مجلة أكاديمية شمال
أوروبا المحكمة للدراسات
والبحوث التربوية والإنسانية
ـ الدنمارك
العدد ـ 15
13/04/2022

The Influence of Electronic Piracy On Electronic Management and Society

Prepared by

Aseil nadhum kadhum
Easeel18@yahoo.com

Aseel nadhum kadhum
Easeel18@yahoo.com

Abstract:

This article discusses a comprehensive study aimed at revealing the reality of achieving cybersecurity and its impact on electronic piracy in all institutions and society in general, as well as offering recommendations for reducing these crimes and identifying the most important variables that contribute to them. Electronic hacking conduct is to get hacked. Electronic hacking has a wide variety of undesirable and negative implications for society, according to the findings of this study, and computers and networks are among the technologies accessible to hackers.

As a result of scientific and technological advancement in communications, information technology, and the Internet, new patterns of advanced electronic hacking and extortion in commissions and media disclosure have evolved (social networking sites). Raising awareness and resisting steps that expose criminals to legal prosecution and consequences commensurate with the magnitude of the crime committed are both required. Random sampling was employed, which was compatible with the study's data and goals, which totaled 130. The study also included a questionnaire and an interview, and the results showed that the sample items agreed on the impact of cybersecurity as a method to an average degree. The researchers selected the descriptive analytical approach as the study's methodology and instruments since it is the most suited way for performing the investigation and achieving its goals.

The findings of this study are the numerous precautionary steps that may be implemented to avoid cyber hacking so that people can enjoy utilizing technology rather than being limited in their use. Work to implement extensive scientific and practical awareness ways to preserve security for public and private institutions and the community, as well as to unify the community's social and cultural activities where the suggestions were made. Finally, we urge a more thorough investigation of cybersecurity and its societal implications.

Key word: cyber, cyber security, various, electronic, technological

Introduction:

Cyber security now encompasses not just the protection of information, which is a company's and society's most important asset, but also all aspects of technical infrastructure. Finance, commercial, emergency services, public services, and

government defense are the engine where society works to reduce and control the possibility of a cyber-attack, and risks must be managed because of a technically interconnected community, where attackers look for vulnerabilities, they engage in malicious actions for reasons such as challenges, profit, or curiosity, and this attraction stems from the ease with which these activities and impairing are carried out, and risks must be managed because of a technically interconnected community, where attackers look for vulnerabilities, they engage in malicious [3] From here, electronic piracy is defined as a violation of intellectual, literary or creative property rights by a person who downloads and copies programs without the permission of its creator, as well as illegal copies of books, music, and computer programs.

The rapid modernization of technology in many societies, where countries tend to agree to work, has led to the growth of electronic thefts in recent years, as well as the global spread of the Corona virus, which has contributed to the rapid modernization of technology in many countries. cultures. Strengthening the distance education system, until the emergence of the Corona virus, in an attempt to adapt to the new reality imposed by the Corona virus on the world. The Internet has evolved into a seemingly natural way to facilitate and control human life. Due to the growing confidence in the Internet, some hackers have been able to take advantage of some of the human communities vulnerable to hacking through electronic hacking operations for current or future personal gain, humanity did not stop the Corona virus issue until the emergence of computer viruses killing those who were not infected with it. As a result, humanity is at risk of contracting two viruses: The Corona virus and computer viruses, the so-called C&C virus, or computer viruses that exploit the Corona virus. [4]

Thousands of computers throughout the world are being targeted, signaling a huge shift in information security that academics understand in concept and that this technology is putting into practice. Many countries and places have experienced terrorism and worry as a result of hacking, including information security corporations in the United States, and Europe and China are two of the world's most powerful economies. While the sacrifices demanded by hackers are insignificant in comparison to the extent of the danger and its moral implications, it does pave the way for a new future for the technical threat's opposite side. The rogue face has the capacity to damage more services than it does individual interests, national economies, or the ability to produce an atomic weapon. [6]

Here, the so-called cyber security, also called information security and computer security, must be activated, a branch of technology concerned with protecting systems, property, networks and programs from digital attacks that usually aim to gain access to, change or damage sensitive information, extort users to obtain money or disrupt business operations [7]

Governments and commercial organizations all over the world make extensive use of information and communication technology, making security a top priority. To achieve this, they implement technical security measures and develop security policies that define proper behavior among employees, consumers, and citizens. The fundamental goal of cyber security awareness campaigns is to persuade people to adopt safe practices. Effective Internet influence, on the other hand, needs more than merely alerting people about what they should and should not do. They must first accept the confidentiality of the pertinent data, then comprehend how it should respond, and last, be ready to do so. Face a slew of additional obligations. [5]

According to Edward Amoruso, author of Cyber Security published in 2017, "the set of technologies that will reduce the risk of attacking software, computers, or networks." Tools to combat hacking, detect and stop digital viruses, and provide encrypted communications are among these methods.

An experiment was used in this study to investigate the factors that may discourage or prevent digital piracy in a developing country in the Middle East. They can better understand the factors deterring digital piracy by separating respondents into groups and using different treatments for each study group.

- **Research questions:**

1) What strategies are employed to strengthen and combat cyber security?

   Is the Internet a Threat to Electronic Management?

2) How important are cybersecurity and cyber flexibility in e-management for mitigating cyber risks?

- **Objective**:

1. Assess the level of strategies used to enhance and combat cybersecurity

2. Recognize the extent of the impact of the Internet and its threat to electronic management

3. How important is the importance of cybersecurity and cyber resilience in electronic management and its impact on society to mitigate cyber risks?

• The importance of cyber security:

The importance of the study can be divided into two aspects:

Theoretical aspect:

The importance of the study is that it studies a topic that was and will remain one of the renewable and important topics for countries, their governments and society, which is the transformation of traditional governments in countries into electronic governments that provide government services electronically. And since the administrations have started this transformation, it is necessary to follow up on this project to ensure its success. This study aims to enhance the aspirations of researchers to advance society to horizons of sustainable knowledge, by employing modern technologies in the provision of administrative services. Therefore, it is hoped that this study will be an addition to intellectual production on the subject of digital transformation and e-government, and the possibility of its application in all environments of society.

The practical side:

The following groups can benefit from the results of this study as follows:

• Institutions and companies: through the possibility of acquainting them with the reality of digital transformation, and assisting decision-makers and officials in developing appropriate strategies and future plans in cybersecurity.

• Citizens and users of e-government services

• Researchers and people with an interest in the subject: Contribute to the creation of a search gateway for scholars and those interested in the subject.

The limits of the study:

The objective limits of the study: This study was limited to identifying the requirements for achieving cybersecurity for society.

Human limits of the study: The study was applied to a random sample of 130 .

The spatial boundaries of the study: This study was applied in the province of Babylon, Iraq

- **Theoretical background**

1) Terms related to cybersecurity

Cyber security is a method that entails installing numerous layers of protection on the computer, network, program, or data that the user want to safeguard. There are a variety of terminology used in the field of cybersecurity, including:

- Cyberspace is an interactive digital realm made up of the weak and intangible aspects of a group of digital equipment, network systems and software, and users, who can be either operators or users. It is referred to as the contemporary army's fourth arm.
- Cyber deterrence is the prevention of dangerous acts against digital space and national assets, as well as assets that enable space operations.
- Any activity that compromises the capabilities and functionalities of a computer network for personal or political gain allows the attacker to manipulate the system without putting the system at danger.
- Cybercrime is a term used to describe a series of illicit acts conducted using electronic devices or devices connected to the Internet that necessitate the use of particular computer technologies and information systems to commit, investigate, and punish.

2) The following are the factors that make the Internet a rich ground for hackers:

- Increase teleworking: Increase the implementation of networks that allow employees to access company databases remotely, with a large increase in employee demand for access, Furthermore, these personnel have a poor cyber security culture, and the majority of them use personal computers that may include non-native or obsolete software. It makes it much easier for many hackers because of the attainable goals and numerous weaknesses that can be exploited.
- Human governance uncertainty, vulnerability to cyber security measures, segregation of the company's IT personnel, and issues managing the e-commerce environment are all challenges in securing the online business environment. Workers whose work area is unknown are included in this category. Anti-theft is becoming increasingly difficult, providing the ideal setting for hackers to fulfill their objectives.
- As more people strive to adopt the concept of social distance, their reliance on virtual discussions via social networking apps and video

calls grows, Intelligence hackers targeted them with the goal of extorting personal information by stealing or encrypting it. They can also take control of their own devices, which will be utilized by botnets to launch cyberattacks against companies, organizations, and governments.

- More time spent on the internet entails more risks: Internet usage has increased, as has social presence. Vodafone, for example, reported that in some countries, the percentage of downloads had surpassed 50%. Some countries, such as Italy, have high levels of internet usage, climbed by 30%, while the United States of America's consumption increased by 18% until March 22 - that is, before it took first place in terms of the number of infections - thus the increase in the period of presence on the Internet also means an increase in the rate of exposure to cyber-attacks.
- Taking Advantage of Human Fear and Anxiety: Not only that, but hackers have taken advantage of human fear and anxiety to undertake cyber hacking operations, since many people are browsing the internet for information about the Coronavirus. More information can be found here. This virus and the symptoms it causes. Hackers have constructed deceptive websites that operate as a trap for visitors once they enter, including health tips to prevent infection and statistics on the number of new cases of the disease. Visitors' personal information is stolen and sold online on one of these sites, or their personal devices are hacked.

3) Definition of malware

They are specialized programs that, in addition to destroying data and information on a computer, phone, or network, attempt to disrupt the system and its operation. User data and files are deleted and encrypted so that they cannot be accessed or received without paying.

4) Methods for detecting exposure to a malicious program

This is mostly unusual damaging conduct that reveals its presence, and we may observe the following:

- If the gadget is slow while the computer or phone is being used normally, this can be noticed.

- The appearance of advertisements on the screen in places where they do not normally appear is one of the most accurate indicators of the presence of malicious software, and it usually takes the form of a lucrative advertisement such as "Congratulations, you won a million dollars," which you should not click on because it will cost you a lot of money.
- After meeting major issues as a result of malware, sudden system shutdown, blue screen, and freeze might occur, particularly on Windows systems.

  The mysterious loss of disk storage space indicates that the computer is infected with a high number of harmful files.

- There has been an unusual surge in the device's internet consumption.
- Background malware activity is indicated by increased consumption of system resources and a very fast fan start.
- Changing the browser's home page without authorization and clicking on links might result in errors and undesirable destinations, as well as slowing down the browser.
- Unexpectedly, new components, tools, or extensions appear in the browser, which is bad for the browser. Antivirus software fails to work, and it is impossible to update it.
- There is a real program that informs you that it has obtained your data and that you must pay a ransom to get it back.

Even if the computer appears to be in good working order and there are no unusual behaviors, there is insufficient evidence of computer health, since malware can be disguised in ingenious ways.

5) What causes a gadget to become infected with malware?

The Internet and email are two of the most prevalent ways to get malware. By visiting one of the sites it has previously recorded, downloading vulnerable files, opening unsafe emails, or clicking on dubious adverts and profit messages, this malware may gain access to you.

6) Stay away from malware.

The most critical precautions to take to avoid becoming infected with malware are as follows: • Only download programs from the company's official website.

- Do not click on any advertisements or offers that show on your screen.

Never open e-mail messages from somebody you don't know.

- Complete disdain for any website that provides services in the form of untrustworthy software or adverts.

7) What type of malware is the most common?

1. Adware is a program that is solely dedicated to displaying advertisements.
2. Spyware: computer monitoring and spying software.
3. Virus: A dangerous program that, when downloaded, links to another program and then repeats itself, infecting more programs.
4. Worms are harmful programs that repeat themselves repeatedly and are ready to spread to other devices, multiply, and destroy files.
5. Trojan: This is one of the most dangerous hazardous programs since it enters the computer without permission, collects financial and personal data, allows alteration, and allows ransomware to be loaded.
6. Ransomware encrypts files and appears in front of you, telling you that you must pay money to get the files back within a certain amount of time.
7. Rootkit: On an infected computer, software that grants the attacker administrator privileges.
8. A keylogger is a malicious program that records every keystroke you make on your keyboard, allowing the attacker to steal passwords and usernames.

- **Previous piracy research**

1. Study by Jessica Dawson and Robert Thomson* The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance
This study aimed to identify the importance of cyber education and workforce development, and that there is a dearth of quantitative evaluation. The method used was a review of the literature related to cyber news. The research focuses on technical skills while recalling the social influences that dictate success or failure in everyday environments. It has identified future hypotheses, developed the workforce in the field of cybersecurity, and made recommendations for social and cognitive measures that may indicate better performance in the future.
2. Study by Bruce D. Caulkins; Karla Badillo-Urquiola et al.: Cyber workforce development using a behavioral cybersecurity paradigm
This paper contributes to the ongoing efforts in the cybersecurity community to enhance the development of the cyber workforce by providing an overview of key gaps and suggesting practical learning strategies. The paper outlines a pilot

educational program launched at the University of Central Florida (UCF) The present paper provides a starting point for further discussion of the human side of cybersecurity, and concludes with considerations of "lessons learned" from early responses to UCF from the program's inaugural student cohort.

3. Study by Melissa Dark et al.: Realism in Teaching Cybersecurity Research: The Agile Research Process

This study demonstrates an urgent need to educate future researchers about the research process itself, which is increasingly unpredictable, multidisciplinary, multi-organizational, and team-oriented. In addition, there is a growing demand for cybersecurity research that can produce fast, reliable and actionable results. The rapid research process is a new approach to providing such rapid and reliable applied research. Designed to be fast, transparent and iterative, each iteration produces results that can be applied quickly. Purdue University uses Agile Research.

4. Hussain Aldawood* and Geoffrey Skinner Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues

This study highlights the persistent pitfalls and issues that organizations face in the process of developing human knowledge to protect against social engineering attacks. A detailed review of the literature is presented to support these arguments with analysis of contemporary methods. The results show that despite modern cyber security preparations and trained personnel, hackers are still successful in their malicious work of stealing sensitive information that is essential to organizations. Factors affecting users' efficiency in detecting and mitigating threats have been identified as business environmental, social, political, constitutional, regulatory, economic, and personal.

5. A study by Nawal bint Ali Al Balushi and others entitled: The reality of digital transformation in Omani institutions

This study aimed to explore the reality of digital transformation in the Sultanate of Oman, by identifying the roles played by the various institutions in the Sultanate in the field of digital transformation and e-government. The study relied on the qualitative descriptive approach, and the semi-structured interview as a main tool for data collection. Among the most prominent findings of the study are: Institutions have made clear efforts and roles for digital transformation, such as awareness, education, training, integration, readiness, and others. The study recommended the need to introduce and promote the available electronic services, by exploiting technology such as various media and social networks, in order to be recognized by the beneficiaries and then expand the scope of their use.

Commenting on previous studies:

Through what has been presented from previous studies, it is clear that the studies that dealt with the field of cybersecurity and its impact on society are very limited

to the researcher's knowledge - but what has been accomplished in scientific research or theoretical literature has emphasized the importance of studying cybersecurity from its various dimensions and the study is proceeding The current trend is in the same direction, with the aim of promoting the idea, culture and awareness of cyber security and reaching the requirements and proposals necessary to achieve cyber security from its various dimensions, especially in Iraq - Babil.
And the current study agrees with all previous studies in the study of cybersecurity in general, as it agrees with some of them in the type of study and the approach followed, which is the descriptive analytical approach, and it agrees with it in the data collection tool, which is the questionnaire.
While the current study differed with Melissa Dark's study, it used the rapid approach of Agile Research, which relied on the use of technical programs. And the Badillo-Urquiola study, which adopted the method of the curriculum as an experimental educational program
The current study was characterized by providing a set of cybersecurity requirements through the application of the research tool (the questionnaire) to random samples from the community and reaching a set of recommendations and results.
In this study, an experiment is conducted to assess the elements that can discourage a young person from engaging in digital hacking.
This study will seek to improve security services in the country in general, and education in particular, in order to combat threats, threats and cybercrime. The results will expose people to diverse cybersecurity activities and risks while creating a public platform model for cyber resilience awareness and promotion.

Methods:
A descriptive survey design was adopted by the researchers. This architecture produces a flat model that allows researchers to provide a thorough account of the variables' cause, effect, and scope. Iraq was chosen as the study's subject. All IT professionals, IT engineers, and security officials who have been exposed to IT are included in this study's community. The researchers utilized stratified random sampling as a method of data collection.
The study's 130 participants were chosen using this way. The "Cyber Security and Resilience Questionnaire" was the primary tool employed in this investigation (CSRQ). The questionnaire was divided into sections "A" and "B," with section "A" containing information regarding the respondents' personal data and section "B" containing two variables such as strengthening cybersecurity and Internet resistance. The technologies employed in the study were utilized to have computer professionals authenticate the face and content. The researchers employed the Cronbach's Alpha reliability method to test the tool's reliability level by APSS

software with 20 subjects who were not included in the main study. A reliability coefficient was calculated as a result of this test (0.81), This indicates the reliability of the research instrument. Respondents presented their audience to the researcher via a cover letter.
Percentages and the chi-square test were used to analyses the data. At the 0.05 alpha level, a significant test was performed on the hypothesis.

- **Results and discussions**

Research Question 1

Research topics are screened to reveal solutions to improve cyber security and resilience in e-government in the face of cyber threats and its impact on society. Percentage analysis was used to answer the question. (see Table 1)

Table 1: Percentage analysis of measures employed in e-government to improve cyber security and cyber risk resilience

PERCENTAGE ANALYSIS	FREQ	%	Remark
Reconstruction of public and private organizations considers and develops a holistic approach to information security, as well as the security measures required to safeguard IT infrastructure.	6	8	5^{th}
To supply this infrastructure, security experts must be trained and developed.	14	18	4^{th}
Act now before the situation worsens and the costs of inactivity mount.	22	23.5	3^{th}
To create a vibrant digital community, create a good network of national computer emergency response teams with strong internet security.	27	21	2^{th}
Cyber simulations should be regulated, and a clear guideline for the central information infrastructure should be established.	31	29.5	1^{th}
Total	100	100%	

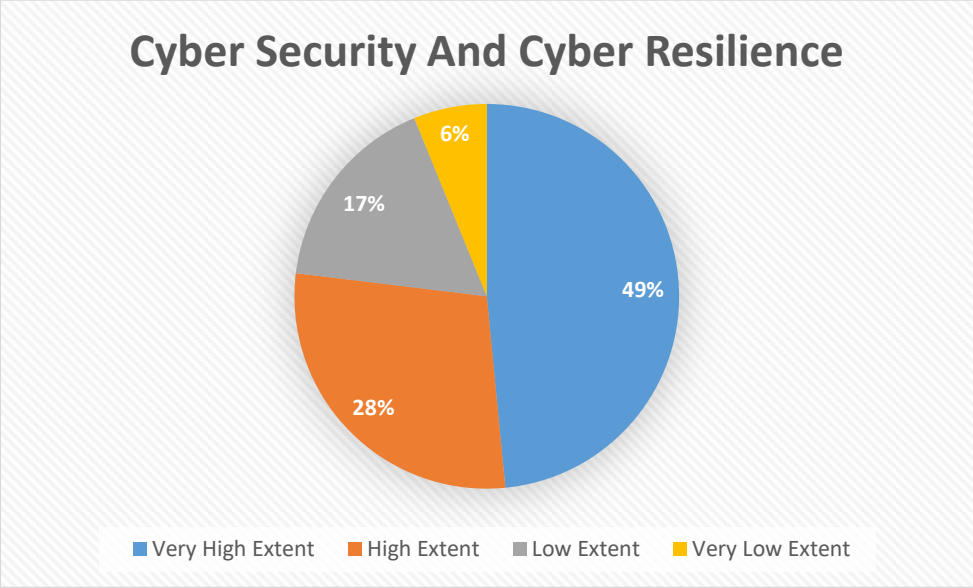
Source: Field Survey

Table 1 shows that "organize simulations of cyber incidents, and build a well-defined policy on critical information infrastructure (CIIP) protection" are the most commonly employed tactics in increasing cyber security and cyber resilience over electronic management (29.5 percent), "Review public and private enterprises, establish their overall approach to information security, and put in place the appropriate security measures to protect vital IT infrastructure," according to the least used plan.

Research Question 2

The purpose of the study was to find out how much cybersecurity and cyber resiliency can help mitigate the challenges that the Internet presents to electronic governance and its impact on society. The solution to the research question can be found in Table 2.

Table 2: Percentage examines how cybersecurity and cyber resilience may assist electronic management reduce cyber risks.



Cyber Security And Cyber Resilience	Freq	Percentage
Very High Extent	63	49
High Extent	37	28
Low Extent	22	17
Very Low Extent	8	6
Total	130	%100

- **Source: Field Survey**

According to the results of Table 2, 58.5 percent of respondents said that cyber security and cyber resilience have aided in the extremely high reduction of cyber risks in cyber management. It was deemed excessive by 31.5 percent of those polled. The third group of people confirmed the 6.5 percent number. While the smallest percentage of respondents (3.5%) reported that cyber flexibility and cyber security had only a minor impact on reducing cyber risks in government.

Hypothesis 1

This null hypothesis indicates that people's perceptions of the influence of cyber security and cyber resilience on decreasing cyber risks in cyber management are not significantly different. (Refer to Table 3)

Table 3: Chi-Square analysis of the extent to which cybersecurity and cyber resiliency greatly help cyber risks in electronic management.

Cyber Security And Cyber Resilience	Freq	Expected Freq	X 2
Very High Extent	63	32.5	51.07
High Extent	37	32.5	
Low Extent	22	32.5	
Very Low Extent	8	32.5	
Total	130	%100	

***Significant at 0.05 level; df = 3; Critical = 7.82**

The value of X2 determined as shown in Table 3 is (51.07). This result was compared to the crucial X2 value (7.82) at 0.05 levels with 3 degrees of freedom to see if it was significant. X2 (51.07) had a calculated value that was higher than the critical value (7.83). As a result, the outcome was important. Thus People's perceptions of the influence of cybersecurity and cyber resilience in minimizing cyber risks differed greatly, according to the survey. Due to the significance of the outcome, the null hypothesis was rejected and the alternative hypothesis was accepted.

• Conclusions

The current study dealt with an analysis of the reality of digital transformation in the world due to the Corona pandemic and the extent of the impact of this transformation in terms of cybersecurity and electronic piracy and its impact on all institutions and society, by clarifying the roles that institutions play in this aspect such as community awareness, education and training, and linking in data and its integration between institutions, And re-engineering its procedures, and measuring the level of its readiness for transformation and other roles, then the study touched on evaluating the level of improving cyber security in institutions - the study sample - and the government cloud and others, in addition to digital society development projects represented in training and awareness programs, and other cybersecurity projects.

Based on the findings of the current study, it recommends the following:

- The importance of introducing and advertising accessible electronic services via the use of technology such as various media and social networks in order to get recognition among beneficiaries and subsequently extend their use.
- In order to achieve sustainability, profit from collected experiences, and avoid work delays or interruptions, build permanent transformation teams in institutions and limit the continual change process in them, which negatively affects the quality and continuity of work. Recommendations
- Companies must raise awareness of cyber security and promote awareness of security risks in online communities.
- Companies must make long-term investments in enabling technology and resources to improve cybersecurity.
- Securing the material needs of the devices and equipment used, providing the technical requirements, adhering to the methods and procedures of modern technology, and educating workers in the field of web technology to use the system, are all important considerations. Training courses for employees and measures to avoid electronic piracy have become. More popular in a variety of professions. Work in the field of data management and help in promoting electronic culture.

Reference:

A. Arabic Reference

1. الأمير، حسين باسم. **(2018). تحديات الأَمْن السيبرانيّ**، مركز الدِّرَاسَات الاستراتيجية ، جامعة كربلاء، العراق، أيار 2018، متوفر على الموقع kerbalacss.uokerbala.edu.iq/wp/blog

2 . محمد. الهادي (2021). ***تحديات واستراتيجيات التحول الرقمي للمصالح الحكومية والمنشآت،*** مجلة الجمعية المصرية لنظم المعلومات وتكنولوجيا الحاسبات، 24(الرابع والعشرون)

3. البلوشية ، نوال علي و الحريصي نبهان حارث و العوفي علي سيف (2020). ***واقع التحول الرقمي في المؤسسات العمانية***. Journal of Information Studies & Technology (JIS&T), 2020(1), 2.

Foreign Reference

4.Schneier, D. & Bruce, C. (2016). **Lessons From the Dyn DDoS Attack**, Schneier on Security Blog, 8 November 2016, https://www.schneier.com/blog/ archives/2016/11/lessons_ from_th_5.html

5.Kaplan, B., James, D. and Tucker, N. (2015) **Theory of deterrence and individual behavior**. Can lawsuits control file be sharing on the Internet? Review of Law and & Economics 3 (3), 693–714.

6.Hashim, M. J., Kannan, K. N., & Wegener, D. T. (2018). ***Central role of moral obligations in determining intentions to engage in digital piracy***. Journal of Management Information Systems, 35(3), 934-963.

7.Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021**). Cyber security in the age of COVID-19**: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248.

8.Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). **The privacy implications of cyber security systems**: A technological survey. ACM Computing Surveys (CSUR), 51(2), 1-27.

9.Dawson, J., & Thomson, R. (2018). **The future cybersecurity workforce**: going beyond technical skills for successful cyber performance. Frontiers in psychology, 9, 744.

10.Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., & Leis, R. (2016, October). **Cyber workforce development using a behavioral cybersecurity paradigm.** In 2016 International Conference on Cyber Conflict (CyCon US) (pp. 1-6). IEEE.

11.Dark, M. B. (2015**). "Realism in teaching cybersecurity research**: the agile research process," in Proceedings of the Information Security Education Across the Curriculum (Hamburg: Springer International Publishing), 3–14. doi: 10.1007/978-3-319-18500-2_1

12.OWASP, “OWASP Application Security Verification Standard.” 2020, Accessed: Dec. 15, 2020. [Online]. **Available**: https://owasp.org/www-project-application-securityverification-standard/.
13.SCOTT GODE, ―Video Conferencing Security Issues and Opportunities,‖ UnifySquare,2020. https://www.unifysquare.com/blog/videoconferencing-security-issues-and-opportunities/ (accessed Dec. 02, 2020).
14.ALEXEI, A., & ALEXEI, A. (2021). **Cyber Security Threat Analysis In Higher Education Institutions,** As A Result Of Distance Learning. International Journal of Scientific & Technology Research.
15.Kaspersky, “Digital Education: **The cyberrisks of the online classroom**,” 2020. Accessed:Dec.06,2020.[Online].Available:https://media.kasperskycontenthub.com/wpcontent / uploads/sites/43/2020/09/04113558/education_report_ 04092020_2.pdf.
16.M. T. J. Ansari, D. Pandey and N. A. Khan,(2019) “**Comparative literature analysis on security requirements engineering,**” International Journal of Engineering Sciences and Research Technology, vol. 8, no. 12, pp. 113–124, 2019.
17.Vovk, Methods of information security IoT, Master’s thesis, NTU of Ukraine "KPI named after Igor Sikorsky", 2018.
18.Kiennert, C., Ivanova, M., Rozeva, A., & Garcia-Alfaro, J. (2020). **Security and Privacy in the TeSLA** Architecture. In Engineering Data-Driven Adaptive Trust-based e-Assessment Systems (pp. 85-108). Springer, Cham.
19.Ning, Y., Xu, S. X., Yan, M., & Huang, G. Q. (2018). **Digital pricing with piracy and variety seeking**. International Journal of Production Economics, 206, 184-195.
20.ALEXEI, A., & ALEXEI, A. (2021). **Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learn**ing. International Journal of Scientific & Technology Research.