جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences

Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Cybersecurity Management for Virtual Private Network (VPN) Applications: A Proposed Framework for the Governance of their Use in the Kingdom of Saudi Arabia

Shahad A. Alashi*, Hanaa A. Aldahawi
Department of Information Science, King Abdulaziz University, Jeddah, Saudi Arabia.

Received 15 Jul. 2020; Accepted 25 Oct. 2020; Available Online 20 Dec. 2020

Abstract

By using the research process, this study addresses the attitudes of the members of Saudi society towards using Virtual Private Network (VPN) applications and the former's perceptions of the latter's concept, security, and privacy, in addition to monitoring their risks to cybersecurity. The main objective of the study is to present a proposed framework for the governance of the use of VPN applications in the Kingdom of Saudi Arabia to strengthen cybersecurity management. To achieve the objectives of the study, the researchers used two methods: the social survey method and the content analysis method. The researchers also relied on the questionnaire tool to collect information from the 455 individuals in the study sample. The study yielded a set of findings, the most important of which are as follows: The use of free VPN applications represents 91% of the sample of the study. Also, the study revealed confusion in perceptions of the actual concept of VPN applications, which may be common among users, and showed a diversity of attitudes and motives for using VPN applications, most of which are related to entertainment. Moreover, the study showed that the study sample individuals had some knowledge about the risks of VPN applications to cybersecurity, although most of them did not use cyber protection means. The study recommended the need to organize and manage the use of VPN applications, conduct an evaluation of VPN applications available on Saudi smartphone stores, and prohibit those which contain security vulnerabilities and malware. The study proposed a framework for the governance of the use of VPN applications in the Kingdom of Saudi Arabia, which comprised three dimensions: legal, organizational and awareness-based dimensions.

I. Introduction

The progressive development of information technology and communications and the growing dependence on them impose new dimensions and ways of attacks that threaten all cyberspace-related issues. In light of the development of cyberthreats and their many forms such as malware, phishing, ransomware attacks, and distributed denial-of-service (DDOS) [1] attacks, and as they have become more destructive than before, cybersecurity has become an urgent necessity to counter and address them. One of the attitudes in the use of technology that leads to cybersecurity threats is the virtual private network (VPN) applications within the smartphone environment, which has spread in the past few years in the world in general and in the Kingdom of Saudi Arabia in particular. Concurrent with the problems that have emerged,

Keywords: *Information Security, Cybercrime, Virtual Private Network (VPN) Applications, Network Security, Cybersecurity, Cybersecurity Management, Cybersecurity Governance, Internet Governance.*

Production and hosting by NAUSS

* Corresponding Author: Shahad A. Alashi
Email: Alashi100@gmail.com
doi: 10.26735/VSDJ4585

such as geographic blocking on many websites, censorship in its many forms, and the increase in piracy activity that endangers data [2], their risks may target individuals or institutions to obtain confidential information or because they are driven by a material motive. They may also misuse or destroy sensitive information for political, economic, or even ideological and intellectual purposes, or they may target the infrastructure of the state in its most harmful form. This calls for cybersecurity to adopt governance and management approaches to ensure the organized use of these applications and to achieve the principle of technology sustainability in light of its cybersecurity. Cybersecurity governance is a framework for managing risks, overseeing compliance and control responsibilities, and defining the cyber mission by mapping structure, authority, and processes to create an effective program that reduces risks associated with cyberspace [3], therefore strengthening the concept of cybersecurity management. Driven by the importance of the application of this concept, the current study seeks to address the risks of using VPN applications to cybersecurity by analyzing the attitudes of their users in Saudi society and presenting a proposed framework for the governance of their use in the Kingdom of Saudi Arabia to strengthen cybersecurity management.

A VPN is considered one of the tools used to secure an internet connection and help counter cybercrime threats [4]. However, their emergence as applications in the smartphone environment and the attitudes towards their use may lead to risks affecting cybersecurity, which includes electronic data and information security, operating system security, wireless network security, device security, and national security. The latter was added "because in the age of networks the scope of national security has changed," [5] so what affects community cybersecurity will affect national cybersecurity as well. According to a survey conducted on the use of VPN applications worldwide, Saudi Arabia ranked sixth [6], which reveals the widespread use of these applications. From this standpoint, the need arose to uncover the attitudes of the members of Saudi society towards the use of VPN applications, monitor their risks to cybersecurity, and present a proposed framework for the governance of their use in the Kingdom of Saudi Arabia to strengthen cybersecurity management.

In addition, to demonstrate the importance of the study, the contents of the Saudi Vision 2030 aim to strengthen and enhance cybersecurity, whether at the level of governments and business enterprises or at the level of individual users of computers and smart phones. Therefore the current study has special importance, as it seeks to address a topic related to cybersecurity in the Kingdom of Saudi Arabia by reviewing VPN applications, whose risks to community and national cybersecurity have been highlighted by previous studies. This study is important, as it identifies the attitudes of the use of VPN applications in Saudi society and presents a framework for the governance of their use in the Kingdom of Saudi Arabia. No studies have yet addressed the governance of the use of VPN applications in the Kingdom of Saudi Arabia. This study will therefore contribute to specialized knowledge in this field.

There are many objectives of this study, which aims to present a proposed framework for the governance of the use of VPN applications in the Kingdom of Saudi Arabia to strengthen cybersecurity management. The objectives will be achieved by looking into VPN applications, their essence, services, and risks, and by researching the perceptions of Saudi society members of the concept of VPN applications. Besides that, the study explores the extent of Saudi society's knowledge of cybersecurity means for smartphones when using VPN applications and identifies the attitudes of Saudi society members towards using VPN applications. In addition, the study looks into the extent of Saudi society's knowledge about the cyber risks of VPN applications.

Furthermore, the main question of the study is represented in the following: What is the appropriate framework for the governance of the use of VPN applications in the Kingdom of Saudi Arabia to strengthen cybersecurity management?. To achieve the objectives of the study and to obtain appropriate data to solve its problem, some sub-questions should be identified such as: What are VPN applications, and what are their services and risks? What are the perceptions of Saudi society members of the concept of VPN applications? What is the extent of knowledge among Saudi society members of the cybersecurity means for smartphones when using VPN applications? What are the attitudes of Saudi society members towards using VPN applications? To what extent are Saudi society members aware of the cyber risks of VPN applications?

II. Methodology and Tools of the Study

In collecting the necessary data to achieve its objec-

tives, the study relied on the following methods:

- An integrated theoretical review of research on the topic of VPN applications on smartphones and their risks to cybersecurity, to establish a theoretical vision upon which to base the completion and analysis of the applied aspect of the study. The review was based on Arabic, English, and Chinese research.
- The use of the social survey method as the main method which "is used to describe the attitudes of samples of individuals representing a certain society, which allows generalizing the results of the survey to the society from which the sample was taken."[6]. This is the appropriate method to study the attitudes of Saudi society members towards using VPN applications. The study will adopt the sample survey method due to the difficulty of conducting a comprehensive survey of all the study individuals. To achieve the objectives of the study, an electronic questionnaire was used to collect information from the study sample. This questionnaire was prepared based on the theoretical framework derived from reviewing the literature related to the subject of the study in a manner consistent with the objectives of the study providing answers to its questions. The validity of the tool of the study was confirmed by presenting it to a group of reviewers from the faculty members in the Department of Information Science who have scientific knowledge of digital security. It was reviewed, and the necessary modifications were made. The questionnaire questions were coded, and data was entered and analyzed using SPSS v.22 software, and a set of appropriate statistical tests were conducted. A 95% trust ratio has been adopted with a 5% error rate.
- The use of the content analysis method as a support method which depends on the analysis of specialized research that addresses the field of the study, to present a proposed framework for an appropriate plan for the governance of the use of VPN applications in the Kingdom of Saudi Arabia to strengthen the concept of cybersecurity management.

The original population of the study is represented by the Saudi society members who use VPN applications on smartphones. Their number amounted to 10,535,460, representing 39% of the total internet users on smart phones in the Kingdom of Saudi Arabia, according to the statistics of a global social media management company for the year 2019 [7]. Given the difficulty of limiting the original population of the study, a non-probability accidental sampling method was adopted, which is a type of sample that does not depend on mathematical calculations to ensure its representation of the original population. The greater the sample size, the more it reflects the reality of the society it represents. The sample comprised 455 individuals, which is a "very good" representation of the original population according to the assessment of the adequacy of the sample representing the population [8]. The study was applied to the sample during the period from 02/03/2020 to 03/04/2020.

III. Previous Studies

Cybersecurity management is directing, guiding, and improving the decisions and actions of individuals to organize the use of VPN applications through the procedures and means that protect devices, operating systems, wireless networks, software, electronic information and national security from cyberattacks. VPN applications are applications installed on smartphones which provide a connection to a fake private network that increases security by encrypting internet traffic and changing the IP address, and showing the user to be in a different location from his actual location [2]. It is an organizational framework consisting of a set of procedures, policies and practices that guide the organization and control of the use of VPN applications in the Kingdom of Saudi Arabia to strengthen cybersecurity management.

After following all research methods in intellectual production, several studies from outside of Saudi Arabia were reviewed in this section that discussed the subject of study from different aspects. They are arranged objectively according to two axes and on a chronological sequence from the most recent to the oldest within each axis, as follows:

A. The First Axis: Studies on the Factors that Drive and Influence the Use of VPN Applications

Namara et al. [10] investigated the emotional and practical considerations towards adopting and rejecting VPNs as a technology to enhance privacy. The study used the survey method on 90 skilled technicians and relied on

the questionnaire and interview tools to explore the motives for using VPNs and the barriers in their adoption. The study found that 98% of the participants had knowledge about VPNs, and 81% used them as a technology to enhance privacy. Moreover, the study found that people who use VPNs for privacy purposes are primarily driven by emotional considerations such as the strong desire to protect their privacy on the internet, in addition to the fear of censorship and data tracking from the internet service providers (ISPs), governments, and companies like Facebook and Google. Conversely, people motivated by practical considerations give up using VPNs, especially when their practical need is no longer there. They cite their access to alternative technology and the effort required to use VPNs as reasons to abandon the use of these applications [9].

Pavlicek & Sudzina, [11] study addressed the effect of personal and demographic features on the use of VPNs and proxy servers. The study used the survey method on 478 university students in the Czech Republic relying on a questionnaire to collect information from the study sample. It focused on the variables of gender, age, and the type of student's job as variables that control the use of VPN applications. The study concluded that conscience affects the use negatively, while openness to experience affects it positively. The study also found that males have more tendency towards use, and students with full-time jobs are the most frequent users compared to all other jobs [10].

B. The Second Axis: Studies on the Risks of VPN Applications in Smart Phones Environment

Asela & Parakum, [12] addressed the use of VPNs in smartphones and the extent of user awareness among Facebook users in Sri Lanka during the period in which social media was banned. The study aimed to determine the extent of users' awareness of security and privacy risks in VPNs applications by using the survey method and relying on the questionnaire tool to collect information from the study sample. The study concluded that 85% of the study sample individuals admitted using VPN applications during this period, and only 21.74% of users were unaware of the security risks related to VPN applications [11].

Zhang et al. [1] conducted an in-depth analysis of the security of 84 open-source VPN applications on Android from several aspects, namely client profile, code execution, and permission management. The study revealed three types of misconfigurations found in many applications which are the insecure custom protocols, poor client-side authentication, and invalid file permissions on Android. These misconfigurations may lead to some dangerous attacks such as decrypting VPN traffic and attacks launched accordingly, which will put users' privacy at risk. The study reviewed the potential causes for these misconfigurations and offered practical recommendations for developers to securely provide VPN services. In the same context, Ikram et al. (2016) also analyzed the privacy and security risks of 283 VPN applications on Android and concluded that 75% of the tested applications used libraries belonging to third parties and are therefore untrusty, and that 82% of the applications requested access to sensitive resources such as users accounts and text messages. In addition, more than 38% of these applications contain malware such as Adware, Trojan, Malvertising Riskware, Spyware, and 18% of the tested applications failed to encrypt user traffic. Moreover, the study showed that in some of the applications which offer online anonymity, some of their developers have sought to collect personal user information that can then be sold to external partners [12].

Donovan [14] aimed to clarify the extent to which vulnerabilities in the Android system could be used to penetrate a VPN connection and concluded that attackers were able to bypass a secure VPN connection using a security vulnerability in the Android system and to divert traffic from an Android device into a system controlled by the attacker, leaving the user completely oblivious to the belief that data is encrypted and secure [13].

Tao [15] revealed the effects of VPN applications for smart phones on network security and concluded that they affect the security of the state network because they work to bypass state censorship on the information network through which many illegal activities are carried out via the internet, since the user's real IP address is hidden and therefore it is difficult to trace their location. The study revealed that this effect brought great challenges to overseeing the security of the information network and suppressing network crimes, and as such these applications affect the cybersecurity of their users' devices and the state network as a whole [14].

The abovementioned studies have a direct and indirect relation to the subject of the current study. They were reviewed to identify the visions and attitudes relating to

the research problem. These studies are considered as supportive studies to the current study, rather than being major studies. It appears that they focus on analyzing the risks of VPN applications. Like the previous studies, the current study contains an analysis of the motives and attitudes of the use of VPN applications and the factors that affect this use. This study differs in that it seeks to specifically uncover the attitudes of Saudi society towards the use of VPN applications and to address their risks by presenting a proposed framework for governing its use in the Kingdom of Saudi Arabia to achieve cybersecurity management.

IV. Theoretical Framework

A. Cybersecurity Management for VPN Applications: A Research Vision

First, we refer to the concept of cybersecurity as a set of tools, policies, concepts, security precautions, guidelines, risk management methods, procedures, best practices, safeguards and technologies that can be used to protect cyberspace and the user's assets in it. It includes connected computing devices, infrastructure, applications, services, communication systems, in addition to sent and stored information [16]. Thus, cybersecurity seeks to ensure that the security features of the user's assets are obtained and preserved against security risks related to cyberspace. Due to developments in the use of information and communication technology, including networks that have enabled individuals and societies to be linked in a single infrastructure, cyberthreats have also evolved. Therefore, the interest in cybersecurity has increased at all levels. This has necessitated the formation of the concept of cybersecurity governance, which is a form of cybersecurity management that is good governance. Since they are relatively recent concepts and have great importance and are in general still the subject of research and controversy, we present a research vision related to the subject of the study.

Based on the above, the cybersecurity management of VPN applications is concerned with guiding the decisions and actions of users to organize the use of VPN applications through procedures and means that protect devices, systems, wireless networks, electronic data, information and national security from cyberattacks. Accordingly, we realize that cybersecurity management of VPN applications is a form of internet governance at the level of the one-state, as being applications that go beyond the control of both the state and the internet service provider (ISP). This necessitates that the concerned authorities must lay down a framework for their use, in anticipation of their risks. This must be done through organizing and controlling their use by adopting sound foundations, policies, and procedures that adapt to this technology and its risks, which is related to the concept of cybersecurity governance.

B. An Overview of VPN Applications on Smartphones

VPN applications on smartphones are widespread, as they are applications based on preserving the privacy of users through an encrypted connection in a way that helps add a layer of protection to the internet connection; everything sent and received via the network when connected will be encrypted [12]. Researchers, such as Abo-Seada [17] and Hassan and Hijazi [2] indicated that the concept of VPNs can be expressed as a technology that creates a private and encrypted tunnel for its user's activity over the internet, making it difficult for any party to see what the user is performing via the internet or to monitor the user. In addition to that it helps to change the geographical location and provides a virtual IP address. This will make it difficult for the websites visited by the user to know his identity and location. We see the concept as a network rather than an application, as it is a network whose characteristics have been employed to suit the smartphone's environment that has been provided through applications installed through stores available on smart phones such as App Store, Google Play Store, and others.

It is important to note that a balance must be made between the concepts of anonymity and privacy when using VPN applications. These applications do not support anonymity to level that enables the network user or system to remain anonymous, because it is possible to track the endpoints of a VPN connection, the required information to maintain a VPN connection. However, other tools offer anonymity such as the Tor application. The problem implied in anonymity solutions is that they do not always protect privacy. In many cases, the traffic that these applications carry anonymously is not encrypted,

which means that the attacker can read it with access to the right part of the network. Privacy on the other hand is to keep information about the network or system user from being disclosed to unauthorized people. When there is need for privacy protection, the VPN connection will be effective because it encrypts the data it carries [18].

C. VPN Applications Services

1) Secure Connection Service:

- It secures browsing the internet in general, and its importance increases where public Wi-Fi networks are used such as those available at coffee shops, hotels, or airports, because of the attacks they contain that enable access to the user's device [19].
- Blocks ads from browsers and applications [20].

2) Privacy Protection Service:

- This service works to bypass the censorship of the internet service provider (ISP) and the work or school network [19].
- It prevents the tracking of browsers and applications [21].

3) Confidentiality Service:

- Provides a virtual IP address [22].

4) Change of Geographical Location Service:

- It helps in accessing sites, games, services, and applications blocked due to geographical location, or those available in specific geographical areas [23].
- It prevents price discrimination based on geographical location, such as e-commerce sites and flight booking sites [21].

5) Internet Connection Boost Service (Latency Reduction):

- In general, a VPN reduces internet speed, but sometimes it can be used to boost it in electronic games. This feature is not always effective as it depends on the user's location, the location of the game's servers, and the VPN to which the user is connected [24].
- Internet websites that are increasingly popular at certain times face pressure on their servers. When connected to a VPN, these sites become faster to access than without a VPN connection [21].

D. Risks of VPN Applications to Cybersecurity

We have previously discussed that a VPN, from a positive side, is a tool that secures internet connection, but like other technologies, it is accompanied by a set of negative repercussions that affect cybersecurity as a result of misuse and poor design. Therefore, the decisive factor is the user's awareness of the security risks carried by these applications. For accurate clarification and identification of risks, we propose to divide them as follows:

1) Risks Threatening Electronic Data and Information Security:

Most VPN applications that were examined were found to violate privacy, as they follow weak privacy policies. Moreover, some of them do not contain privacy policies at all. Therefore, their developers seek to collect users' data and to sell them to third parties such as advertising companies [13]. Some of these applications include permissions that require access to sensitive resources such as users accounts on smartphones [25]. They may also require precise geographical location data so that they can access the GPS [26]. Also, they contain malware with the aim of spying and accessing user's information such as Riskware, Spyware, Malvertising, and Trojan. These spywares read all text and mail messages, all personal and confidential data, and bank data on the user's device and send them to the hacker [27].

The VPN connection is subjected to a man-in-the-middle attack (MITM) as a result of poor authentication on the part of the client. A client connects to a VPN, which is the link between the user and the VPN, and weak security and authentication processes based on weak client encryption protocols and standards leave the server's identity uncertain, causing exposure to that attack and detecting data sent between the server and the client [22]. Zhang et al. [1] added that these applications leak sensitive data such as users' IP addresses and share it with others. This means that other users use the same

IP address, which poses a danger if one of those users behaves improperly. If that happens, the other user will be exposed to legal accountability.

2) Risks Threatening Operating System Security:

Donovan [14] discusses the malware contained in VPN applications which are designed to destroy operating systems by exploiting their vulnerabilities and diverting traffic from the user's device to a system controlled by the hacker. Ikram et al. [13] indicated that this malware includes riskware which disables the general performance of the user's operating system, adware which displays annoying ads with malicious content, trojan horses that disable operating systems and anti-virus software installed on the device, in addition to ransomware that infiltrates security barriers to completely disable the operating system. Cyware [28] also indicated that another threat is browser hijacking, which controls internet traffic and directs the browser to certain websites without the user's permission [29].

3) Risks Threatening Wireless Networks Security:

Some VPN applications disable network speed as they contain malware such as riskware [13],[30]. Some of these applications steal the users' bandwidth, intending to sell it to other companies to use it as servers and in some cases selling it to governments to exploit users in other issues [31]. Such applications contain permissions requesting access to Wi-Fi network information [26]. They also carry threats called Denial of Service Attacks (DDOS) that may come from a malicious client-side application. Since many smart-phones systems are multi-application systems, the incorrect permission of another application's management interface may allow other applications on the same device to control the VPN connection and to block it and to cause a denial of service attack [1], which affects the lack of immunity of the network that has been controlled and then manipulates and controls it [4].

Some VPN applications execute tunnelling protocols without encryption or use an insecure encryption algorithm and may use opacity instead of encryption, exposing the network to hacking attacks [1]. As discussed above, the idea of a VPN connection is based on the encapsulation of the user's network traffic over the internet to keep it hidden, and the previous factors affect the detection of this connection, which affects the security of the wireless networks.

4) Risks Threatening Hardware Security:

Based on the above, we realize that risks are interrelated and that those related to data and information, operating systems, and wireless networks affect the entire security of devices. Certainly, malware and viruses cause errors, slowdowns, and damage to devices, and controlling internet traffic by hackers and exploiting security vulnerabilities in operating systems all affect hardware resources.

5) Risks Threatening National Security:

Cyberspace has become a domain of warfare in the twenty-first century and has become a major challenge to national security [32]. In this context, security in cyberspace - as it is in the physical world - is a matter of concern to states everywhere. Therefore, cybersecurity is intrinsically linked to national security [33]. In furtherance of the above, we refer to the letter written by Senators Wyden & Rubio [34] addressed to the Director of the Cybersecurity and Infrastructure Security Agency (CISA) in the United States stating the risks of VPNs to national security. The letter shed light on a major flaw in the way in which most VPNs are archived, especially those on smartphones, as VPN providers direct all user traffic through their servers and national security problems arise when the locations of these servers and the companies that run them are located in countries that do not share values and interests with the United States. VPN providers will have access to sensitive government officials' information via these applications, and therefore the national security of the United States will be compromised by the reconciliation of this data. The senators urged the Director of (CISA) to conduct an assessment of VPN threats to national security related to the use of VPN applications by US government employees and provide the powers to block these applications after testing, assessing and confirming the threats they pose to the national security of the United States.

The response of the Director of (CISA) stated that reports indicate that providers of VPN applications can take advantage of users data for malicious purposes, and cited - as evidence of the danger posed by VPN applications - a Russian law issued in November 2017 that allows the Russian government to reach VPN providers

located in Russia. He also cited a warning issued by the Indian government that the Chinese government is using Chinese VPN applications to collect users' data [35]. At this level and within the Kingdom of Saudi Arabia, we realize that national security is the most challenging aspect of cybersecurity, which is related to national security in terms of the use of VPN applications by employees of sensitive sectors that contain important data thus leading to cyber spying on the state. Moreover, the modern concept of cybersecurity is not limited to political aspects only, as it also keeps pace with the threats and challenges that may pose a stumbling block to the state's digital and knowledge economy. Thus, the threats of VPN applications have numerous dimensions: political, cultural, social, and economic.

Based on what has been reviewed in the theoretical frameworks, previous studies, and research, it has become clear that the aforementioned risks affect free software more than paid ones. This should not lead to trusting paid applications, as we realize that as long as there is a third-party intermediary between the user and the internet, it is possible for the company providing the VPN service to keep records of its users, as it is subject to the laws of states. The ideal solution is to establish a private server.

In addition to the above, and to clarify the vision, we point out that VPN connections are more suitable for fixed devices such as computers, because their connection to the network is stable, unlike mobile devices, as they are less reliable because they are prone to losing connectivity while switching from one network to another. For example, a mobile phone may switch between Wi-Fi and 4G, or between one Wi-Fi network and another, and disconnection or connection changes may cause disconnection to the VPN, which leads to frequent application failure and data loss [36].

E. Ethics and Conduct for Using VPN Applications

The emphasis on addressing this aspect comes through the awareness of the capabilities provided by VPN applications for privacy, confidentiality, and censorship circumvention and the abnormal issues that may be involved. These may include, for example, access to the dark web, which is a parallel network to the internet. The dark web is accessed for illegal purposes [37], to visit harmful and prohibited sites that are a danger to moral and intellectual values. Therefore, it is a tool that can harm or benefit the individual and society according to the way they are used and harnessed.

On the other hand, like other technologies, such applications have benefits and ethical uses, including its use by economists for search engine optimization (SEO). This is done by analyzing data from VPN providers who provide statistics for browsing a specific product in a particular state. Therefore, this will help them to study the market and develop new strategies. These applications can also be used to access some sites that are prohibited due to the local conditions of the user, as he may be in a certain state and he needs to access work, university or school websites. The applications also enable users to send very important data without being stolen or spied on and to facilitate communication between branches of companies very effectively and quickly, even with the presence of a wide geographical distance. In addition, they may also be used to follow the expansion of commercial activity [38] and have a range of other uses that do not cause harm to the individual or others. Among the supporting views of this issue is what was presented by Pavlicek & Sudzina [11], which stated that personal and demographic characteristics influence the use of VPNs. They pointed out that some factors such as conscience, openness to experience, gender and field of work have an impact and may control the type of use positively or negatively.

Through the previous review, we note that cyberspace contributes to the escalation of negative conduct, and on the other hand there are many opportunities for the emergence of positive conduct. This overlap between individual privacy, community security, and businesses that benefit from VPN technology requires the presence of a balance in organizing their use in the light of these objectives.

F. Governance of the Use of VPN Applications

The term "Governance" in general is essential to clarify what is meant by the governance of the use of VPN applications. It has been used in a variety of contexts and generally refers to management rather than control. Governance is the level of good performance of the government agency in its broad sense, that is, departments, authorities, ministries, and other government agencies that take decisions, implement policies, oversee the application of laws and legislations and monitor their implementation. Governance should be characterized by

transparency, credibility, and accountability [39]. Since VPN applications involve risks to societal and national cybersecurity, as discussed above, their use must be governed. As such, it is clear that the term most related to the subject of the study is Cybersecurity Governance, which is a framework that aims to manage risks, oversee compliance responsibilities and control, define the cyber mission by mapping the structure, authority and processes, and establish cyber training and awareness programs to present an effective program to reduce the risks associated with cyberspace [3]. This concept shall cover the elements of cybersecurity governance. It must be noted here that states are the enabling factor that provides the legal and organizational framework within which the governance of the use of VPN applications can be planned and implemented.

G. Experiences of States in the Governance of the Use of VPN Applications

In developing the proposed frameworks, it is important to take advantage of global experience in the field. By looking into research outside of Saudi Arabia, especially British and Chinese, through various research tools, no framework for governance of state-level VPN applications has been found. The research has centered on the experiences of different states in dealing with VPN applications.

The legality of VPNs differs from one state to another. Some states have banned their use entirely while others have made it possible under specific controls. We will shed light here on the best practices in managing and organizing this use in Arab and Asian states. Such experiences were chosen due to many considerations, including the similarity of the UAE and the Sultanate of Oman in their environmental conditions to those in the Kingdom of Saudi Arabia, and for Iraq's rationale in managing their use, and the fact that China and Russia are states with cyber sovereignty. In this context, we will review some the experiences various states to benefit from them in building the proposed framework:

1) Governance of the Use of VPN Applications in Arab States:

The Experience of the United Arab Emirates: The UAE regulated the use of VPNs by imposing a penalty exclusively related to their use to commit crimes. It is one of the few states in which there are laws explicitly related to the use of VPNs. Article 9 of the Federal Law of 2012 on combating cybercrimes stipulates that violators "Shall be punished by imprisonment and a fine not less than one hundred and fifty thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever uses a fraudulent computer network protocol address by using a false address or a third-party address by any other means for the purpose of committing a crime or preventing its discovery." [40], since the penalty is related only to the fraud referred to. The UAE Telecommunications Regulatory Authority (TRA) indicated in 2016 that there is no regulation that prevents the VPN technology used by companies, institutions, and banks use to access their internal network via the internet [41].

The Experience of Iraq: Iraq banned the use of VPNs completely in 2014. This means that any attempt to access the home page of the VPN provider or any attempt to initiate a VPN client connection will be terminated by the internet service provider (ISP). As stated, the ban was issued to track down and stop ISIS from manipulating social media platforms [42]. There are currently no penalties in Iraq for violating this system.

The Experience of the Sultanate of Oman: Many efforts were rendered in this regard, but the legal status of the use of VPNs in Oman is still a gray area. The Telecommunications Law in Oman forbids the use of any encryption method without explicit permission from the government in advance, but this law does not have any practical implications because the encryption is an essential aspect of the internet. The Telecommunications Regulatory Authority (TRA) sought public advice in 2010 on draft regulations that would make the use of VPNs illegal for individuals and require organizations to obtain a license from the TRA for commercial use [43]. We could not obtain the advice received by the TRA in this regard. Meanwhile, some sources indicated that the use of VPNs was rationed so that only government-approved VPNs were permitted to be used and that fines were imposed on violators [44]. However, until the date of this study, no document, law, or official news has been made available to confirm this.

2) Governance of the Use of VPN Applications at the Level of Foreign States:

The Experience of China: The use of VPNs was regulated by taking measures to restrict and limit it by various departments. The Ministry of Industry and Information Technology (MIIT) issued regulations limiting the use of VPNs to those permitted (including companies, universities, and research institutions) through authorized business service providers [45]. China prevents the use of these applications to gain access to politically sensitive content, to transfer sensitive data outside the state, or to facilitate capital flight. Therefore, regulations prohibit individuals but permit companies and academic institutions. The Ministry of Public Security (MPS) considers cyber activities as part of its mandate to maintain homeland security, and to this end, it has begun to send notifications to internet service providers to block VPNs. It has requested Apple to remove all unlicensed VPN applications from the Chinese applications store. The leadership in China considers information technology and communications as a critical security risk that should be managed [46]. The law stipulates that it is not permissible to create or rent dedicated lines (including VPNs) and other channels without the consent of the Communications Department to carry out business activities. International leased lines should create user files in a centralized manner, and it is clearly indicated that they are for internal office use only and should not be used to link data centers or business platforms internally and externally to implement telecommunications business operations [47]. In 2016, the regulations defined the possible penalties in light of illegal uses, which are fines of up to 15,000 yuan, equivalent to 2,117 USD. It was clarified that this announcement is a reformulation of the regulations issued by the State Council in 1996 [48]. This means that China has regulated the use of VPNs from an early date as well as continuing to update its regulations.

The Experience of Russia: Russia has regulated the use by only permitting the use of VPNs approved by the government and subject to its supervision. The Russian government passed a law regulating VPNs in 2017 prohibiting VPNs that allow access to websites and networks banned in Russia. This law does not prohibit the use of VPNs, but it requires VPN operators to prevent Russian users from accessing websites and other resources that have been blocked by the Russian authorities. However, this law allows federal security agencies to access VPN servers and their data content. And in cases where the owner does not comply with the law, his network will be blocked. Legal analysts predict that there will soon be an additional regulation to impose fines on VPN owners who refuse to comply with the law [49, 50]. In statements on this ban, the Russian government clarifies that VPNs support illegal content. Russia is following China's approach that anonymous networks such as VPNs are not good, as they allow dissident elements to launch attacks against governments. Fig. 1 summarizes the governance of the use of VPNs in the aforementioned states.

Fig. 1. Governance of the use of (VPN) applications for some states in Asia.

V. The Applied Framework: Analysis and Discussion of the Findings of the Study

In this part, the study addressed the presentation and analysis of data and statistical methods used and discussed the findings by analyzing the questionnaire tool to achieve the objectives of the study. The questionnaire consisted of two parts. The first addressed general data with 7 questions, while the second consisted of 34 questions asked through 4 axes: They were as follows: Measuring the perceptions of the concept of VPN applications, measuring the knowledge of cybersecurity means for smartphones when using VPN applications, the attitudes towards the use of VPN applications, and lastly measuring the knowledge of cybersecurity risks of VPN applications. The questionnaire was sent to the study sample using social media platforms (Twitter, WhatsApp, Instagram, LinkedIn, Telegram, and Snapchat). 462 responses were obtained and then were filtered to 455 questionnaires valid for analysis. The evaluation of the items with closed answers relied on a three-point

TABLE I
DISTRIBUTION OF STUDY SAMPLE INDIVIDUALS ACCORDING TO THE VARIABLE OF GENERAL DATA

Categorical Variables and their Coding	Frequency	Percentage %
Gender	**455/455**	**100**
1=Male	255	56.0
2=Female	200	44.0
Age in Years	**455/455**	**100**
1= from 10 to 19	73	16.0
2= from 20 to 29	181	39.8
3= from 30 to 39	133	29.2
4= from 40 to 49	46	10.1
5= 50 years and above	22	4.8
Academic Qualification	**455/455**	**100**
1= Undergraduate	167	36.7
2= Bachelor	204	44.8
3= Master	63	13.8
4= PhD.	21	4.6

[a] *Note: The categories of primary, intermediate, and secondary were merged due to the limited number of frequencies in one category, namely "Undergraduate"*

Likert scale, giving a score of 1 for (Disagree), 2 for (Neutral), and 3 for (Agree).

VI. RESULTS

A. Findings Related to the Description of the Study Sample Individuals

Table I shows a description of the study sample individuals, which is related to general data. It was noticed that the number of male respondents exceeded the number of females, and most of the respondents were aged between 20 and 39 years old with a percentage of 69% of the total study sample representing the youth. This is probably because the youth constitute most users of the internet and therefore most users of VPN applications. Whereas the percentage of bachelor's degree holders was approximately 45%, representing the highest percentage of total respondents. Undergraduates and were approximately 37%, and then holders of master's degrees were approximately 14%, while PhD holders formed the lowest percentage.

To determine the prevalence of the use of VPN applications at the sectoral level, the study sample was asked to determine the job category to which they belong. Fig. 2 shows the diversity of the job categories that use VPN applications with the increasing demand by students.

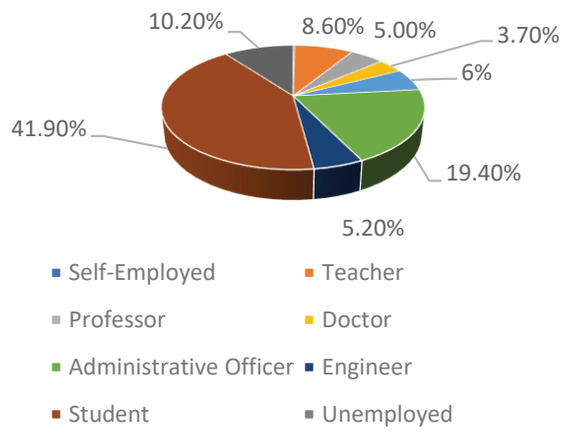


Fig. 2. Percentage of the study sample individuals according to the variable of job category

To recognize the extent of the study sample individuals' exposure to the risks of VPN applications, questions were asked regarding the type of operating systems and VPN applications used. It became clear that there is a con-

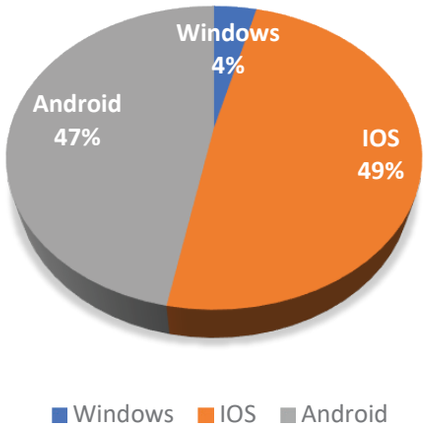


Fig. 3. Percentage of use of the study sample individuals of (VPN) applications according to the variable of operation system type

Fig. 4. Percentage of use of the study sample individuals of (VPN) applications according to the variable of application type

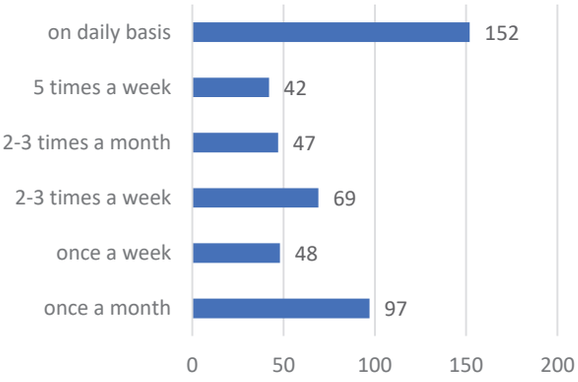


Fig. 5. Distribution of the study sample individuals according to the variable of times of use of (VPN) applications

vergence in the ratio between (IOS) and (Android) users. As for the use of free applications, it significantly exceeded the paid ones, as in Fig. 3 and 4. From this, it is evident that there is a large percentage exposed to the risks of VPN applications, due to their use of Android systems in addition to the use of free VPN applications, and this is also the conclusion [1, 13] and [14] have come to.

The study asked a question that tracks the frequency of use of the study sample individuals of VPN applications to indicate the degree of use. It was found that there is a permanent use for the majority of the study sample individuals, and it is represented in daily use. Fig. 5 illustrates the variation in the use of VPN applications among the study sample individuals with the tendency of the majority towards daily use.

B. Findings Related to the Questions of the Study

In this part, the main axes of the study were evaluated using descriptive statistical methods in analyzing the findings of the field study to describe the views of the study sample individuals from the Saudi society using VPN applications on smartphones towards the questionnaire questions, by displaying the frequencies and percentages and calculating the arithmetic mean the standard deviation and ranks of the responses of the study sample individuals on the terms of each axis. Then the weighted arithmetic mean was calculated to evaluate each axis of the main study axes separately and to measure the consistency of the answers through the standard deviation. The scores were expressed by relying on the three-point Likert scale. The weighted arithmetic mean was evaluated by first calculating the length of the period, which is a sum of 2/3, where 2 represents the number of distances from 1 to 2 as first distance, and from 2 to 3 as second distance, and 3 represents the number of choices. Dividing 2 by 3 results in the length of the period equal to 0.67 to be added to the beginning of each period, and so on until the evaluation of the arithmetic mean according to the periods from 1 to less than 1.67 for (Disagree), and from 1.67 to less than 2.34 for (Neutral), and from 2.34 to 3 for (Agree).

Through Table II, the second objective of the study was achieved, which included identifying the perceptions of the members of the Saudi society of the concept of Virtual Private Network VPN applications.

The results in Table II showed that most of the study sample individuals agree with the statements related to

TABLE II
RESPONSES OF THE STUDY SAMPLE INDIVIDUALS ON THE STATEMENTS OF PERCEPTIONS MEASURING REGARDING (VPN) APPLICATIONS CONCEPT

First Axis	Frequency	Degree of Agreement			Standard Deviation	Arithmetic Mean	Ranks
Statements	Percentage	Agree 3	Neutral 2	Disagree 1			
1. Network that can be connected remotely	455 100%	242 53.2%	171 37.6%	42 9.2%	.66	2.44	4
2. Applications to encrypt internet connection	455 100%	288 63.3%	133 29.2%	34 7.5%	.63	2.56	1
3. Applications for digital anonymity	455 100%	282 62.0%	127 27.9%	46 10.1%	.67	2.52	2
4. Applications for internet censorship circumvention	455 100%	285 62.6%	121 26.6%	49 10.8%	.68	2.52	2
5. Tool to secure internet connection	455 100%	224 49.2%	186 40.9%	45 9.9%	.66	2.39	5
6. Applications for information privacy and security	455 100%	265 58.2%	134 29.5%	56 12.3%	.70	2.46	3
Weighted Arithmetic Mean		**Agree**			**.42**	**2.48**	

the concept of VPN applications. This is through the result of the weighted arithmetic mean of the first major axis (2.48), which indicated a degree of (Agree), and the standard deviation indicates the presence of consistency in the approval of the sample individuals regarding the concept of VPN applications.

It is evident from the above results that the perceptions of the sample individuals of the concept of VPN applications are not exactly clear, as the percentage of their choice of the concept of "digital anonymity" was ranked in second place with a percentage of (62.0%) which are applications that do not conceal their identity as is common, because the VPN connection encrypts the data that it holds to keep it safe and protects it from spying and hacking, and does not provide any anonymity that includes the user's ability to remain anonymous on the network or system since there are other tools for this purpose. On the other hand, it is clear that their perceptions about its concept as a "tool to secure internet connection" was ranked last, although it is an effective tool for that as it was created for this purpose. This result is explained by the fact that there is a confusion in the perceptions of the study sample individuals between the actual concept of VPN applications and the common concept among its users which is not correct, which leads to risks affecting cybersecurity.

Table III achieves the third objective of the study, which includes identifying the extent to which the members of the Saudi society are aware of the means of cybersecurity for smartphones when using VPN applications.

The results in Table III showed that the knowledge of the study sample individuals of the cybersecurity means for smartphones when using VPN applications was neutral. This is due to the result of the weighted arithmetic mean of the second axis 2.05, which indicated a degree of (Neutral), and the standard deviation indicates consistency in the neutrality of the study sample individuals on the knowledge of cybersecurity means for smartphones when using VPN applications.

It is evident from the results above that the majority of the study sample individuals did not use the most important means of cybersecurity when using VPN applications. The essential means were ranked last despite their importance, such as reviewing the laws of the state to which these applications belong to before using them (by 21.8%), and reviewing the locations of VPN servers and their funding sources, as some of them may be funded by states that do not share interests with the states of their users. This is in addition to reading their privacy policies, which represents a basic aspect because some of them follow weak privacy policies or may not contain privacy policies at all. Moreover, it was clear that a small

TABLE III

RESPONSES OF THE STUDY SAMPLE INDIVIDUALS ON THE AXIS OF KNOWLEDGE MEASUREMENT OF CYBERSECURITY MEANS FOR SMARTPHONES WHEN USING (VPN) APPLICATIONS

First Axis	Frequency	Degree of Agreement			Standard Deviation	Arithmetic Mean	Ranks
Statements	Percentage	Agree 3	Neutral 2	Disagree 1			
7. I update the operating system (Android-Windows-iOS) frequently	455 100%	324 71.2%	107 23.5%	24 5.3%	.58	2.66	1
8. I download the anti-virus "Android users" and update it frequently	454 100%	170 37.4%	183 40.3%	101 22.2%	.76	2.15	3
9. I refer to reviews and ratings of (VPN) applications before downloading	455 100%	160 35.2%	186 40.9%	109 24.0%	.76	2.11	4
10. I review the owner's information of (VPN) applications	455 100%	107 23.5%	226 49.7%	122 26.8%	.71	1.97	6
11. I review the funding sources of (VPN) applications	455 100%	84 18.5%	219 48.1%	152 33.4%	.71	1.85	10
12. I review the information of the State to which the (VPN) applications belong	455 100%	89 19.6%	214 47.0%	152 33.4%	.72	1.86	9
13. I review the laws governing information privacy in the State to which the (VPN) applications belong	455 100%	99 21.8%	200 44.0%	156 34.3%	.74	1.87	8
14. I review the information about the locations of the (VPN) application servers	455 100%	101 22.2%	213 46.8%	141 31.0%	.72	1.91	7
15. I review the encryption standard that (VPN) applications follow	455 100%	74 16.3%	215 47.3%	166 36.5%	.70	1.80	11
16. I install (VPN) applications from a trusted developer and the official store (App Store, Google Play)	455 100%	259 56.9%	143 31.4%	53 11.6%	.69	2.45	2
17. I review the permissions requested by (VPN) applications	455 100%	144 31.6%	198 43.5%	113 24.8%	.75	2.07	5
18. I read the privacy policies followed by (VPN) applications	455 100%	108 23.7%	176 38.7%	171 37.6%	.77	1.86	9
Weighted Arithmetic Mean		**Neutral**			**.48**	**2.05**	

percentage of the study sample individuals (16.3%) usually review the used encryption standards, even though it is a basic point when starting to use these applications. This result is explained by the lack of knowledge of the majority of the study sample individuals of cybersecurity means when using VPN applications, which leads to the use of these applications without following security measures and thus poses risks to security in the cyberspace.

The fourth objective of the study, which includes identifying the attitudes of the members of the Saudi society towards using VPN applications, is shown in Table IV.

Indeed, Table IV reviews the motives for using VPN applications, in which the weighted arithmetic mean of the third main axis (2.27) indicated the neutrality of the study population motives for using VPN applications. The standard deviation indicates that there is consistency in the neutrality of the study sample individuals on the motives for using VPN applications.

It is noticeable that the degree of agreement of the study sample individuals (62.9%) focuses on the use of VPN applications as the highest priority to access entertainment content such as electronic games and watching Netflix content. This was followed by maintaining ano-

TABLE IV

RESPONSES OF THE STUDY SAMPLE INDIVIDUALS ON THE AXIS OF ATTITUDES OF USING (VPN) APPLICATIONS

First Axis	Frequency	Degree of Agreement			Standard Deviation	Arithmetic Mean	Ranks
Statements	Percentage %	Agree 3	Neutral 2	Disagree 1			
19. I use (VPN) applications to access entertainment content (e-games, Netflix)	455 100.0	286 62.9%	113 24.8%	56 12.3%	.71	2.51	1
20. I use (VPN) applications to access social media networks or news services	455 100.0	230 50.5%	134 29.5%	91 20.0%	.78	2.31	3
21. I use (VPN) applications to maintain anonymity while browsing the internet	455 100.0	258 56.7%	122 26.8%	75 16.5%	.76	2.40	2
22. I use (VPN) applications to access websites or files or services at work	455 100.0	210 46.2%	138 30.3%	107 23.5%	.80	2.23	5
23. I use (VPN) applications to access restricted download websites	455 100.0	203 44.6%	136 29.9%	116 25.5%	.82	2.19	6
24. I use (VPN) applications to communicate with friends or family abroad	455 100.0	212 46.6%	150 33.0%	93 20.4%	.78	2.26	4
25. I use (VPN) applications for protection when using public Wi-Fi	455 100	146 36.0%	207 45.5%	84 18.5%	.72	2.18	7
26. I use (VPN) applications to avoid price discrimination in online stores and flight booking tickets based on my geographical location	455 100	141 31.0%	214 47.0%	100 22.0%	.72	2.09	8
Weighted Arithmetic Mean		**Neutral**			**.46**	**2.27**	

nymity while browsing the internet, and then for accessing social media networks and news services (50.5%). The percentage converged between their use of these applications for communicating with friends or family abroad and accessing sites at work or school and to access banned download sites. The use of VPN applications decreased due to securing the internet connection when using public Wi-Fi networks, and to prevent price discrimination in electronic stores and booking airline tickets based on geographical location by (36.0%) and (31.0%), respectively, with a clear difference from other percentages, although it is good and distinctive uses.

Other reasons mentioned by participants included choices most of which fall in the classification of entertainment and amusement, such as blocking ads in applications and e-games, watching movies with prohibited content, and a choice that leads to work which is using them for work purposes and accessing the system and resources of the enterprise remotely.

From the previous review, it is clear that the motives for using VPN applications varied, but most of them were in the area of entertainment. It is noted that some uses in this area may carry moral and intellectual risks, and on the other hand only a minority of the participants who are using it for fruitful and beneficial aims. The results can be linked to what was previously reviewed in the frequency of the use of VPN applications, where daily use constituted the largest percentage of the study sample individuals, in addition to the high percentage of use among the youth. This confirms that the most likely trend in use is for entertainment.

Through Table V, the fifth objective of the study was achieved, which includes identifying the extent of knowledge of the members of the Saudi society of the cyber risks of VPN applications.

TABLE V
RESPONSES OF THE STUDY SAMPLE INDIVIDUALS ON THE AXIS OF MEASUREMENT OF KNOWLEDGE ON THE CYBER RISKS OF (VPN) APPLICATIONS

First Axis	Frequency	Degree of Agreement			Standard Deviation	Arithmetic Mean	Ranks
Statements	**Percentage %**	**Agree 3**	**Neutral 2**	**Disagree 1**			
27. Hackers and computer thieves can decrypt (VPN) connection	455 100.0	187 41.1%	216 47.5%	52 11.4%	.66	2.30	1
28. (VPN) applications require access rights to sensitive resources such as user accounts	455 100.0	114 25.1%	275 60.4%	66 14.5%	.62	2.11	4
29. (VPN) applications contain malware that affects the security of the operating system	455 100.0	132 29.0%	262 57.6%	61 13.4%	.63	2.16	3
30. (VPN) applications collect users' personal information and sell them to external partners	455 100.0	113 24.8%	262 57.6%	80 17.6%	.65	2.07	5
31. (VPN) applications track the location of the device by accessing the GPS of the user's device	455 100.0	139 30.5%	265 58.2%	51 11.2%	.62	2.19	2
32. (VPN) applications allow sharing the IP address given by the application with other users	455 100.0	122 26.8%	282 62.0%	51 11.2%	.60	2.16	3
33. (VPN) applications direct the browser to websites without your permission	455 100	98 21.5%	272 59.8%	85 18.7%	.63	2.03	6
34. (VPN) applications steal the bandwidth and resell it	455 100	93 20.4%	280 61.5%	82 18.0%	.62	2.02	7
Weighted Arithmetic Mean		**Neutral**			**.45**	**2.13**	

The results in Table V show that the knowledge of VPN applications risks to cybersecurity was neutral, based on the result of the weighted arithmetic mean of the fourth main axis (2.13) which indicated (Neutral) degree. The standard deviation indicates that there is consistency in the neutrality of the study sample individuals regarding the knowledge of VPN applications risks to cybersecurity.

It is evident from the above that the majority of the study sample individuals tended to be neutral, and some of them agreed on VPN applications risks, as 41.1% of the total study sample individuals agreed on the phrase that hackers can decrypt VPN connection, followed by close rates that these applications can access the GPS of the user's device and that they include malware that affects the security of operating systems. Moreover, they request access rights to sensitive resources and collect personal user information and sell them to external partners also in very close proportions. Agreement that they steal bandwidth came last by 20.4%. It is now clear that the study sample individuals have some knowledge of VPN application risks to cybersecurity. This is related to the result of Table III, which indicated that most of the study sample individuals did not use and know the means of cybersecurity when using VPN applications, and this is due to a lack of integrated perception of their risks.

C. The Significant Differences between the Arithmetic Means of the Study Axes according to General Data

In this part, inferential statistic methods were used to determine the significant differences between the arithmetic means of the study axes according to general data and to study the relationships between the main axes of the study and some general data and data related to the

TABLE VI
DIFFERENCES IN THE RESPONSES OF THE STUDY SAMPLE INDIVIDUALS ACCORDING TO THE VARIABLE OF GENDER

Axis	Statistical Significance Level for T-Test	Degrees of Freedom	Critical T Value	Application Type	Standard Deviation	Arithmetic Mean	Number
Perceptions of (VPN) applications concept	.000 (HS) [a]	385.551	20357.50	Male	248.17	2.55	255
				Female	202.29	2.39	200
Knowledge of cybersecurity means when using (VPN) applications	.912 (NS)	379.599	25346.50	Male	227.40	2.05	255
				Female	228.77	2.04	200
Knowledge of (VPN) application risks on cybersecurity	.437 (NS)	395.845	24442.00	Male	223.85	2.11	255
				Female	233.29	2.15	200
Axis	**Statistical Significance Level for T-Test**	**Degrees of Freedom**	**Critical T Value**	**Application Type**	**Standard Deviation**	**Arithmetic Mean**	**Number**
Attitudes of using (VPN) applications	.005 (SS) [b]	453	2.816	Male	274.07	2.32	255
				Female	243.60	2.20	200

[a] *there is a statistically significant relationship at significance level = 0.01,*
[b] *there is a statistically significant relationship at significance level = 0.05*

use of VPN applications. Several tests were used in proportion to each variable as follows:

1) Differences According to the Variable of Gender:

To study the presence of a significant difference in the axes of the study according to the difference in general data on the use of the application (gender, type of application), t-test was used, which is one of the parametric tests for the two independent samples when the consistency of the data of the two groups is achieved by the Levene's test. When the consistency was not achieved, the non-parametric Mann–Whitney U test was used to study the differences between the opinions of the males and females in the two groups, as in Table VI.

It is evident through the previous results that there are statistically significant differences at a significance level of 0.01 for the perceptions of the concept of VPN applications according to the variable of gender. And it was also observed that the average perceptions are higher among males than females. As for the attitudes, they differed at a significance level of 0.01 and were higher among males than females. Since perceptions among males are higher, then the vision is unclear about the concepts of VPN applications and what they offer. Thus, motivations and attitudes of this section are increasing. As for the knowledge of cybersecurity means for smartphones and knowledge of VPN application risks to cybersecurity, there were no differences in their evaluation between males to females.

2) Differences According to the Variable of Application Type:

It is evident from Table VII that there are statistically significant differences at a significance level of 0.01 in the knowledge of cybersecurity means for smartphones among users of free and paid applications, as it was higher for users of paid applications. As for the rest of the variables, there were no differences between them according to the type of application. This is since paid applications are of a higher security level, therefore it is more likely that those with knowledge of cybersecurity will use them.

3) Differences According to the Variable of Academic Qualification:

The presence of a significant difference in the study axes according to the variable of academic qualification was tested by using the Analysis of Variance (ANOVA), as long as it was classified for more than two groups. After confirming the non-consistency of the data with the Levene's test, the Kruskal-Wallis test was used. The re-

TABLE VII
DIFFERENCES BETWEEN THE RESPONSES OF THE STUDY SAMPLE INDIVIDUALS ACCORDING TO THE VARIABLE OF APPLICATION TYPE

Axis	Statistical Significance Level for T-Test	Degrees of Freedom	Critical T Value	Application Type	Standard Deviation	Arithmetic Mean	Number
Perceptions of (VPN) applications concept	.609 (NS)	453	.512	Free	.416	2.48	416
				Paid	.413	2.45	39
Knowledge of cybersecurity means when using (VPN) applications	.000 (HS) [a]	453	-3.975	Free	.475	2.02	416
				Paid	.409	2.33	39
Attitudes of using (VPN) applications	.437 (NS)	453	-.941	Free	.467	2.26	416
				Paid	.415	2.34	39
(VPN) application risks on cybersecurity	.163 (NS)	453	-1.398	Free	.455	2.12	416
				Paid	.444	2.22	39

[a] *there is a statistically significant relationship at significance level = 0.01*

sults are shown in Table VIII.

Table VIII indicates that there are no statistical differences at significance level of 0.05 for knowledge of VPN application risks to cybersecurity and the knowledge of cybersecurity means for smartphones when using VPN applications, according to the variable of academic qualification. This is due to a deficiency in addressing the security and risks of VPN technology in curriculums, as well as a general lack of awareness in the educational sectors.

As shown in Table X, perceptions differed significantly between bachelor and below, as well as between undergraduates and master, as it was higher for undergraduates. Therefore, it is evident that the confusion in perceptions was higher among the categories of undergraduates in the "elementary, secondary, and primary" stages. This is because education in these stages focuses on aspects other than technology, and thus the vision is unclear in these stages. This is in addition to weak self-awareness and self-education. Therefore, such applications are used without awareness of their risks.

Also, the attitudes towards the use of VPN have differed according to the variable of academic qualification, as shown in Table XI between undergraduate and master, and between bachelor and master; the attitudes of use were less among master. This may be attributed to the high awareness of these applications, so they are used in a minimalistic manner in this category.

C. The Relationship between the Main Axes of the Study and the General Data of the Study Sample

The relationship between the axes of the study and the two variables (age and frequency of use) was tested using Spearman's coefficient to study the correlation among categorical variables, which explains the strength and direction of the correlation for the relationship.

The results in Table XII indicated the presence of a weak inverse correlation between age and perceptions at a significance level of 0.01; the greater the age the less the perceptions of VPN applications. This result explains that as age increases the perception that VPN applications do not actually achieve all the concepts increases, and so the perceptions have decreased. Moreover, it also indicated the presence of a very weak direct correlation between the frequency of use and both the knowledge of cybersecurity means for smartphones when using VPN applications and attitudes of use at a significance level of 0.01. So the more the knowledge of cybersecurity means for smartphones when using VPN applications and attitudes in VPN application use increases the more the frequency of use increases.

VII. DISCUSSION OF THE FINDINGS

As per the findings previously explained, we discovered the following:

- The use of VPN applications is centered among the youth between 20 and 39 years old.
- The use of VPN applications is widespread among

TABLE VIII
DIFFERENCES IN THE RESPONSES OF THE STUDY SAMPLE INDIVIDUALS ACCORDING TO THE VARIABLE OF ACADEMIC QUALIFICATION

Axis	Statistical Significance Level for Kruskal-Wallis Test	Degrees of Freedom	Chi-Squared Critical Value	Academic Qualification	Arithmetic Mean Grade	Arithmetic Mean	Number
Perceptions on the concept of (VPN) applications	0.00 (HS**)	3	19.758	Undergraduate	261.53	2.59	167
				Bachelor	215.86	2.44	204
				Master	190.08	2.34	63
				PhD.	193.10	2.39	21
Knowledge of (VPN) applications risks on cybersecurity	(NS)	3	1.243	Undergraduate	219.99	2.12	167
				Bachelor	230.38	2.13	204
				Master	238.42	2.13	63
				PhD.	237.36	2.18	21
Axis	**Statistical Significance Level for Kruskal-Wallis Test**	**Degrees of Freedom**	**Chi-Squared Critical Value**	**Academic Qualification**	**Arithmetic Mean Grade**	**Arithmetic Mean**	**Number**
Knowledge of cybersecurity means when using (VPN) applications	0.61 (NS)	3	2.474	Undergraduate	.460	2.10	167
				Bachelor	.480	2.04	204
				Master	.514	1.91	63
				PhD.	.426	2.08	21
Attitudes of using (VPN) applications	.000 (HS) [a]	3	10.396	Undergraduate	.446	2.38	167
				Bachelor	.454	2.26	204
				Master	.417	2.01	63
				PhD.	.524	2.28	21

[a] *there is a statistically significant relationship at significance level = 0.01*

employees of different sectors, with the increasing demand from students.

- The study found that a large percentage of the study sample individuals tend to use free VPN applications. In addition to that, nearly half of the sample used smart phones with the Android system. Therefore, they are exposed to the risks of VPN applications. This agrees with the findings of previous studies [1],[13] and [14].
- The results showed that the majority of the study sample individuals always use VPN applications, represented by daily use.
- The study showed that the perception of the study sample individuals of the concept of VPN applications is not exactly clear, as there is confusion between the actual concept and the common incorrect concept among users.
- The study found that the majority of the study sample individuals did not use the most important cyber protection means when using VPN applications, which is an indication of the lack of knowledge of such means, which leads to the use of these applications without following security actions and thus poses risks to cybersecurity.
- The study revealed a diversity in the motivations of the study sample individuals to use VPN applications, most of which are focused on entertainment. And on the other hand, a minority tended to use these applications for beneficial uses.
- The results also showed that less than half of the study sample individuals agreed that VPN applications imply risks. Thus, it is evident that there is knowledge, to some extent, of VPN application risks to cybersecurity.

TABLE X
RESULTS OF DIFFERENCES IN PERCEPTIONS ACCORDING TO THE VARIABLE OF ACADEMIC QUALIFICATION

Academic Qualification (I)	Academic Qualification (J)	Difference between Arithmetic Means (I-J)	Statistical Significance Level for Dunnett T3 Test
Undergraduate	Bachelor	.14538*	.002
	Master	.24591*	.002
	PhD.	.20093	.223
Bachelor	Undergraduate	-.14538*	.002
	Master	.10053	.561
	PhD.	.05556	.991
Master	Undergraduate	-.24591*	.002
	Bachelor	-.10053	.561
	PhD.	-.04497	.999
PhD.	Undergraduate	-.20093	.223
	Bachelor	-.05556	.991
	Master	.04497	.999

TABLE XI
RESULTS OF THE DIFFERENCE IN ATTITUDES ACCORDING TO THE VARIABLE OF ACADEMIC QUALIFICATION

Academic Qualification (I)	Academic Qualification (J)	Difference between Arithmetic Means (I-J)	Statistical Significance Level for TKI Test
Undergraduate	Bachelor	.11363	.074
	Master	.37054*	.000
	PhD.	.09674	.789
Bachelor	Undergraduate	-.11363	.074
	Master	.25692*	.000
	PhD.	-.01689	.998
Master	Undergraduate	-.37054*	.000
	Bachelor	-.25692*	.000
	PhD.	-.27381	.075
PhD.	Undergraduate	-.09674	.789
	Bachelor	.01689	.998
	Master	.27381	.075

- The high percentage of the youth using VPN applications, and their daily use, confirm that the motives of use are directed towards entertainment.
- Most of the study sample individuals do not use cybersecurity means and are not aware of such means when using VPN applications. This confirms that they lack awareness of their risks.

A. Results of Statistical Indicators

1. There are statistically significant differences at the significance level of (0.01) for the perceptions of the concept of VPN applications according to the variable of gender, where the arithmetic mean of perceptions is higher for males than for females. Since male perceptions are higher, their perceptions are unclear about the concept of VPN applications and what they offer. Accordingly, their motivations and attitudes towards using and adopting them increase.
2. Motivations for using VPN applications differed according to the variable of gender and were higher for males than females. This is in line with

TABLE XII

THE RELATION BETWEEN THE AXES OF THE STUDY AND THE VARIABLES OF AGE AND FREQUENCY OF USE

Cyber-security Risks	Attitudes of Use	Knowledge of Cyber-security Means	Perceptions of Concept	Frequency of Use	Age	Correlation Coefficient	Variable
-.002	-.061	.074	-.321 [b]	-.117 [a]	1.000	Spearman's Coefficient	Age
.966	.191	.115	.000	.013	.	Correlation Significance	
-.022	.199 [b]	.126 [b]	.11 4[a]	1.000	-.117 [a]	Spearman's Coefficient	Frequency of Use of (VPN) Applications
.634	.000	.007	.015	.	.013	Correlation Significance	
.117 [a]	.414 [b]	.028	1.000	.114 [a]	-.321 [b]	Spearman's Coefficient	Perceptions of (VPN) Applications Concept
.012	.000	.546	.	.015	.000	Correlation Significance	
.139 [b]	.275 [b]	1.000	.028	.126 [b]	.074	Spearman's Coefficient	Knowledge of Cyberse-curity Means when Using (VPN) Applications
.003	.000	.	.546	.007	.115	Correlation Significance	
.228 [b]	1.000	.275 [b]	.414 [b]	.199 [b]	-.061	Spearman's Coefficient	Attitudes of Use of (VPN) Applications
.000	.	.000	.000	.000	.191	Correlation Significance	
1.000	.228 [b]	.139 [b]	.117[a]	-.022	-.022	Spearman's Coefficient	(VPN) Applications Risks on Cybersecurity
.	.000	.003	.012	.634	.966	Correlation Significance	

[a] *there is a statistically significant relationship at significance level = 0.05,* [b] *there is a statistically significant relationship at significance level = 0.01.*

the study of Pavlicek and Sudzina [11] which found that males have more motivation towards using VPNs. This is explained by their incomplete vision about the concept of VPN applications and what they offer.

3. The knowledge of cybersecurity means for smartphones when using VPN applications and the knowledge of cybersecurity risks of VPN applications showed no difference in their evaluation between males compared to females.
4. There are statistically significant differences at a significance level of (0.01) in the knowledge of the cybersecurity means for smartphones among users of free and paid VPN applications, as they were higher for users of paid applications because these applications are the most secure. As for the rest of the variables, there were no differences between them according to the type of application.
5. There are no statistically significant differences at a significance level of (0.05) for the knowledge of cybersecurity risks for VPN applications and the knowledge of cybersecurity means for smartphones according to the variable of academic qualification. This may be attributed to a deficiency in addressing the security and risks of VPN technology in school curricula, as well as a lack of awareness in the educational sectors.
6. Perceptions differed according to the variable of academic qualification, between undergraduate and bachelor, as well as between undergraduate and master as it was higher for undergraduates. This is because education in these stages focuses on aspects other than technology, so the vision is unclear in these stages. It is also due to lack of

awareness and self-education. Therefore such applications are used without awareness and consideration of their risks.

7. The attitudes towards the use of VPN applications also differed according to the variable of academic qualification, between undergraduate and master, and between bachelor and master, as the use attitudes were less among masters. This may be attributed to the high level of awareness of VPN applications in this category, as they are used in a minimalistic manner.
8. There is a weak inverse correlation between age and perceptions, at a significance level of (0.01); the greater the age the less the perceptions of the concept of VPN applications. This is an indication that the greater the age the higher the perception that VPN applications do not achieve all services. Therefore, perceptions about these applications decreased.
9. There is a very weak positive correlation between frequency of use and both knowledge of cybersecurity means for smart phones when using VPN applications and attitudes of the use of VPN applications at a significance level of (0.01). The greater the knowledge of cybersecurity means and attitudes of use of VPN applications the greater the frequency of use.

B. Recommendations

1. Communications and Information Technology Commission (CITC) in the Kingdom of Saudi Arabia should modernize the regulations related to information technology and communications in line with VPN applications.
2. It is imperative to consider awareness, in general, to be directed to all segments of society by various means that are compatible with different age stages and educational qualifications. Moreover, it is necessary to focus on awareness directed to students and employees in government sectors such as education and other sensitive sectors.
3. It is necessary to add courses related to cybersecurity that address the security and risks of VPN technology and the ethics of their use at all educational stages.
4. The use of VPN applications should be regulated and controlled, and the scope and powers of use should be defined.
5. It is of great importance to conduct a risk assessment for VPN applications available on Saudi smart phone stores and to block those containing vulnerabilities and malware.

VIII. Outcomes of the Study

A. Proposed Framework for the Governance of the Use of VPN Applications in the Kingdom of Saudi Arabia

The Anti-Cyber Crime Law (2007) issued by the CITC aims to help achieve information security, preserve the rights arising from the legitimate use of computers and information networks, protect the public interest, ethics and public morals, and protect the national economy [51]. This framework falls within the set of objectives affirmed by the Anti-Cyber Crime Law which seek in their entirety to regulate the use of the internet and related aspects, which is known as internet governance. Based on the results obtained about the attitudes of the members of the Saudi society towards using VPN applications and the current state of the Anti-Cyber Crime Law, in addition to benefiting from the best practices of states in regulating and managing the use of VPN applications, we propose a framework for the governance of the use of VPN applications. The axes of this framework shall be as follows:

B. Importance of the Proposed Framework

The governance of the use of VPN applications plays an important role in achieving the objective of managing national and community cybersecurity. The current governance framework seeks to develop the issue to update the current security policies and regulations in line with these applications, implement some organizational controls and procedures related to restricting the scope of their use and managing their powers of use, conduct continuous review and evaluation processes to proactively manage their risks, and raise awareness in the society about their correct use to encourage positive behaviour.

C. Justifications for the Proposed Framework

Given the wide use of VPN application technology, cybersecurity measures should be modernized to keep

pace with this issue. The perspective of the framework is to address the risks of their use on cybersecurity that were previously reviewed in the theoretical framework. We seek to form an appropriate governance framework. This is due to the unorganized use of VPN applications by the majority of their users among members of the Saudi society, a lack of integrated awareness of their risks, the minority of those who use appropriate cybersecurity means when dealing with them, and their widespread use at the level of individuals belonging to different sectors as shown by the results of the study. This is in addition to the absence of regulations to control their use in the Kingdom of Saudi Arabia, as evidenced by examining the Anti-Cyber Crime Law.

D. Objectives of the Proposed Framework

1. To develop a guiding plan to organize and manage the use of VPN applications in the Kingdom of Saudi Arabia.
2. To establish a conviction for the need to control the use of VPN applications in anticipation of their risks.
3. To emphasize the importance of imposing a law explicitly related to the use of VPN applications, in addition to policies and procedures that go in the same direction.
4. To place emphasis on the necessity to determine the scope of use of VPN applications in their positive form by the concerned authority, whether at the level of individuals, institutions, or businesses.
5. To limit the negative use of VPN applications that affect societal and national cybersecurity by members of the Saudi society and employees belonging to particularly sensitive sectors.

E. Dimensions of the Proposed Framework

The governance of this type of complex networks that carry hybrid threats - mixing traditional and non-traditional methods in an adaptive way to achieve objectives - is a multi-faceted task. Therefore, the proposed framework, Fig3, will consist of three dimensions that complement each other and include the elements of governance of the use of VPN applications distributed according to their relation to each dimension. This is namely to demonstrate the importance of structuring procedures and defining responsibilities to reduce overlapping powers and to activate the follow-up and monitoring processes to manage their use. These dimensions were formed on the basis of the concept and elements of cybersecurity governance. They will be as follows:

1) The Legal Dimension:

Law plays a central role in governance, and it is an essential characteristic of governance called "accountability" which requires activating the role of laws in prosecuting anyone who commits error. The legal dimension is formed in the element of governance through regulations, as they are among the strict methods that control the use of VPN applications by imposing penalties exclusively related to illegal use, such as IP address spoofing by using a virtual, fictitious, or dependent address of others, to commit an offence, crime or access illegal content prohibited by the CITC, or causing harm in one way or another. This requires specifying an article in the Anti-Cyber Crime Law that clarifies the illegal use and the penalties applied in this respect, which will lead to achieving safety and balance in use and to preserve rights arising from use that may harm others. The legal dimension is the structure within which the rest of the dimensions interact with flexibility and a clear method that achieves the main objective, which is the governance of the use of VPN applications.

2) The Organizational Dimension:

The organizational process and procedural measures are necessary for the proper implementation of any type of plan. This dimension explains the necessity of having an organizational plan for laying down a framework for the use of VPNs, which includes continuous assessment of security risks and vulnerabilities and defining them to control and block those containing vulnerabilities and malware, and to develop policies that define the scope and management of powers for the use of VPN applications at the level of individuals and employees of institutions and sensitive sectors. Such a plan should include a series of guidelines that layout procedures to assist in making decisions about use management processes, considering that they should be announced and published to reach stakeholders. This is in addition to monitoring the application of policies to reach the objective, which is to comply with the law that controls the use of VPN applications. The development of policies is the core of the governance framework, as cybersecurity technology

alone is not sufficient to achieve security without policies and continuous update according to developments resulting from continuous risk assessment. Moreover, procedures should be developed, and human-centred control processes should be activated to manage cybersecurity as required.

3) The Awareness-related Dimension:

Awareness is considered the first line of defence and the decisive factor for the prevention against the risks of VPN applications on cybersecurity, since the human factor represents the weakest link in the chain of combating cyber risks. Therefore, concerted efforts are required to adopt and activate awareness initiatives with sustainable impact, in order to clarify the risks resulting from the use of the applications under study, provided that these programs are multi-level and adapted to all groups of different academic degrees and educational levels.

The role of the communications and information technology sector comes primarily in raising public awareness on the risks of VPN applications through audio and visual media, SMS awareness messages and social media platforms, and clarifying their risks and the importance of discipline in their use. Other sectors must subsequently play a role such as education, as it has a major role in this regard by providing awareness initiatives in universities and schools through electronic courses and means such as digital platforms, including the Saudi Digital Library platform. The results of the field study showed that the largest percentage of users are students, while there is widespread use at the level of different sectors. Therefore, awareness should also be provided at the level of government and other sectors, as it is possible for VPN service providers to access sensitive information of government officials and employees through these applications. In order for the initiatives to be successful, it is imperative to identify the qualified individuals responsible for implementing awareness programs. In this dimension, the application of the principle of convincing the target community on the importance of cybersecurity awareness and the effects of incorrect use of VPN applications is worth mentioning, in order to encourage internet users from the Saudi society to adopt safety precautions and to train them on the means of security in cyberspace when using these applications and to convey the message to them clearly, Fig. 6 shows a summary of the proposed framework.

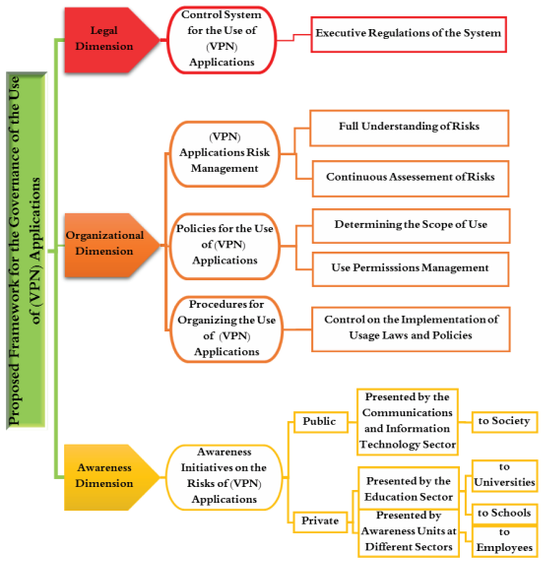


Fig. 6. Outline of the suggested framework for the governance of the use of (VPN) applications in the Kingdom of Saudi Arabia

References

[1] Q. Zhang, J. Li, Y. Zhang H. Wang and D. Gu, "Oh-Pwn-VPN! Security Analysis of OpenVPN-Based Android Apps," presented at Int. Conf. Cryptol. Net. Secur., Hong Kong, China, Nov. 30-Dec. 2, 2017, pp. 373-389. doi: 10.1007/978-3-030-02641-7_17.

[2] N. A. Hassan and R. Hijazi, "Online Anonymity," in Digital Privacy and Security Using Windows, Berkeley, CA, USA: Apress, 2017, ch, 4, pp. 123-194.

[3] National Cybersecurity Authority, Aldawabit Al'asasiah lil'amn Alsybrani [Essential Cybersecurity Controls] Saudi Arabia: National Cybersecurity Authority, 2018. [Online]. Available: https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

[4] M. Otayf and A. Qassem, "Cybersecurity," 2019, Jazan.

[5] He Ye, "Effectiveness of governance of the global network security," M.S. thesis, Department of Diplomacy, China Foreign Affairs University, Beijing, China, 2015. [Online]. Available: http://cdmd.cnki.com.cn/Article/CDMD-10040-1015037284.htm.

[6] GO-Globe.com, The State of VPN Usage – Statistics and Trends [Infographic], 2016. [Online]. Available: https://www.go-globe.com/vpn-usage-statistics/ (accessed Feb. 25, 2020).

[7] R. Al Jamal, Muqadimah fi Manahij Albahth fi Aldirasat Al'iielamia [An introduction to research methods in media studies] Cairo, Egypt: Open Education Center-Cairo University, 2019.

[8] A. Fonteneau, Saudi Arabia in 2019: A Year of Digital Growth, 2019. [Online]. Available: https://www.socializeagency.com/2019/01/30/digital-in-2019-saudi-arabia/ (accessed Feb. 10,

2020).

[9] A. L. Comrey and H. B. Lee, A First Course in Factor Analysis, 2nd ed. New York, NY, USA: Psychology Press, 1992. doi: 10.4324/9781315827506.

[10] M. Namara, D. Wilkinson, K. Caine and B. P. Knijnenburg, "Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology," in Proc. Priv. Enhanc. Technol., vol. 2020, no. 1, pp. 83-102, Jan. 2020, doi: 10.2478/popets-2020-0006.

[11] A. Pavlicek and F. Sudzina, "Use of virtual private networks (VPN) and proxy servers: Impact of personality and demographics,"in 2018 Int. Conf. Digit. Inf. Manage. (ICDIM), Berlin, Germany, 2018, pp. 108-111, doi: 10.1109/ICDIM.2018.8846991.

[12] A. Jayatilleke and P. Pathirana, "Smartphone VPN App Usage and User Awareness Among Facebook Users," in 2018 Nat. Inf. Technol. Conf. (NITC), Colombo, 2018, pp. 1-6, doi: 10.1109/NITC.2018.8550081.

[13] M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar and V. Paxson, "An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps," in IMC'16: Proc. 2016 Internet Meas. Conf., Santa Monica, CA, USA, Nov. 2016, pp. 349-364, doi: 10.1145/2987443.2987471.

[14] F. Donovan, Android security hole could enable attackers to bypass VPN, 2014, Fierce Mobile IT.

[15] S. Tao, "The Effects of Mobile Phone's VPN Technology on the Network Security," Netinfo Secur., vol. 2013, no. 6, p. 22, 2013.

[16] R. De Bruin and S. H. von Solms, "Cybersecurity Governance: How can we measure it?," 2016 IST-Africa Week Conf., Durban, 2016, pp. 1-9, doi: 10.1109/ISTAFRICA.2016.7530578.

[17] A. Abo-Seada, "Virtual Private Network (VPN)," (in Arabic), Arab J. Inform. Stud., vol. 1, pp. 111-135, Jul. 2012.

[18] J. M. Stewart, Network Security, Firewalls, and VPNs, 2nd ed. Burlington, MA, USA: Jones & Bartlett Learning, 2014.

[19] A. Karaymeh, M. Ababneh, M. Qasaimeh and M. Al-Fayoumi, "Enhancing Data Protection Provided by VPN Connections over Open WiFi Networks," in 2019 2nd Int. Conf. on new Trends in Comput. Sci. (ICTCS), Amman, Jordan, 2019, pp. 1-6, doi: 10.1109/ICTCS.2019.8923104.

[20] R. Leibovitz, Why Your VPN Service Should Offer an Ad Block Feature, 2019. [Online]. Available: https://securethoughts.com/why-your-vpn-service-should-offer-an-ad-block-feature/ (accessed Apr. 2, 2020).

[21] "VPNs: Access All Website Blocked in the UK," Comput. Act!ve, vol. 532, pp. 50-57, 2018.

[22] T. Bui, S. Rao, M. Antikainen and T. Aura, "Client-Side Vulnerabilities in Commercial VPNs," in Secure IT Systems. NordSec 2019. Lecture Notes in Computer Science, vol 11875, A. Askarov, R. R. Hansen and W. Rafnsson, Eds, Cham, Switzerland: Springer, 2019, pp. 103-119, doi: https://doi.org/10.1007/978-3-030-35055-0_7.

[23] C. Cawley, 11 Reasons Why You Need a VPN and What It Is, 2018. [Online]. Available: https://www.makeuseof.com/tag/reasons-to-use-vpn/ (accessed Apr. 2, 2020).

[24] B. Jansen, Why VPN can make your online gaming better, Mar. 2018. [Online]. Available: https://www.technologytimes.pk/2018/03/03/vpn-make-online-gaming-better/

[25] "STOP USING VPNs That Are Unsafe!," Computer Act!ve, vol. 573, pp. 50-57, 2020.

[26] S-mart.biz. Servizi VPN per Android: oltre il 62% richiede permissioni invadenti esuperflue [VPN services for Android: over 62% request intrusive and superfluous permissions]. Accademiaitalianaprivacy.com. [Online]. Available: https://www.accademiaitalianaprivacy.it/dettaglioNews.asp?id=126 (accessed Mar. 23, 2020).

[27] Saudi Group for Information Assurance (Hemaya), "Smart devices risks and protection," (in Arabic). [Online]. Available: http://eds.a.ebscohost.com.sdl.idm.oclc.org/eds/detail/detail?vid=2&sid=f7d3ecaf-eb35-4f22-902b-4da8643b1e42%40sessionmgr4007&bdata=JnNpdGU9ZWRzLWxpdmU%3d#db=bsu&AN=94293472 (accessed Mar. 24, 2020).

[28] Cyware, The Essentials of VPN: Is Paid VPN Safer Than Free VPN Service?, 2017. [Online]. Available: https://cyware.com/news/the-essentials-of-vpn-is-paid-vpn-safer-than-free-vpn-service-434029a2 (accessed Mar. 22, 2020).

[29] S. Alexander, Alexander: How to avoid browser hijacking, June 2018. [Online]. Available: https://www.startribune.com/alexander-how-to-avoid-browser-hijacking/485950411/?refresh=true

[30] M. Singhal, "Analysis and Categorization of Drive-By Download Malware Using Sandboxing and Yara Ruleset," M.S. thesis, Faculty of the Graduate School, The University of Texas, Arlington, TX, USA, May 2019. [Online]. Available: https://rc.library.uta.edu/uta-ir/bitstream/handle/10106/28148/SINGHAL-THESIS-2019.pdf?sequence=1&isAllowed=y

[31] S. Taylor, Free VPN Services – What You Need to Know, 2019. [Online]. Available: https://restoreprivacy.com/vpn/free/ (accessed Mar. 22, 2020).

[32] K. S. Alghathbar and A. N. Alsabih, "An Analytical Study of Saudi Hackers," (in Arabic), J. Inf. Stud., vol. 10, pp. 243-270, 2011.

[33] J. H. Arishee and S. A. Aldossari, "The role of higher education institutions in promoting a culture of information security in society," (in Arabic), King Fahad Nat. Lib. J., vol. 24, no. 2, Apr.-Sep. 2018.

[34] R. Wyden and M. Rubio, Wyden and Rubio VPN Letter to DHS, Feb. 2019. [Online]. Available: https://www.wyden.senate.gov/imo/media/doc/020719%20Wyden%20Rubio%20VPN%20Letter%20to%20DHS.pdf (accessed Mar. 24, 2020).

[35] Alwatan, "America warns ... VPN apps are dangerous!," (in Arabic). [Online]. Available: https://bit.ly/3ex2KR0 (accessed Fab. 10, 2020).

[36] A. Alshalan, S. Pisharody and D. Huang, "A Survey of Mobile VPN Technologies," in IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1177-1196, Secondquarter 2016, doi: 10.1109/COMST.2015.2496624.

[37] W. Allababidi, "Report: 'Dark Web' is a looming danger that threatens the Internet sector," (in Arabic), Aug. 12, 2017. [Online]. Available: https://www.albayan.ae/economy/local-market/2017-08-12-1.3023571

[38] S. Shukla, Virtual Private Network (VPN) | An Introduction, Oct. 2017. [Online]. Available: https://www.geeksforgeeks.org/virtual-private-network-vpn-introduction/ (accessed Mar. 31, 2020)

[39] T. Noir, "Information Governance in the Arab Countries," in Public and Private Corporate Governance for Economic and Structural Reform, Cairo, Egypt.

[40] Judicial Department, Law to Combat Information Technology Crimes. [Online]. Available: https://www.tra.gov.ae/ar/media-hub/press-releases/2016/8/1/telecommunications-regulatory-authority-issues-statement-on-the-use-of-vpn-to-clarify-media-reports.aspx (accessed Apr. 1, 2020).

[41] Telecommunications Regulatory Authority, Telecommunications Regulatory Authority issues statement on the use of VPN to clarify media reports, Aug. 1, 2016. [Online]. Available: https://www.tra.gov.ae/ar/media-hub/press-releases/2016/8/1/telecommunications-regulatory-authority-issues-statement-on-the-use-of-vpn-to-clarify-media-reports.aspx (accessed Apr. 1, 2020).

[42] A. Senft, J. Dalek, H. Noman and M. Crete-Nishihata, Monitoring Information Controls in Iraq in Reaction to ISIS Insurgency [Transl. Cyber Arabs], June 24, 2014. [Online]. Available: https://bit.ly/3blf0SG (accessed Apr. 1, 2020).

[43] R. Abdul Aziz, Using VPN For Security, 2012. [Online]. Available: https://muscatdaily.com/Archive/Stories-Files/Using-VPN-for-security (accessed Apr. 1, 2020).

[44] A. O'DRISCOLL, Where are VPNs legal and where are the banned?, May 2019. [Online]. Available: https://www.comparitech.com/vpn/where-are-vpns-legal-banned/#Z (accessed Apr. 1, 2020).

[45] D. Reisinger, How VPN Restrictions Imposed by China, Russia Impact Internet Freedom, Aug. 2017. [Online]. Available: eweek.com/security/how-vpn-restrictions-imposed-by-china-russia-impact-internet-freedom.

[46] Oxford Analytic, China cross-border cyber controls undergo shift, 2017. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/OXAN-DB224436/full/html

[47] Ministry of Industry and Information Technology, Notice of the Ministry of Industry and Information Technology on Clearing and Regulating the Market of Internet Network Access Services, Jan. 2017. [Online]. Available: http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html (accessed Apr. 11, 2020).

[48] Y. Wei, China's New Cybersecurity Regulations: Analyzing the Ban on VPN Services, Apr. 2017. [Online]. Available: https://jsis.washington.edu/eacenter/2017/04/17/chinas-new-cybersecurity-regulations-analyzing-ban-vpn-services/ (accessed Apr. 2, 2020).

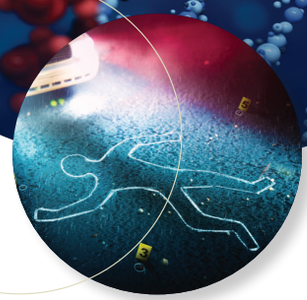
[49] M. Wyciślik-Wilson, Russia orders NordVPN, ExpressVPN, HideMyAss and other VPNs to block numerous sites. [Online]. Available: https://betanews.com/2019/03/29/russia-vpn-blocks/

[50] The Associated Press, Law outlawing use of VPNs comes into effect in Russia, Nov. 2017. [Online]. Available: https://apnews.com/article/0c9b28eae516460082efe3957c175b3c

[51] Communications & Information Technology Commission, The Anti-Cyber Crime Law, 2007. [Online]. Available: https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_004_%20A_%20Anti-Cyber%20Crime%20Law.pdf (accessed Apr. 16, 2020).

AJFSFM | Arab Journal of Forensic Sciences and Forensic Medicine

CALL FOR PAPERS



The Arab Journal of Forensic Sciences and Forensic Medicine (AJFSFM) is pleased to welcome the submission of scientific articles in all disciplines of forensic science and forensic medicine. The AJFSFM is a peer-reviewed, open access (CC BY-NC), international journal dedicated to the development and application of forensic sciences and forensic medicine knowledge and research for the purpose of law and justice across the globe.

The AJFSFM is an official publication of the Arab Society for Forensic Sciences and Forensic Medicine (ASFSFM) and is published twice a year.

Focus and Scope:

The topics covered in the AJFSFM include, but not limited to:

- Forensic Pathology
- Odontology
- Histochemistry
- Toxicology (drugs, alcohol, etc.)
- Psychiatry and Hypnotics
- Forensic Anthropology and Archeology
- Fingerprints and Impressions
- Firearms and Toolmarks
- Digital forensics and Cyber crimes
- Criminal justice
- Crime scene
- Investigations of value to public health
- Forensic chemistry (Inks, Paints, Dyes, Explosives, Fire accelerants)
- Forensic Biology (Serology, Human DNA profiling, Entomology, population Genetics, Anthropology)
- White collar crimes (Counterfeiting and Forgery; Questioned documents)

The AJFSFM publishes original contributions that fall under any of the following manuscript categories: Original research papers, Case reports, Review articles, Book Reviews and Conferences / Symposia Proceedings.

Papers can be written in English or Arabic. Articles received are sent for blind peer review, with a review procedure completed within 4-6 weeks of submission. Authors can also submit their manuscripts online or send them via e-mail: ajfsfm@nauss.edu.sa

For more information, please contact:

Journal's Website: https://journals.nauss.edu.sa/index.php/AJFSFM/index
Journal's Mail: ajfsfm@nauss.edu.sa