. To maintain their technical and legal capabilities in line with the ongoing development of cybercrime [6].

Online learning and training module proposed as a tool to improve law enforcement agencies staff capabilities and to achieve the continuous learning and capacity building. This module includes learning materials in the form of online videos, articles, tutorials, and discussion forums. Besides, a module of law enforcement agencies needs Assessment proposed to evaluate the capacity building needs for these agencies. Also, Information sharing module to help investigators and experts to share experience and information about new cybercrimes and cyberattacks types and trends, investigation, protection, and prevention tools and methods.

Investigating cross-border cybercrime faces obstacles in differing legislations and laws related to some cybercrime from one country to another. For example, some countries classify the publication of pornography as a cybercrime; other countries do not consider it a crime, while some countries consider it a cybercrime within restrictions such as age [23]. To achieve cooperation between one country and another in the investigation of cybercrime, investigators must know and understand the law of the country to cooperate with. In addition to knowledge of the international laws and agreements signed by that country. A module of Laws, Conventions, and agreements proposed to publish domestic and international laws and agreements.

While people spend more and more time using technology, there is a lack of knowledge of how to be secure in cyberspace. Therefore, many people sharing information on cyberspace can be stolen [24]. Many individuals become victims of cybercrime due to a lack of knowledge of technology, or because of personal goals in the use of technology. For example, people over the age of 60s fall victim to Internet fraud, and this fraud is called elder fraud, and other people who fall victim to fraud because of searching for romance on the Internet, so they fall victim to cybercrime of romance fraud, UNODC [17]. Public awareness module proposed to educate the public about cybercrime, types of cyberattacks, and means of protection against cyberattacks.

Cooperation between the public and private sectors leads to improved protection and the prevention or mitigation of cyberattacks. Cybercrime investigators and experts discover or identify weaknesses and vulnerabilities in operating systems, business software, and protection systems after or during the commission of cybercrime. For example, Microsoft president Brad Smith claimed about the U.S national security agency (NSA) knowledge of vulnerabilities in Microsoft operating systems that were exploited by ransomware before informing the company of these vulnerabilities [25]. A private sector alerting Module proposed to improve the cooperation between the public-private sector and to alert the private sector about any discovered vulnerabilities in their software and systems to improve it and to achieve proactive security.

By the Palestinian cybercrime law under Decree No. 10 [15] there is a specialized prosecution called the Cybercrime Prosecution. There are also units and sections to combat cybercrime among the police and the Palestinian security forces. As these units investigate cybercrimes and then refer them to the competent cybercrime prosecution to complete the investigation and prosecution in court. To combat cross-border cybercrime, Palestine signed the Budapest convention of 2001, as well as the League of Arab States Convention on Combating Information Technology Offences of 2010. With the apparent increase in cybercrime in Palestine, especially in the years 2018 and 2019, many challenges arise for law enforcement agencies. The lack of specialized human resources in cybercrime, because of the level of salaries in the government sector compared to the private sector.

Procurement procedures are challenging to provide technical resources and tools for cybercrime and renew their licenses annually. Judges and jurists' understanding of the cybercrimes digital evidence. Individuals have a fear of reporting complaints due to social traditions and reputation. Business and the private sector have fear for their reputation. Other challenges facing combating cross-border cybercrimes such as Anonymity and encryption mechanisms. Sometimes, there is a lack of laws harmonization in some countries and international organizations in the different types of cybercrime. As a result, an extra length of judicial procedures for cross-border crimes is appearing. The international contacts and diplomatic procedures cause additional complexities in the cybercrime investigation process. International Private Sector companies mostly avoid cooperation with national agencies due to some legal and political issues [26].

The Proposed electronic portal as a technical solution to mitigate challenges related to law enforcement agencies capacity building and to facilitate and accelerate international cooperation in investigating cross-border cybercrime. This portal must be managed and supervised by a specialized department under an International Organization like the United Nations. The proposed international cybercrime portal modules can include the following:

- Law enforcement agencies communication module.
- Law enforcement agencies Assessment module.
- Information sharing module.
- Online learning and Training Module.
- Publications and Reports Module.
- Laws, conventions, treaties, and agreements Module.
- Private Sector Alerting Module.
- People Awareness.

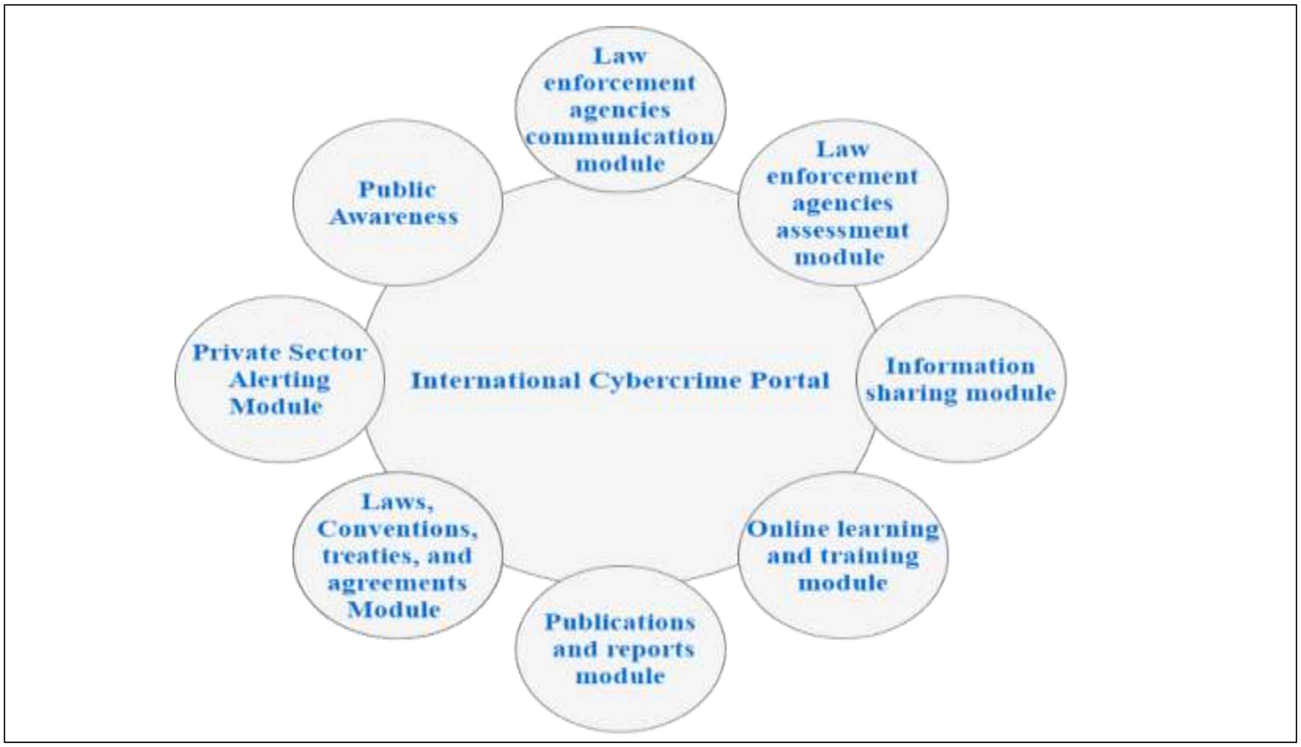

Law enforcement agencies communication module
Public Awareness
Law enforcement agencies assessment module
Private Sector Alerting Module
International Cybercrime Portal
Information sharing module
Laws, Conventions, treaties, and agreements Module
Online learning and training module
Publications and reports module

Fig. 1. *Cybercrime Portal Modules.*

The designed demo version here is applied for the law enforcement agencies' communication module. The user interface for the whole portal is prepared to be ready for the implementation of the other modules in the near future. The law enforcement's communication module is designed to solve the complexity of communications between law enforcement agencies in combating cybercrime, speedup, and facilitating procedures for investigating cross-border cybercrimes. In this module, the data flow between the module and two different types of users, local law enforcement agency users, and international law enforcement agency users, as explained in Figure 3 and Figure 4.

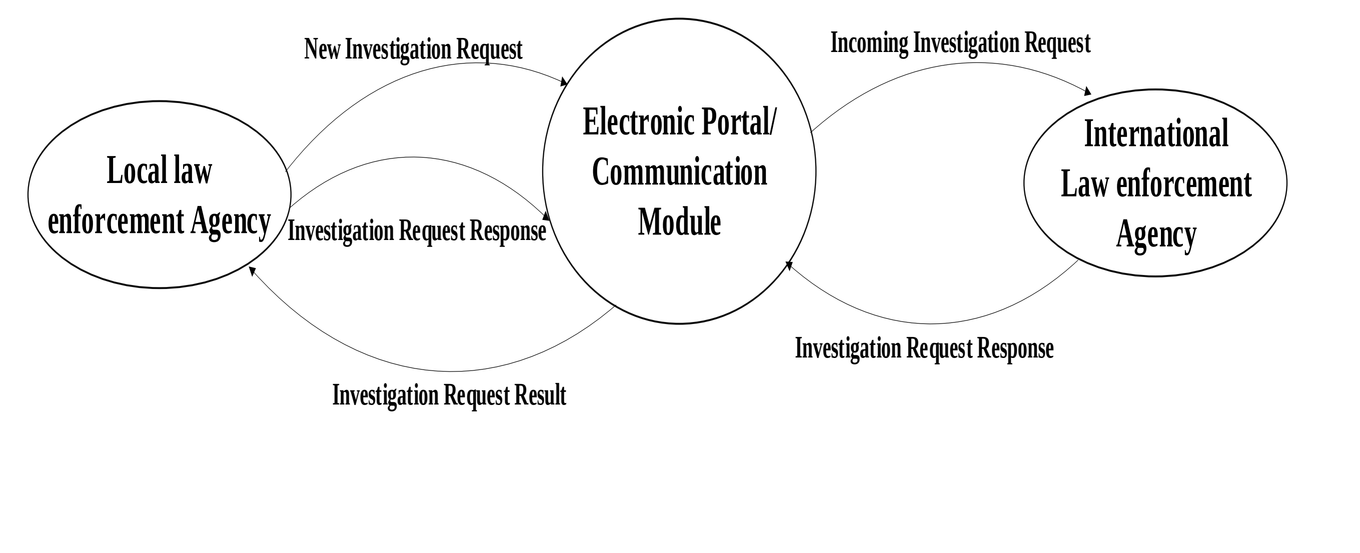

New Investigation Request
Incoming Investigation Request
Electronic Portal/ Communication Module
International Law enforcement Agency
Local law enforcement Agency
Investigation Request Response
Investigation Request Response
Investigation Request Result

Fig. 2. *Context Diagram for Law Enforcement Agencies' Communication Module.*

The law enforcement agencies' communication module is divided into two sub-modules based on the different types of agencies and users. The first sub-module is the local law enforcement agency sub-module. In this sub-module the local law enforcement agencies user's activities are described. The local law enforcement agency user orders a new investigation request. The local law enforcement agency user reviews the list of sent investigation requests, respond to any more information needed by the international agency or the attack source country. This user type can also receive the results of investigation requests. Also, he reviews the incoming investigation requests and responses to these requests.

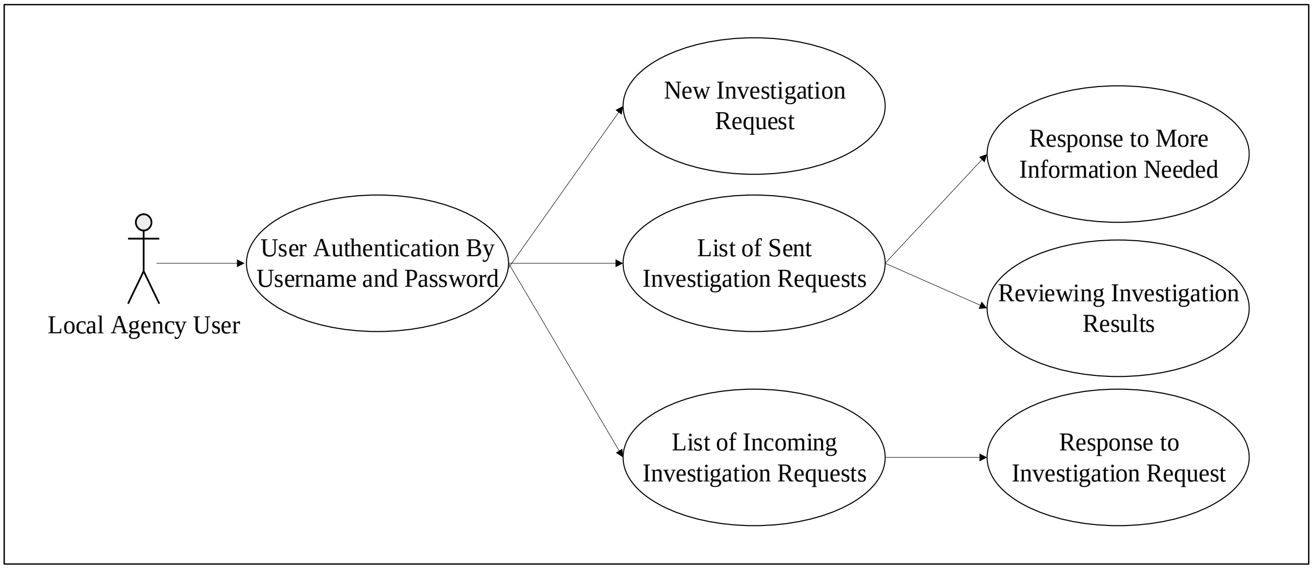

New Investigation Request
Response to More Information Needed
User Authentication By Username and Password
List of Sent Investigation Requests
Reviewing Investigation Results
Local Agency User
List of Incoming Investigation Requests
Response to Investigation Request

Fig. 3. *Use Case Diagram for Local Law Enforcement Agency Users.*

The second sub-module is the international law enforcement agency sub-module. In this sub-module, the international law enforcement agency user's activities are described in Figure 4. The international law enforcement agency experts are responsible to review the investigation requests between local users of different countries. If more information or details are needed by the international agency from the requesting country, the investigation request is returned to the requesting country. Then the international law enforcement agency transfers the investigation request to the attack source country.

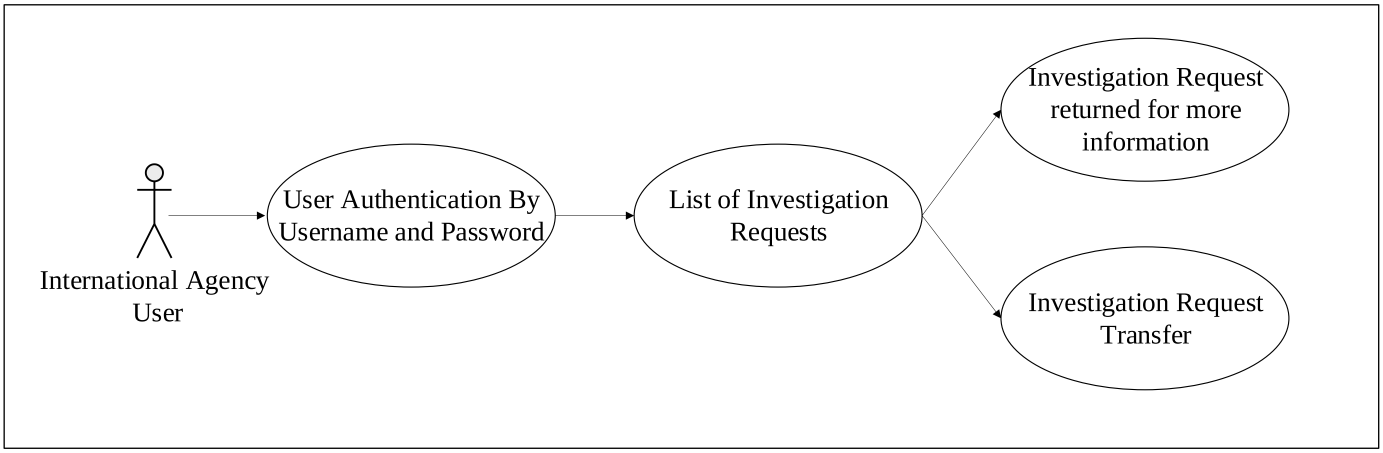

Investigation Request returned for more information
User Authentication By Username and Password
List of Investigation Requests
International Agency User
Investigation Request Transfer

Fig. 4. *Use Case Diagram for International Law Enforcement Agency Users.*

The law enforcement agencies' communication designed module is implemented to provide the local and international law enforcement agencies a secure communication channel to facilitate and speed up the communication between them to speed up the investigation process in cross border cybercrimes. In addition, a secure channel for the technical assistance requests is used for investigating cybercrime cases. When the local investigators determine the source of the cyberattack from another country, there is a need for investigation or assistance from the law enforcement agencies in the source country.

The local law enforcement agency authenticates to the portal using their account by user name and password. Then they can fill the form of investigation/ assistance request. In the case of bilateral agreements, the requested investigation/ assistance is directly transferred to the local user of the attack source country. While the international agency analyzes the request to decide if more information needed from the attacked country or it is possible to transfer the request directly to the law enforcement agency in the local user of the attack source country if no bilateral agreements exist. Therefore, the investigators in the attack source country can respond to the investigation request. Finally, the investigation result will be transferred directly to the law enforcement agency in the attacked country.

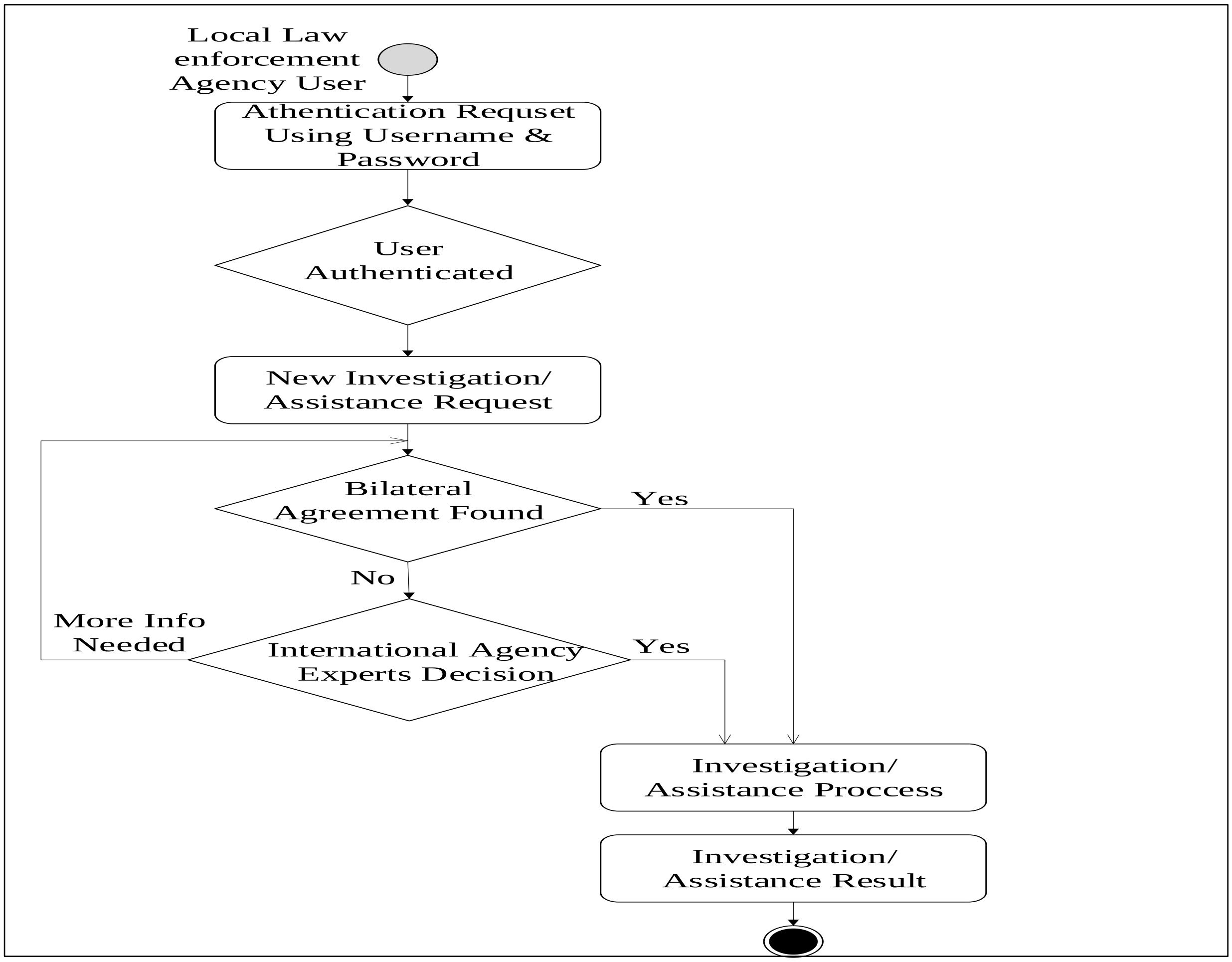

Local Law enforcement Agency User
Athentication Requset Using Username & Password
User Authenticated
New Investigation/ Assistance Request
Bilateral Agreement Found
Yes
No
More Info Needed
International Agency Experts Decision
Yes
Investigation/ Assistance Proccess
Investigation/ Assistance Result

Fig. 5. *Law Enforcement Agencies Communication Module.*

A simplified form of the proposed portal is designed and implemented using asp.net web programming technology with C# programming language in Microsoft Visual Studio environment and Microsoft SQL Server as a Database engine. In the proposed design, the other modules and services such as training and education, experience exchanging, and information related to cybercrime can be in the future included in the design.

3. Results

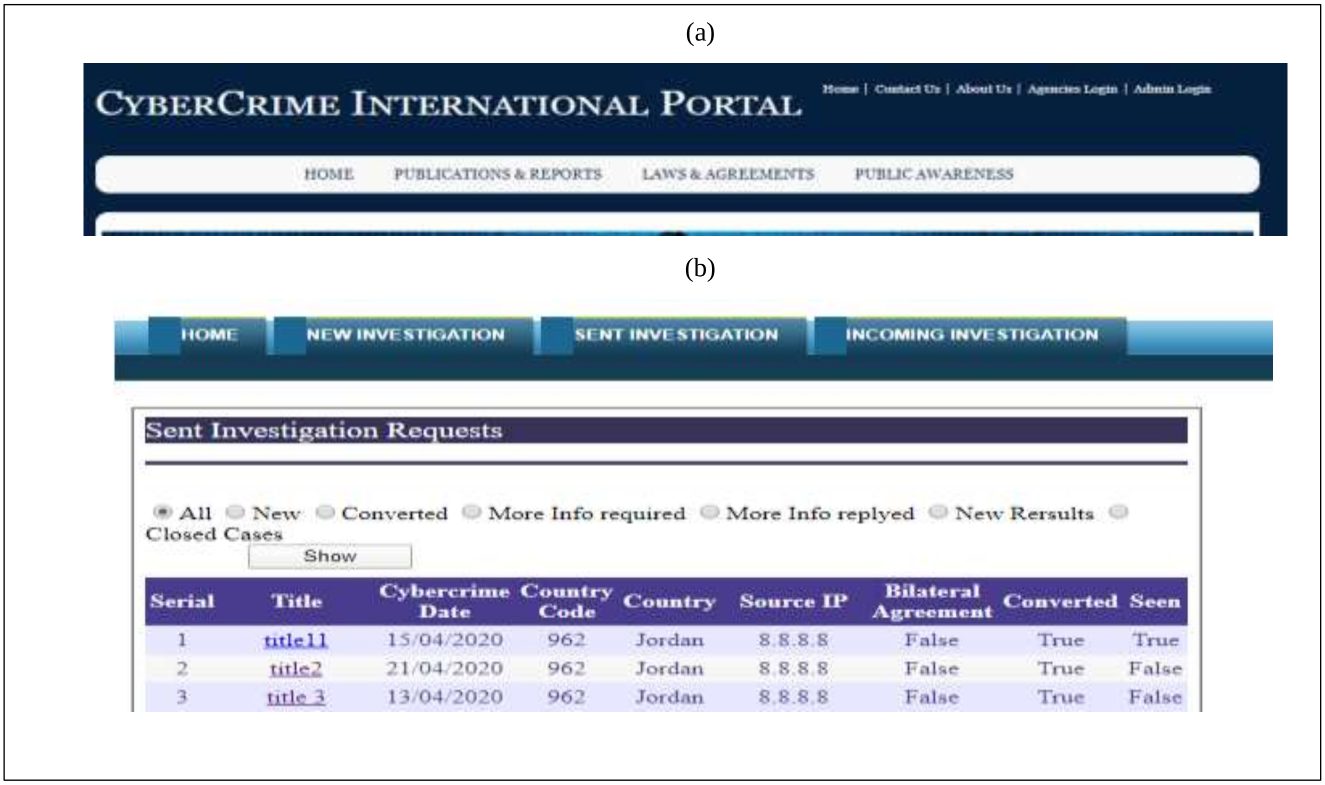
Depending on the discussed international cooperation cybercrime laws legal, technical, and operational challenges, a communication portal was designed with the proposed modules. The proposed portal is designed by a web-based technology with a centralized database administered and supervised by an international agency or office under the United Nations Organization. The sample web implementation of the portal is shown in Figure 6. It was considered that the portal should be comprehensive to provide services to various groups of users, such as the technical and legal staff of law enforcement agencies, experts, researchers, private sector, and for those interested in topics of cybercrime.

In the portal's workflow, the different types and permissions of users have been identified such as international agency users, local law enforcement agencies users. The communication between agencies was taken into consideration by the direct communication between the countries that have bilateral agreements. As well, indirect communication through the international agency of the countries without bilateral agreements is applied. This portal is a preliminary reference model for starting a project related to international cooperation in the field of cybercrime. At this stage, the module on communication between law enforcement agencies was implemented and examined in terms of requesting investigation between users from different states.

This solution was subjected to an evaluation process and discussions about the possibility of enhancing international cybercrime cooperation by referring to an expert from Palestinian Public Prosecution [26]. Generally, it was accepted that the proposed cybercrime international portal with the eight modules that are shown in Figure 1 can enhance the cross-border cybercrime investigations. As well, the evaluator confirmed that the communication process during cross-border cybercrime investigations is one of the most difficult challenges due to political conflicts, lack of bilateral and unified international agreements, differences between states' domestic laws and regulations, and long diplomatic communication process … etc. Therefore, the availability of a direct, unified, and systematic communication process between the local law enforcement agencies under the control of a unified international law enforcement agency will highly contribute to mitigating the complexity of international communication challenges.

The implemented module was tested and validated by creating virtual users and countries. The users were created in different user types such as international agency users (admin) and local agencies users. Some countries were considered to have bilateral cybercrime agreements, while other countries do not have bilateral agreements. Virtual cross-border cybercrime cases were assumed for different users. Successful implementation results were obtained for different conditions.

In the case of bilateral agreements availability, the requests and responses were successfully applied directly between the source and the attacked countries users without any inference of the admin from the international agency. As well, the cross-border cybercrime cases between countries without bilateral agreements were successfully forced to be managed under the control of the admin from the international agency. The figures (6a-6c) show some of the implementation testing processes.



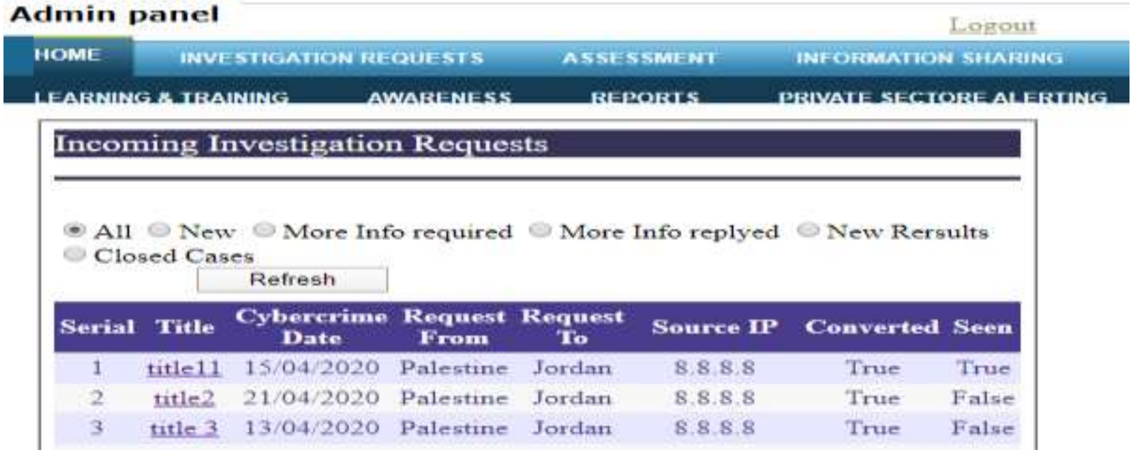
Sent Investigation Requests

● All ○ New ○ Converted ○ More Info required ○ More Info replyed ○ New Rersults ○ Closed Cases

Show

Serial	Title	Cybercrime Date	Country Code	Country	Source IP	Bilateral Agreement	Converted	Seen
1	title11	15/04/2020	962	Jordan	8.8.8.8	False	True	True
2	title2	21/04/2020	962	Jordan	8.8.8.8	False	True	False
3	title 3	13/04/2020	962	Jordan	8.8.8.8	False	True	False

(c)



Incoming Investigation Requests

● All ○ New ○ More Info required ○ More Info replyed ○ New Rersults ○ Closed Cases

Serial	Title	Cybercrime Date	Request From	Request To	Source IP	Converted	Seen
1	title11	15/04/2020	Palestine	Jordan	8.8.8.8	True	True
2	title2	21/04/2020	Palestine	Jordan	8.8.8.8	True	False
3	title 3	13/04/2020	Palestine	Jordan	8.8.8.8	True	False

Fig. 6. *Portal Implementation: (a) is the basic home page menu with different user types login and the main menu; (b) is the basic page for the list investigation requests; (c) is the basic administration control panel that managed by an international agency for investigation requests other related modules in the menu.*

4. Conclusion

The International cooperation of cybercrime laws challenges classified in terms of legal, technical, and operational, see Table 1. The cross-border cybercrime causes the greatest harm on a large scale, whether against countries, societies, businesses, or individuals as provided by most of the national and international reports. The harm caused by cross-border cybercrime varies according to the motivations of cybercriminals, whether organized criminal groups, terrorist groups, or individuals. By the review of many national and international reports, it was noted that international cooperation against cybercrime is one of the most complicated challenges due to different national and international laws and agreements. The study proposed a web-based portal solution to contribute to the mitigation of combating cross-border cybercrime challenges. This portal contributed to mitigating the complexity of international communication, contributed to legal and technical staff capacity building in domestic law enforcement agencies, contributed to knowledge publication for public people, researchers, and experts.

The proposed portal enables the contribution of public and private sector cooperation. In this solution, the bureaucracy in international communications during the cybercrime investigation can be avoided. As well, such types of solutions take advantage of the bilateral agreements and international agreements as choices for a faster investigation process. For different agencies and staff, the learning, training, experience exchange, and knowledge sharing can be enhanced with minimal cost possibilities using the portal. The communication module, which was implemented, tested, and evaluated, would enhance and speed up the cross-border cybercrime investigation by mitigating the international communication complexity between countries. This demo version can be extended in the future to include other proposed modules to be a comprehensive international cybercrime portal.

The challenges for the practical implementation and usage of the proposed solution should be studied by international law experts and researchers to override the expected legal difficulties and obstacles. For example, the absence of comprehensive international law, unified law enforcement agency, and the lack of harmonization of national laws with regional and international laws and agreements can still be obstacles during the implementation and use of the proposed solution. The cross-border cybercrime combating can be enhanced by the leadership of cybercrime international law enforcement agencies.

5. References

[1] Shahbazi, A. (2019). Technological development in cyperspace and comission of the crime in international law and Iran. Journal of Legal, Ethical and Regulatory Issues, 22(4), 1–12.

[2] Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses. Cogent Social Sciences, 5(1). doi:10.1080/23311886.2019.1675404

[3] Mittal S. and Sharma, P. (2017). A review of international legal framework to combat cybercrime. International Journal of Advanced Research in Computer Science, 8(5), 1372–1374.

[4] Khweiled, R., Jazzar, M., & Eleyan, D. (2021). Cybercrimes during COVID-19 Pandemic. International Journal of Information Engineering & Electronic Business, 13(2).

[5] Gercke, M. (2014). Understanding cybercrime: Phenomena, challenges and legal response. International Telecommunication Union [ITU]. Retrieved September 17, 2020, from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

[6] Sawaneh, I. A. (2018). Examining the Effects and Challenges of Cybercrime and Cyber Security Within the Cyberspace of Sierra Leone. *International Journal of Intelligent Information Systems*, *7*(3), 23. doi:10.11648/j.ijiis.20180703.11

[7] Brar, H. S., & Kumar, G. (2018). Cybercrimes: A Proposed Taxonomy and Challenges. Journal of Computer Networks and Communications, 2018, 1-11. doi:10.1155/2018/1798659

[8] Ajayi, E. F. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1-12. doi:10.5897/jiis2015.0089

[9] ITU Estimate. (n.d.). Retrieved September 17, 2020, from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[10] 2019 Internet Crime Report Released. (2020, February 11). Retrieved October 14, 2020, from https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[11] Challenges in the age of cyberspace. (n.d.). Retrieved October 14, 2020, from http://www.supremecourt.justice.nsw.gov.au/Documents/Publications/Speeches/2016%20Speeches/McDougall_20161021.pdf

[12] Billah, M. (2018). Sufficiency of Omani laws to suppress cybercrimes in light of the UN comprehensive study on cybercrimes. Arab law quarterly, 32, 158–184.

[13] Combatting Cybercrime: Tools and Capacity Building for ... (n.d.). Retrieved October 15, 2020, from https://openknowledge.worldbank.org/handle/10986/30306

[14] Council of Europe [COE] (n.d.). Council of Europe[Online]. Retrieved from: https://www.coe.int/en/web/portal/home. [Accessed 15 April 2020].

[15] Law by Decree No. 10 of 2018 on Cybercrime The President ... (n.d.). Retrieved October 15, 2020, from https://security-legislation.ps/sites/default/files/law/Law%20by%20Decree%20No.%2010%20of%202018%20on%20Cybercrime.pdf

[16] Palestine, P. P. (n.d.). Public Prosecution - State of Palestine [Online]. Retrieved from: http://www.pgp.ps/ar/SP/Pages/TheAnti-CyberCrimesProsecution.aspx. [Accessed 02 April 2020].

[17] UNODC. (n.d.) Cybercrime [Online]. Retrieved from: https://www.unodc.org/unodc/en/cybercrime/index.html. [Accessed 25 April 2020].

[18] INTERPOL. (n.d.). Cybercrime[Online]. Retreived from: https://www.interpol.int/Crimes/Cybercrime. [Accessed 15 April 2020].

[19] Challenges in the age of cyberspace. (n.d.). Retrieved October 14, 2020, from http://www.supremecourt.justice.nsw.gov.au/Documents/Publications/Speeches/2016%20Speeches/McDougall_20161021.pdf

[20] Sunde, N. A. D. I. (2019). Cognitive and human factors in digital forensics: Problems, Challenges, and the Way Forward. Digital Investigation, 29, 101–108.

[21] 2019 Internet Crime Report Released. (2020, February 11). Retrieved October 14, 2020, from https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[22] Peters, A. and Jordan, A. (2019). Countering the cyber enforcement gap: Strengthening Global Capacity on Cybercrime [Online]. Retrieved from: https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime. [Accessed 20 March 2020].

[23] Quarshie, H. (2017). Cyber Crime in a World without Boarders. Texila International Journal of Academic Research, 4(2), 1–7.

[24] Ratten, V. (2019). The effect of cybercrime on open innovation policies in technology firms. Information technology & people, 32(5) 1301–1317.

[25] Chernenko, E. (2018). Increasing international cooperation in cybersecurity and adapting cyber norms [Online]. Retrieved from: https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms. [Accessed 27 March 2020].

[26] Nisreen, R. Interviewee personal communication. (17 March, 2020). Palestinian cybercrime prosecutor [Interview].