جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
أوراق السياسات الأمنية
https://nauss.edu.sa/
Security Policy Papers
https://spp.nauss.edu.sa/index.php/spp
ورقة تحليل سياسات أمنية

سياسات التعاوُن الرقمي بين الأجهزة الأمنيَّة العربيَّة

Digital Cooperation Policies between Arab Security Agencies

Key Outcomes:

- Exchanging information and data within the means of transferring information developed and required to be developed through the channels of international co-operation to encounter international crimes through secured applications and technological software.
- Early examination of information indicating the association of terrorist cells or criminal organizations within states through joint investigations and information evidence.
- Providing means of communications and transmitting information among Arab police agencies in order to achieve complete confidentiality.

Abstract

Digital security cooperation among countries contributes significantly to the decline and elimination of organized crimes, particularly terrorist crimes. This suggests the need for states to be mutually motivated and to increase efforts in order to encourage and activate such cooperation by creating cooperative means in security matters to prevent crime and locate the perpetrators in case any incidents occur. This can be achieved by using reliable networks that allow the transfer of data, information and applications among the concerned Arab police services, and the use of secured and fast techniques that allow digital exchange of information among police agencies. Such efforts shall prevent and detect crimes, prosecute criminal and terrorist plots in all its forms, and get information ahead in order to maintain the national security of Arab states.

1.Introduction

The history of information is closely related to the history of humanity. Since the human being who has the information becomes the fittest, the information is the source of power, the cornerstone of the process of development. The digital cooperation in the field of external criminal security is concerned with information that has to do with any activity (criminal or terrorist) outside the state that could threaten the internal security of the state (Shafiq, 2019).

Digital policies and their issues have recently imposed, especially after the COVID-19 crisis, on the world a process of rapid digital transformation in many sectors. The digital transformation has become a reality that all countries of the world address with the disparity in capacity and potential. It is worth considering the important role and formulation of digital policymaking in the security decision making and rationalizing process. Therefore, "digitization" plays an important role in the process of decision making and rationalizing in light of the transformations taking place in the world in the field of digitization (Abdul Sadiq, 2020).

As an indicator, ICT has spread globally, accounting for about 4.57 billion internet users, representing about 59% of the world's population.

Information & Communication Technology (ICT) is the main technology for change in societies of the present day, and it has moved the world from the information economy to the knowledge economy. In fact, the development and promotion of ICT is the cornerstone of the economic structure. Information is the meaning derived from the data, and sources of information include the following: computers, means of communication and the network of information and data that can be stored, processed, retrieved and transmitted by these computers, as well as all the software necessary to operate these systems. On the other hand, informatics is the rational handling run by automatic machines using information as a pillar of the capacity of regulatory agencies, law enforcement agencies, and other agencies specialized in combating money laundering, terrorism and organized crime; in other words, information is the petrol of the century (Al Jundi, 2014).

The research problem is represented in the variety and development of crimes from one society to another and from one state to another, along with the rapid development of technology and the use of the cyber environment in committing crimes and cyber-attacks, whether on the criminal or terrorist side. This leads to the inability to confront international crime with the means to thwart it; therefore, it is urgently needed to strengthen digital exchange to combat crime. Thus, it is extremely necessary to stress and encourage the exchange of information among the criminal police authorities. Furthermore, we have to bridge the digital gap among the Arab security services, as the process of digital cooperation among Arab security agencies and institutions is

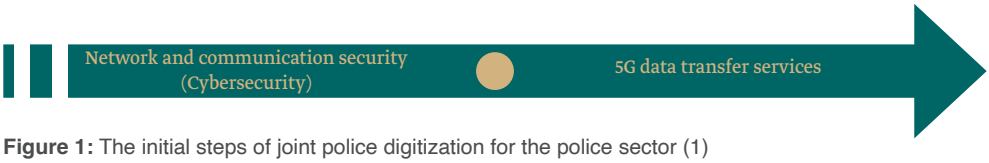

Figure 1: The initial steps of joint police digitization for the police sector (1)

extremely difficult. This paper offers the appropriate solutions to increase the volume of security information exchange with the aim of preventing crime (the official website of the Ministry of Communications, 2016).

2. Concerns about international digital security cooperation in combating crime

International cooperation in the field of security, on different levels, achieves several key objectives that truly represent the new aspects of this cooperation and increase the need to reach such goals. One can say that such efforts represent in their essence goals that all security institutions in the Arab countries seek to achieve in order to reach the objectives of building bridges of cooperation among Arab security institutions and achieving Arab national security.

No single state can combat transnational crime in a way that is different from others, as the basic work of the security agencies depends on a core axis that is complemented by the collection and exchange of information with international law enforcement agencies in various areas of combating transnational crime. Such a type of crime takes on aspects that go far beyond the traditional work of law enforcement agencies; therefore, policies of digital cooperation among Arab security agencies must be developed to address common challenges and coordinate work among themselves to track terrorist and criminal organizations whose activity goes beyond state boundaries.

In addition, It is important to coordinate efforts to process information among countries and utilize technical tools, artificial intelligence techniques, information records and tools to trace terrorist cells through which they operate before and after the crime. Furthermore, criminal information applications are necessary tools that are considered one of the cores for international and Arab police information and coordination. No single state can eliminate or minimize crime on its own, especially if it is cross-border committed by individuals or

Figure 2: The development of digital policies among Arab police agencies

groups organized in a particular state and then transferred to another state, reducing the chances of arresting, and punishing the perpetrators. Hence, the priority is to focus on digital security cooperation to enable law enforcement agencies in countries to fight crime in all its forms and maintain Arab national security through the use of rapid technological development and artificial intelligence technologies (UAE, 2020).

Figure (1) highlights the initial steps towards developing digital cooperation policies among Arab security agencies.

Figure (2) also refers to the development of digital policies among Arab police agencies by integrating and exchanging technologies as well as transferring and exchanging the required information through a joint strategy by transmitting information through private, secured and fast networks in order solve the mysteries of cases, prevent crimes at various levels (criminal, terrorist or organized) and protect public security in the states. In fact, the prevailing challenge in the Arab and African region is terrorism, and it is a threat that threatens the whole world. It does not consist of an individual or two, but it is run by organizations supported by states that provide funding to achieve suspicious interests and objectives. There is a direct correlation among security and development, as there is no growth, prosperity and development without security.

The relationship between security and the economy is a harmonious one that cannot

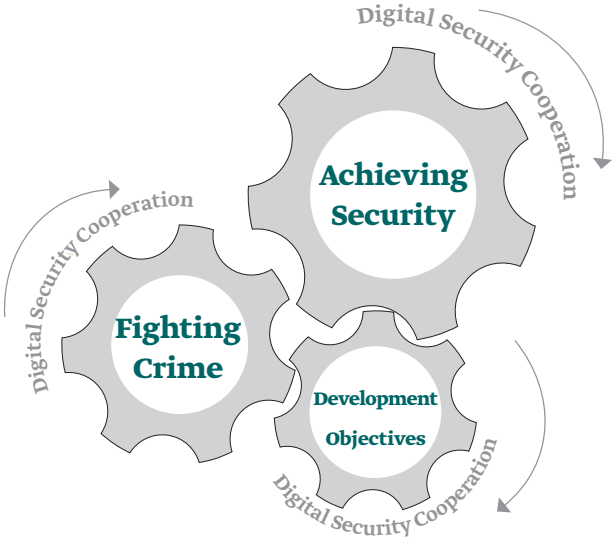

Figure 3: the role of digital cooperation in strengthening the relationship between security and sustainable development goals and combating crime (Al Babli, 2021).

be separated, and one cannot survive without the other for a long time. However, security is the most important factor, as if the economy relapses, it may not lead to a direct deterioration in security, while if security deteriorates, the economy will relapse as a direct result of the deterioration of security. The more the economy grows, the higher the standard of living of citizens and the greater the well-being of the citizen, the more indebted we become to the security personnel who have created a safe and stable environment that has enabled us to give, produce and contribute to the building of the economy, as figure (3) illustrates.

3- The themes of developing digital cooperation policies among Arab security agencies:

- First: collecting, analyzing and assessing information related to terrorism: threat levels must be identified, warnings have to be issued, and information collected should be analyzed. Moreover, and the experience of police and government counter-terrorism departments and agencies should be combined, as the information is analyzed and processed on a common basis with the participation of the Interpol and Europol in exchanging new applications and genetic fingerprint applications (The National Anti-Corruption Academy, 2019).
- Second: exchanging security information: it is important to promote the exchange of information concerning terrorist groups' activities, crimes, leaders, members, locations, training centers, sources and sources of financing and arming, means of communication, communication and propaganda, and the travel documents they use.

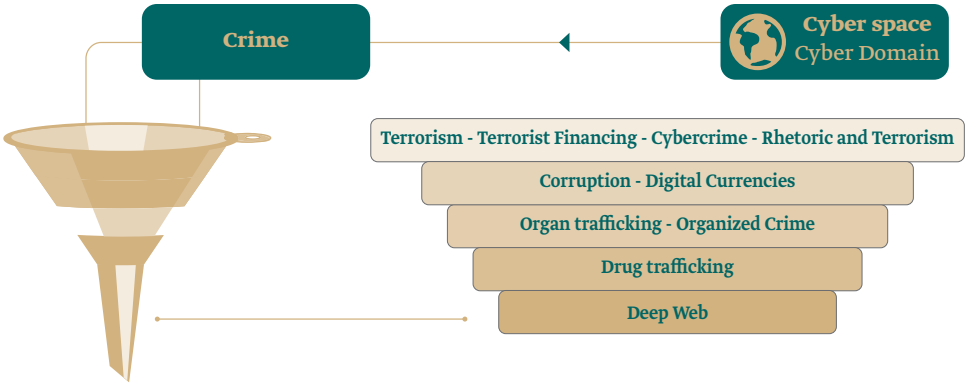

Figure 4: Crimes in Cyberspace

It is also essential to exchange information and data in various areas of security, particularly activities and crimes of terrorist or hostile groups and organizations, organized crimes, trafficking offences and illegal trafficking and use of narcotic drugs and psychotropic substances as well as the perpetrators (Al-Saeed, 2013).

- Third: investigations: assistance should be provided in the investigation and arrest procedures for fugitives accused or convicted of terrorist offences.
- Fourth: securing the confidentiality of information and enforcing the information security policies: security protection should be provided for data transfer and applications, and information encryption systems and 5G services should be used to transfer data at a high speed.

Targeted Digital Security Cooperation Frameworks:

A- Towards a joint digital policing strategy (Digital Policing) To exchange information in joint investigations and gather evidence, Arab States should consider concluding multi-party agreements that allow the competent authorities to establish joint investigative bodies while addressing matters that are the subject of international investigations, prosecutions or judicial proceedings in one or more countries. The concerned states must ensure full respect for the sovereignty of the state party where such an investigation will be conducted within its territory. This can be done by adopting a common strategy by various Arab police agencies to reach a close vision on the areas where these security institutions should follow in similar footsteps. In addition, assistance

Monitoring mailing addresses online	Monitoring international bank account numbers	Social network accounts
Personal accounts online.	Suspected relatives	Aliases and code names
Previous visas and places of residence	Organizations they belong to	The relationship of the organizations to each other and the sources of funding

should be provided to disseminate border management strategies, promote border control capabilities, help law enforcement, and create applications, software and information exchange systems to prevent and combat drug trafficking and other crimes, such as: trafficking firearms and illegal weapons, and money laundering. Moreover, the capabilities of law enforcement and criminal justice agencies should be reinforced in forensic science related to drug trafficking in terms of collecting, preserving, and presenting forensic evidence in order to prosecute drug-related offenders (Khalifa, 2018).

B- Digital Means of Collaboration (Digital Information Exchange)

Most of the new crimes occur in the realm of cyberspace, and terrorist and criminal organizations communicate under the cover of the electronic space, making it difficult for the security services to track and trace them as shown in Figure (4).

In the event of having digital security cooperation, the means of investigations, exchange of information, tracking such members, and collecting information about all will be enhanced dramatically.

The researcher will address the ways of digital cooperation as follows:

Terrorism crimes and financing of terrorist groups:

- Promoting the exchange of information on the identity, locations and past activities of suspects. It is also important to share the means and methods used to commit such crimes, the Movement of money laundering proceeds and terrorist financing by the means and techniques used to commit such crimes (Interpol, 2021).
- Exchanging information on activities and crimes of terrorist groups and organizations, mutual relationship, leadership, members, secret organizational structures, public cover, main centers, means of financing, training methods, weapons they use, and digital information in terms of the following:
  - Cooperating to exchange investigations and information regarding the crimes that have been identified as well as revealing the suspects' identity, locations and activities, and the movement of funds related to these crimes.
  - Exchanging applications and databases that are being developed to collect, maintain, and update information on money laundering and terrorist financing offences, including information provided by states and regional and international organizations. Moreover, it is essential to develop, retain and update integrated lists of this field, as well as exchanging information with

state parties in the area of money laundering and terrorist financing crimes (United Nations, 2021).

- Developing and strengthening methods of monitoring and exchanging information to reveal plans or activities aimed at transferring, importing, exporting, storing, or using weapons, ammunition, explosives and other materials and other means that help to commit terrorist acts across borders.

- The role of information exchange in combating corruption crimes:
  - Cooperating among law enforcement authorities, and the need for each state party to take measures by initiating and providing useful information to the competent authorities for the purposes of investigation and proof, as well as exchanging criminal records of perpetrators of corruption in order to use such information in criminal proceedings to control criminal circles and gangs.
  - Consult experts in analyzing prevailing corruption trends, circumstances in which corruption crimes are committed, exchanging statistics and analytical experience on corruption, and sharing experiments with anti-corruption practices (Ali, 2020).
  - Exchanging information on the means and methods used to commit or conceal corruption offences, including crimes committed using modern technology and early detection, as well as cooperating in conducting investigations regarding the identities of suspects involved in corruption crimes, their locations and activities, and the movements of proceeds and property obtained from such crimes.

- Exchanging information among law enforcement agencies to control perpetrators

  Communication channels should be strengthened to facilitate the safe and speedy exchange of information on crimes, including their links to other criminal activities and crimes against public security. Information should be also shared on the identity, locations, activities, or other persons involved, as well as the movement of criminal organizations and the tools used in committing such crimes. Necessary materials should be provided for analysis or investigation, and technical assistance tools within the investigation and video work within criminal laboratories, examination and analysis must be shared (Al Wazzan, 2014).

- Container control program:
  - The United Nations Office on Drugs and Crime established the Container Control Programme (CCP) in 2004,

Evidence of Acquittal or Conviction	Rape	Suicide	Murder	Terrorist Incidents
	Unidentified Bodies	Proof of Parentage Cases	Crime Scenes	Identifying Missing Persons

and it consisted of over 30 port control units and significantly helped raising the level of detecting and confiscating drugs and other illegal goods. Under the CCP, the World Customs Organization and the United Nations Office on Drug Control and Crime made great efforts to establish modern port control units and use the World Customs Organization's Network Communication Platform (CENcomm) as an international information exchange tool to gather information from units established under the CCP and from other port

Viruses and malware	Ransomware software
Malicious software to collect data	Malicious bot software
Piracy for cryptocurrency mining	Hidden Network and Deep Internet
Previous Cyber Incidents	

control experts around the world. (Containers, 2019).

- Exchanging and linking databases with Arab ports through fast and secured electronic platforms. Previously recorded information regarding violations, crimes and persons who had previously committed multiple smuggling crimes, whether drug smuggling, human trafficking or contraband, is exchanged. It is worth mentioning that it is essential to link these databases to the INTERPOL and Europol system since the nature of container transport through ports is an international issue and is not limited to Arab countries.

- Transnational organized crime
  - Exchanging information and data about transnational organized crimes, leadership, members, organizational structures, activities, mutual relationship, experience related to methods and means of control, and the advanced and developed systems of the combating agencies. Joint measures should be taken to ensure confronting various transnational organized crimes, especially money-related crimes, smuggling and laundering, as well as smuggling artifacts and illegal trafficking of cars.
- Illegal production, trafficking and use of narcotic drugs and psychotropic substances:
  - Exchanging information and data on crimes of illegal production, trafficking and use of narcotic drugs and psychotropic substances as well as the involved perpetrators in accordance with the laws of each country. It is also important to exchange information and expertise relevant to control means and methods, the developed and innovated systems used by control authorities, and the latest investigative methods.
  - Setting up and maintaining surveillance equipment at free ports, airports and border checkpoints, and providing useful information to governments of countries involved in drug smuggling, cultivation and trafficking (Al Arabiya, 2021).
  - Exchanging drug-related information, where appropriate, among law enforcement agencies and border control through channels that include the following: multi-party electronic portals, information centers, and the United Nations Office on Drugs and Crime's regional networks. It is also essential to conduct joint investigations and coordinate operations to detect, disrupt and dismantle organized criminal groups in domain of illegal production and trafficking of narcotic drugs and psychotropic substances (Omran, 2021).
  - Exchanging information and data on crimes of illegal production, trafficking

and use of narcotic drugs and psychotropic substances as well as the involved perpetrators. It is also important to exchange information and expertise relevant to control means and methods as well as latest developments, the updated and innovated systems used by control authorities, and the mutual assistance in field matters.

- Providing mutual assistance in the field of procedures for apprehending fugitives accused in cases or wanted in drug trafficking crimes.

- Exchanging DNA Databases:
  - Exchanging DNA information and records plays an effective role in detecting perpetrators of crimes, as it allows linking crimes series, or determining the presence of a suspect at the crime scene. The DNA data may also help prove the innocence of a suspect, especially in the following circumstances:
- Cybercrimes and Hacking Information Systems:
  - In light of the continuing development of the cybercrime phenomenon, Arab police agencies are forced to share information and knowledge in order to take real-time, information-based action on the compilation of digital criminal evidence and the exchange of development research.

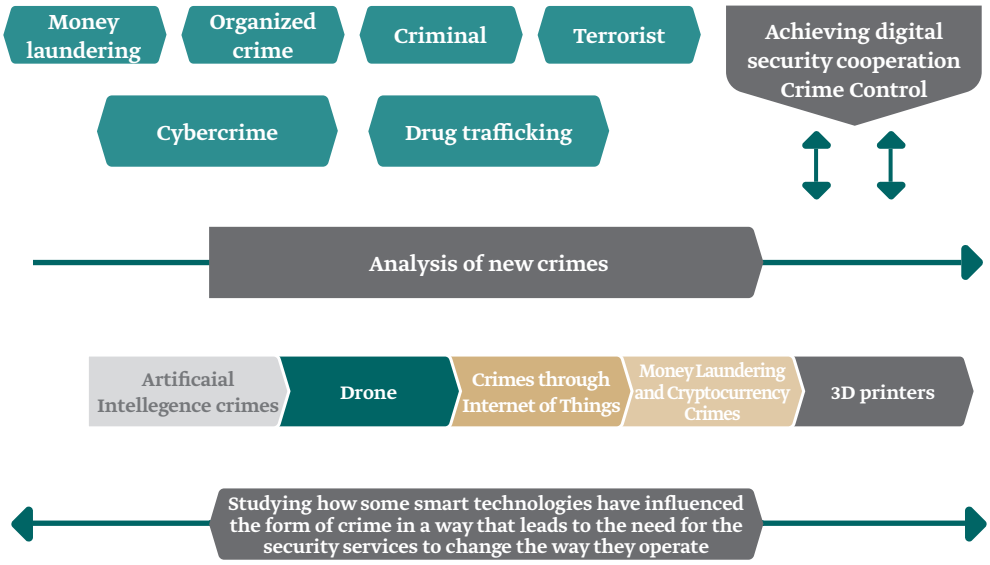

Figure 5: Digital Security Cooperation in Crime Control

- Reviewing the progress of data from one country to another as well as the IP tracking data (IP address).
- Exchanging cybercrime data and records as a service, as criminals use new techniques to commit cyberattacks against governments, companies and individuals. Such crimes are not confined to specific borders, whether physical or hypothetical, and they cause serious damage and concrete threats against victims around the world. This makes exchanging technologies extremely important, particularly for police agencies required to combat cybercrime in order to understand the potential they offer criminals and how to use them as tools to combat cybercrime, especially how they exploit the changing behaviors and trends on the Internet in light of the Covid-19 epidemic.
- Exchanging the expertise of security agencies by bridging security gaps associated with systems management, which criminals may attempt to exploit to collect and analyze available information on criminal activities in the digital space with the aim of providing states with consistent intelligence information that can be translated into practical and technical action. In fact, the ultimate objective of exchanging information through Arab police agencies:

Protecting critical electronic infrastructure from cyber hacking, and protecting important and vital facilities from cyberattacks, particularly Denial of Service (DoS) attacks.

- Exchanging knowledge related to cybercrime among law enforcement agencies, governments, international organizations and experts from cybersecurity and information security companies in order to exchange non-police field information related to cybercrime. This can be accomplished through joint collaboration to provide communications and exchanges for users to discuss the latest cybercrime trends, prevention strategies, and detection and investigation techniques with authorized colleagues in the Arab countries.
- Exchanging artificial intelligence platforms for cybersecurity, as AI can process over 100 terabytes of global threat data per day, starting with hundreds of threat intelligence to identify emerging threats, which allow police in Arab countries to align their defense against them before they attack.

- With over 4.5 billion people online, more than half of humanity is at risk any moment of falling victim to cybercrime, which calls for digital cooperation among police agencies in Arab countries along

with partnership and cooperation with cybersecurity companies. In fact, cybercrime is one of the most widespread forms of international crime. It is estimated that it will cause the global economy $10.5 trillion in losses annually between now and 2025 (Morgan, 2021).

- Enhancing cyber competencies, knowledge and technical capabilities, including training programs, projects, tools, capacity-building platforms and information and communication security in order to allow police in Arab countries to effectively combat cybercrime.
- Exchanging digital evidence management databases for the purposes of investigations and prosecutions to collect digital evidence in accordance with the law, and to preserve evidence and present it in an understandable and acceptable way to the courts.
- Exchanging linking tools between cyber and actual information by finding the relationship between digital traces and actual information in order to locate the perpetrators of cybercrimes.
- Cooperation services in the field of combating cybercrime by activating the role of joint training among Arab police agencies on the level of investigations, technical examination methods and tools, the extraction of electronic digital evidence and the exchange of information on social engineering and relevant risks and damages to citizens, companies and banks (Shafiq, 2019).
- Exchange available information on any money laundering crime, provided that an explanation is given on the circumstances surrounding the crime, the perpetrators, the victims, the injured, the resulting effects, and the methods used utilizing cyberspace, the Internet and the Deep Web as a cover. This enables security services to exchange mailing addresses, track down the “profiles” and “accounts” of the perpetrators, using electronic digital evidence tools and programs for examination and tracking across networks, and follow the movements of the digital criminal impact within the cyber domain and identify the locations of danger, gatherings, terrorist organizations and their activities on the social networks.
- In order to achieve digital security cooperation within the field of cyberspace, there should be partnership between telecommunications companies, giant technology companies, and sectors concerned with the cyber field within the Arab police agencies and the International Telecommunication Union. This will help activate the field of research and tracking of crime fighting in which criminals use cyberspace to

commit their illegal acts (Kamel, 2011).

- Developing common standards for digital forensic tools to collect dark web evidence in computers.

Figure 4 indicates the security importance of digital security cooperation in the fight against crime:

5. Mechanisms for implementing and achieving digital cooperation among Arab security agencies:

- Establishing an international counter-terrorism information center to develop methods for exchanging information, collecting complete data on members or suspects belonging to terrorist groups, means of terrorist recruitment, places of training, sources of funding, types of ammunition used, information analysis, prediction of operational objectives, and strengthening cooperation among specialized agencies though data (Al-Saad, 2020). This center shall exchange information through the following ways:
  - Creating a virtual network to exchange information with the aim

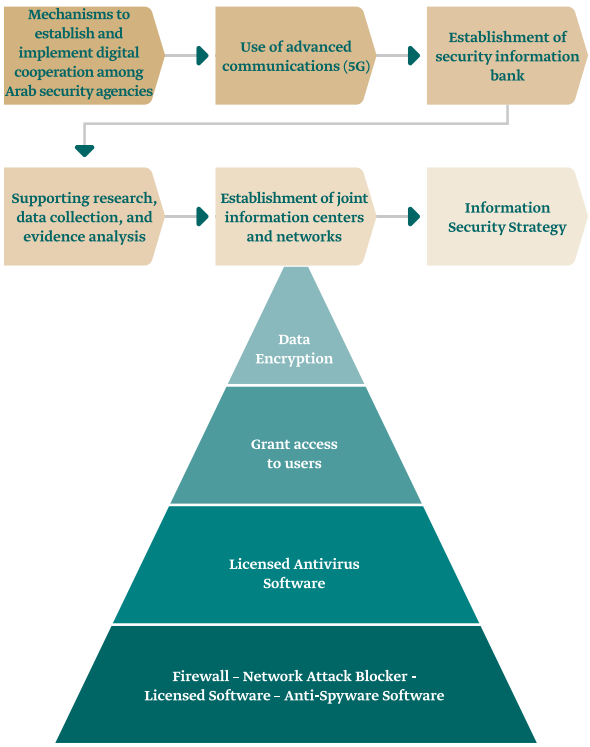

Figure 6: Mechanisms to establish and implement digital cooperation

of strengthening policing to promote the fight against terrorism, as it has become necessary for Arab security services to communicate more effectively.

- Establishing a security information bank to monitor all data on dangerous terrorist organizations of an international character, support confidence by recalling information, speed up the identification process of all matters relating to terrorist activities, and approve the creation of an information bank for foreign fighters. We look forward to expanding the circle of digital cooperation to reach EU countries, particularly Europol since many young Europeans remain influenced by the extremist ideology and may turn into lone wolves carrying out terrorist attacks at any time, which cannot be expected or prevented.

- Coordination and cooperation among the various security institutions in the Arab security arenas in order to eventually achieve a reduction in crime rates, besides completing bridging the gap in security information through international digital cooperation to collect and exchange security information at the Arab level. Moreover, there always should be work to develop databases and information to combat international crimes and detect terrorism plans and organized crime.
- Providing the opportunity to manage transnational security vulnerabilities and work to provide the best ways to address them in order to prevent and control terrorist crime.
- Encouraging the prompt exchange of information among law enforcement agencies, the Public Prosecution Office and relevant financial units. It is also essential to provide statistical information and analysis related to the cultivation, production, manufacture, illegal drug trafficking and money laundering for various purposes, such as: reflecting and analyzing such information in order to strengthen the measures taken by the criminal justice agencies in this regard.
- Promoting proactive information exchange and coordination among financial institutions, law enforcement agencies, intelligence and judicial bodies through an Arab intelligence platform, as well as coordination with the International Police Agency (INTERPOL), including a database of suspicious transactions.
- Imposing strict procedures and following new conditions for the use of prepaid phone cards, as the purchase of such cards was without official documents. They also must be enlisted in the databases of civil records and civil registry. Moreover, the digital reference data, such as fingerprints in national identity cards, shall be made mandatory.
- Supporting research, data collection,

evidence analysis and information exchange. It is also important to strengthen the measures taken by law enforcement, criminal justice and legislative bodies through promoting international cooperation in order to prevent and combat drug-related criminal activities using the Internet in accordance with relevant applicable provisions of law (Al-Saad, 2020).

- Using advanced communications - fifth generation (5G) - it is the next technological revolution in mobile broadband, which will enable the exchange of information among police agencies in the Arab countries to quickly search for information while enjoying much faster download and upload speeds with a low level of latency. This means the time it takes for devices to connect to wireless networks is significantly reduced. 5G networks provide significantly faster data speeds, with peak data rates reaching up to 20 Gbps (Al Babli, 2018).
- Securing information and communication networks (cybersecurity) and maintaining the confidentiality of information by applying cybersecurity strategies in accordance with the quality of information security as in the quality of information security for ISO IC 27001. Actually, they are the set of information capabilities that institutions use to protect and repel cyber-attacks, and they can be described as a set of technical and non-technical means that allow the defense of critical information systems in cyberspace, as well as all the tools necessary to achieve cyber security to maintain the information infrastructure. This is extremely necessary to apply when creating and activating the information networks that transmit data, applications and virtual networks in order to exchange information to protect them from electronic intrusions and piracy operations. The following reviews the most important technical security points needed to achieve cyber security, secure networks, and transfer information among Arab police agencies:

Anti-Hacking Protection Systems:

- IT has a variety of ways to protect networks, and the most important of which is firewalls, which have multiple features including spam filtering, virus protection capabilities, IDS/IPS detection and prevention, filtering web page content, and the conventional functions of firewalls. (Al-Babli, 2018).
- Unified Threat Management Equipment (UTM): traditional firewalls were known as filters, and they eventually evolved into UTM (Unified Threat Management) equipment. It is convenient to run two firewalls together, one main and one backup. When the first fails the second works in its place, and firewall operating systems have instructions that must be carefully prepared to determine how long the backup wall should wait until it

takes over.

Users Permissions and Identity Systems:

- Technologies and equipment, or a combination of both, for the organization to use to verify the identity of an access requester (user) and to allow only those who are permitted to access network resources.
- Installing state-of-the-art intelligent TV monitoring systems in all computer facilities, focusing on the hardware and communications room with facial recognition systems.
- Promoting the use of barometric fingerprints inside information centers and sensitive systems, and for registering users of networks linking police agencies in Arab countries in order to grant authorized access to devices, systems and databases to avoid identity theft or loss or misuse of sensitive data.

Operating Systems and Hardware Security:

- Updates: updating operating systems for servers, computers, and network devices such as routers, extenders, wireless access points and software in order to prevent vulnerabilities that result from not updating the system.
- Many measures should be taken to protect operating systems and software applications from the risks of disruption caused by vulnerabilities and manufacturing errors by installing corrective and security updates issued by manufacturers. This can be achieved by having an environment similar to the production environment to test the updates before installing such updates in the production environment (National Cybersecurity Authority, 2018).

Information Encryption Systems:

- The purpose of information encryption is to protect the confidentiality of digital information. Data or plain text is encrypted using an encryption algorithm and an encryption key. The process results in an encrypted text, which can only be displayed in its original form if it is decrypted using the correct key.
- Many measures should be taken to protect operating systems and software applications from the risk of crashes caused by vulnerabilities and manufacturing errors by installing corrective and security updates issued by manufacturers. This can be achieved by having an environment similar to the production environment to test the updates before installing such updates in the production environment (National Anti-Corruption Academy, 2019).
- Figure 6 indicates the mechanisms of digital cooperation among security agencies:

6. Conclusion

The international community is struggling for the transformation from analog to digital technology in a more comprehensive and efficient manner than ever before. What makes this endeavor complicated is the hope that technology will flourish

while avoiding limitless dangers that may occur if not all measures and procedures are taken to reach the desired objective. Despite the advantages that result from digital technological progress, it is tainted by some challenges due to the growing digital divides, cyber threats and human rights violations on the Internet. That is why it was necessary for the United Nations to establish a kind of international digital cooperation in order to have a more peaceful and stable digital global community, progressing towards a bright and prosperous future.

International digital security cooperation is of paramount importance in combating transnational organized crime. This is due to the nature and specificity of such crimes as well as being considered one of the most dangerous modern criminal systems, as it also has dire consequences that affect all aspects of the international and national community alike. In light of the changes taking place in the world, no country no matter how advanced and powerful it is, can confront the phenomenon of crime alone. This is due to the wide range of crimes and their spread across countries.

International digital security cooperation also leads to the widest exchange of expertise among Arab security agencies, which leads to raising the efficiency of these agencies to be able to deter organized criminal groups due to the fact that such digital cooperation provides information and data that a single state is unable to provide. This also helps to reveal members of criminal, terrorist and cyber groups. The cross-border nature of such crimes requires the existence of broad and continuous channels of communication, especially at the level of information collection and information.

Recommendations:

- Artificial intelligence can be used to detect threats and other potentially malicious activities, and traditional systems cannot keep up with the huge number of malware that is created. Here is where artificial intelligence can step in and address this problem. Cybersecurity companies teach AI systems to detect viruses and malware using complex algorithms, so AI can turn on pattern recognition in programs. AI systems are trained to identify even the smallest behavior of ransomware and malware before they enter the system, and then isolate them from the system. They can also use predictive functions that go beyond the speed of traditional methods.
- Encouraging the provision and investment in digital goods, such as software, data, and artificial intelligence models, and contributing to achieving sustainable security development goals.
- Adding a “DNA” fingerprint and a face and eye print to the national ID card database, with the aim of making it easy to identify people anywhere without

stopping them, asking them to show their identity and locating people wanted by security.

- Promoting digital public goods in order to create a more equitable world, ensure digital inclusion for all - including the most vulnerable groups, enhance digital capacity building, support global international cooperation in the field of artificial intelligence, and improve confidence and security in this environment.

Organizing specialized scientific meetings and conferences to support this cooperation in order to enhance international relations and cooperation and exchange expertise, best practices and advice in the areas of enhancing global peace and security.

Arabic References:

الأكاديميَّة الوطنيَّة لمكافحة الفساد. (2019). الإستراتيجيَّة المصرية الثانية لمكافحة الفساد (2018 - 2021). إستراتيجيَّات مكافحة الفساد، القاهرة.

الأمارات، ح. د. (2020). السلامة السيبرانية والأمن الرقمي. دبي: حكومة دولة الأمارات..https://u ae/ar-ae/information-and-services/ justice-safety-and-the-law/cyber-safety-and-digital-security.

الأمم المتحدة، م.م. (نوفمبر، 2021). تبادل المعلومات. متاح على الرابط التالي: https://www.gcc-sg.org/ar-sa/ CooperationAndAchievements/ Achievements/SecurityCooperation/ Achievements/Pages/ Seventhcooperationinthefightag.aspx.

البابلي، عمار ياسر. (2018). الآليَّات الحديثة لحماية وتأمين نُظُم المعلومات وآثارها على المنظومة الأمنيَّة. رسالة دكتوراه. أكاديميَّة الشرطة، كليَّة الدراسات العليا. القاهرة. ص 204.

الجندي، م. (2014, ديسمبر). البيانات الضخمة بترول قرن ال 21. القاهرة: مجلة لغة العصر.

الحاويات، ب.م. (2019). مكتب الأمم المتحدة المعني بمكافحة المخدرات والجريمة.

خليفة، إيهاب. (2018). تنامي التهديدات السيبرانيَّة للمؤسَّسات العسكريَّة. اتجاهات الأحداث. مركز المستقبل للأبحاث والدراسات المتقدِّمة، أبو ظبي، الإمارات العربيَّة المتَّحدة. العدد 22. متاح على: https://futureuae.com/ar/Activity/ Item/.

السعد، صالح. (2020). محفِّزات التعاوُن الدَّولي في محاربة الإرهاب، التحالف الإسلامي العسكري لمحاربة الإرهاب، متاح على: https://www. imctc.org/ar/Pages/default.aspx.

السعيد، أحمد. (2013). تكنولوجيا المعلومات في المجال الأمني. دار النهضة العربيَّة. القاهرة.

شفيق، نوران. (2019). أشكال التهديدات الإلكترونيَّة ومصادرها. دراسات مكافحة الإرهاب. المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات. برلين، ألمانيا.

عبد الصادق عادل (2020). مُنظَّمة التعاوُن الرقمي: آليَّة جديدة نحو التنمية المستدامة. مركز الأهرام للدراسات السياسيَّة والإستراتيجيَّة. القاهرة. متاح على: https://acpss.ahram.org.eg/ News/17017.aspx

العربية، 1. (2021). التعاون في مجال مكافحة المخدرات. متاح على الرابط التالي: https://www.gccsg.org/arsa/ CooperationAndAchievements/ Achievements/SecurityCooperation/

الوزان، السيد حلمي. (2014). سلطة المعلومات: رؤية أمنيَّة معاصرة. دار النهضة العربيَّة. القاهرة.

الهيئة الوطنية للأمن السيبراني. (2018). الضوابط الأساسية للأمن السيبراني. متاح على: https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

Foreign References:

INTERPOL. (2021). report identifies top cyberthreats in Africa https://www.interpol.int/a. 33

Morgan, Steve. (2021). 2021 report: cyberwarfare in the C-suite. Cybersecurity Ventures. Available at: https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

Achievements/Pages/Seventhcooperationinthefightag.aspx

علي، معتز عبد الرحمن. (2020). دور التبادُل الدولي للمعلومات في الإثبات الجنائي: دراسة مقارنة. رسالة دكتوراه. أكاديميَّة الشرطة، كلية الدراسات العليا. القاهرة. ص 33.

عمران، أ. (2021). توصيات الجلسة الختامية للمؤتمر العربي 34 لرؤساء أجهزة مكافحة المخدرات. متاح على الرابط التالي: https://gate.ahram.org.eg

كامل، شريف سيد. (2011). الجريمة المُنظَّمة. دار النهضة العربيَّة. القاهرة.

الموقع الرسمي لوزارة الاتصالات. (2016). مركز المعلومات. متاح على الرابط التالي: https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

Received 09 Sep. 2021; Accepted 20 Oct. 2021; Available Online 31 Dec. 2021.

Amar Yaser Elbably

Researcher in Information Security

Egypt

عمار ياسر البابلي

باحث في أمن المعلومات

جمهورية مصر العربية

Keywords: Security Studies, Information Security, Digital Cooperation, Information Exchange, Cooperation Policies

الكلمات المفتاحية: دراسات أمنية، الأمن المعلوماتي، التعاون الرقمي، تبادل المعلومات، سياسات التعاون.

Production and hosting by NAUSS

* Corresponding Author: Amar Yaser Elbably

Email: 3marelbably@gmail.com

doi: 10.26735/HJOO8882