Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 17 (1), 2025
pp. 674 - 683

College Students' Perceptions Toward Jordanian Cybercrime Law

Diab M. Al-Badayneh[1], Hajar T. Nassar , Mohammad A. Al Sharairi 2

[1]*Ph.D*. Methodology, Criminology, and Security Studies

dbadayneh@gmail.com

ORCID 0000-0001-7416-6722

Department of Security Studies, Graduate College, Police Academy, MOI, Qatar & IKCRS, Amman, Jordan

[2]Hajar.nassar@bau.edu.jo

0009-0007-6414-984X

AllBalqa Applied University Jordan

[3]MALSHARAIRI@MOI.GOV.QA

ORCID 0000-0003-4823-3949

Department of law, Police College. Police Academy. Qatar

Abstract: This study analyzes the perspectives of Jordanian college students regarding the Jordanian cybercrimes law (JCL). The study sample consisted of 494 Jordanian students from four universities in Jordan (TTU, MU, JU, and BU). Among these, 43% were male, and 57% were female. The reliability, as measured by the method Cronbach's α, was 0.95, while the validity, indicated by the correlation with the low self-control (LSC) scale, was 0.309 (α = 0.00, F = 11.981, α = 0.00). More than 25% of the sample scrutinized the JCL and observed the politicization of the law. Moreover, three-quarters of the sample received information about it. Over fifty percent of the sample observed illegal activities online that warranted penalization. Fewer than 10% of the sample engaged with the JCL or participated in an online action that warranted penalty. More than a quarter of the sample (26.9%) viewed the law negatively; of them, 10.7% were males and 16.2% were females. Regreasing gender, net use, perpetration, knowledge, cyber extremism, and LSC explained 31% ($R^2 = .313$) of the variance in college students perceptions toward Jordanian cybercrime law. Table 2 showed that the overall effect of gender, net use, perpetration, knowledge, cyber extremism, and LSC was significant (F = 37.053, α = .000). Table 3 showed the unique contribution of each variable. Each variable significantly influenced college students' perceptions of Jordanian cybercrime law. except the gender. We discussed the educational, legal, and security implications.

Keywords. College students, cybercrimes, law, Jordan, perception

Received: 05 May 2025 **Accepted:** 22 June 2025 **Published:** 02 July 2025

INTRODUCTION

The study of control and communication in both engineered and natural systems is known as cybernetics, which derives from the Greek word Kubernetes, or steersman. Plato and Ampère introduced it in antiquity, and Norbert Wiener further developed it in his 1948 book. Cybernetics emphasizes control and communication in both engineered and evolved systems, focusing on their goals rather than creators' control. Norbert Wiener coined the term cybernetics in the 1940s, which has since become popular, ubiquitous, and revolutionary. Science fiction television serials like The Cyborgs and The Six Million Dollar

[*] Corresponding Author: Diab Al-badayneh dbadayneh@gmail.com

Man first used the term, depicting the combination of humans and machines to create a perfectly controlled system. Today, cybernetics encompasses various terms, like cyberspace, cybermalls, and cybercrime. [1]

Cybercrime is a rapidly growing phenomenon with evolving online behaviors, leading to challenges in measuring it. Various sources of data, including police statistics, victimization surveys, and private company reports, fail to provide accurate information about cybercrime trends. Factors impacting the measurement of cybercrime include a lack of common definition and comprehensive classification, a legal and harmonized framework surrounding cybercrime, a lack of awareness of being a victim, and disagreement on units of measurement. The Budapest Convention of Cybercrime in 2001 provided guidelines for creating legal provisions for certain cybercriminal acts. The absence of a standard classification for cybercrime, especially hybrid acts, poses challenges to the legal framework governing online crime. The lack of definitional and legislative clarity also impacts complaints to the police and victimization surveys, as people may not always be aware of the illegality of certain acts or their right to complain. Cross-checking official statistics can pose a challenge, as multiple victims in victimization surveys may report the same act as reported by police statistics. [2].

Cybercrime is a global issue involving online criminal acts, classified into three types: internet-specific crimes, fraud and forgery, and illegal online content. The European economy is at risk due to cybercrime, with its economic impact increasing fivefold between 2013 and 2017. The EU has implemented legislative actions, such as the 2013 Directive on information system attacks and proposed regulations for cross-border electronic evidence access in criminal investigations. The EU Cyber Security Strategy aims for a secure cyberspace for all citizens. [3].

The first cyber attack occurred in France in 1834, but cybercrime gained prominence in the late 20th century. Cybercriminals have since evolved their tactics and techniques for malicious gain, expanding into an ecosystem with leak sites, as-a-service models, and lucrative attack vectors like business email compromise. The modern history of cybercrime began in 1962 with Allen Scherr's cyber attack on MIT computer networks. In 1971, researchers created the first computer virus, the Creeper Virus. Ian Murphy was the first person to face a cybercrime conviction in 1981. In 1988, Cornell grad student Robert Morris' "Morris Worm" infected computer systems at Stanford, Princeton, Johns Hopkins, NASA, Lawrence Livermore Labs, and UC Berkeley. In 1989, ransomware, the AIDS Trojan, appeared on floppy disks. [4][5]

Cyberattacks have evolved significantly, with 30 million new malware samples detected in 2023, a two-thirds reduction from 2019. 93.6% of malware was polymorphic, evading detection. Machine-learning-powered tools are being adopted to detect commonalities between apps and known malware families. 45% of business and 53% of consumer PCs were reinfected within the same year. Successful cyberattacks affected 84.7% of surveyed organizations, down from 85.3% in 2021. [6].

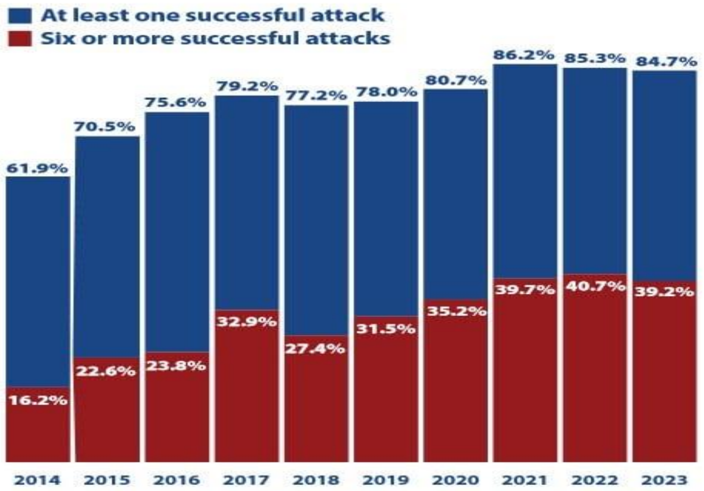

Figure 1: Percentages compromised by at least one successful attack and by six or more successful attacks.

2023 Cyberthreat Defense Report

Source: [7, p.1]

Kantar on behalf of Kantar Belgium in the 28 Member States of the European Union (EU) between 8 and 22 October 2019. The Directorate-General for Communication from the European Commission conducted face-to-face interviews with approximately 27,607 EU citizens from various social and demographic categories in their native language at home. Just over half of respondents (52%) think they are well informed about cybercrime, but only 11% say they feel very well informed. As was the case in 2018, there are still significant differences between countries. 80% of respondents in Denmark feel well informed, compared to 30% in Romania. Younger, longer-educated, and more financially secure respondents are the most likely to feel well informed. A study shows that 76% of respondents believe cybercrime risks are increasing, but 52% don't think they can protect themselves adequately. Only 22% are aware of official channels for reporting cybercrimes. While most countries believe that cybercrime risks are on the rise, only 15% of respondents feel that they can adequately protect themselves. At least 68% of respondents feel their online information isn't secure, and 78% avoid disclosing it online. Younger and longer-educated individuals perceive increasing cybercrime risks and confidence in self-protection, as they are more likely to perceive the need for increased security measures. The survey shows that 67% of respondents are concerned about cybercrimes, including bank card or online banking fraud, malware infection, identity theft, and hacking. Concerns about encountering child sexual abuse or promoting racial hatred or religious extremism have declined since Oct.-Nov. 2018. Half of the respondents are aware of someone who has experienced victimization, with the most common experience being the receipt of fraudulent emails or phone calls. Cybercrime victims often take action by contacting the police, a website, or a vendor. Over 37% of respondents protect children from online harassment. Fewer than one in five have reported a cybercrime or illegal online behavior. [8]. A Eurobarometer survey was conducted to gauge the awareness, experience, and perception of cybersecurity among EU citizens. 52% of respondents feel they cannot adequately protect themselves against cybercrime, while 52% are fairly or very well informed about it. Common concerns include bank card fraud, malicious software infection, and identity theft. 77% are unaware of reporting methods, and 70% do not report a cybercrime..[9].

Cybernetics is the scientific study and mathematical modeling of system regulation and control, encompassing biocybernetics, artificial intelligence, robotics, and systems science. [10].Cybercrime is a criminal activity involving computers, networks, or devices, often motivated by financial gain. It can be divided into three categories: crimes involving computing devices, using computers as weapons, and using computers as accessories. Common types include cyberextortion, cryptojacking, identity theft, and cyberespionage. Examples include DDoS attacks, malware, phishing campaigns, and illegal gambling. [11][12].

In early 2023, Jordan had 9.95 million internet users, with 88.0 percent penetration. Social media users accounted for 58.4% of the population, and there were 8.61 million cellular mobile connections. Internet usage increased by 6.8% between 2022 and 2023, but 12.0% of the population remained offline. The median mobile internet connection speed decreased by 2.76 Mbps, while fixed internet connection speeds increased by 21.10 Mbps. Government surveillance, online activity restrictions, and a new cybercrime law limit internet freedom in Jordan. Social media accounts account for 56% of the population, with LinkedIn, Snapchat, and Instagram being the most popular platforms. [13]. Jordan's internet users, comprising 88% of the population, have significantly impacted everyday life. Despite responsible precautions, a deviant subculture in cyberspace pollutes the online environment through criminal activities. The country recognizes cybercrimes as a social, political, legal, and health problem, offering victims reporting services and legal action options. Jordan experienced a surge in cybercrimes, with over 1103 crimes committed until November 2011. There have been 47 reported cases of impersonation, threats, financial fraud, and email theft since 2012.[14]. Jordanian prosecutors highlight cybercrime harassment as a significant issue, which can lead to potential consequences such as threatening victims, family breakdown, social decay, loss of values, skepticism, and security instability. [15]. Jordan's cybercrime issue requires further research to estimate prevalence and cause factors, aiding strategic plans, preventive measures, and awareness campaigns for safer university environments. Jordan has modernized cybercrime legislation since 2010, with the Cyber Crimes Act 2015 and the Cyber Crimes Act 2023. However, the Cybercrimes Act 2023 has sparked criticism from human rights organizations and activists. The law's potential impact on freedom of expression is crucial as Jordan navigates cybersecurity while upholding democratic values. [16].

LITERATURE REVIEW

Cybercrime: The concept

A literature review by Akdemir, Sungur, and Basaranel (2018) identifies two commonly used academic definitions of cybercrime: Thomas and Loader's 2000 definition of computer-mediated activities as illegal or considered illicit, and Gordon and Ford's 1996 definition of crimes facilitated using computers or hardware devices. Cybercrime, originating from cybernetics, has been dominant since 2000, primarily used for harmful activities like cyberbullying, cyberterrorism, and cyberstalking. However, a systematic approach is lacking. [17]Cybercrimes encompass a wide range of offenses and behaviors, and due to the diverse set of behaviors and rapidly expanding field, no comprehensive list exists. The number of instances increased from 1995 to 2000. The UN manual on computer-related crime (1994) uses the terms computer crime and computer-related crime interchangeably but does not provide a definition. The UNODC defines cybercrime as illegal behavior targeting computer systems and data processing, including offenses like computer-related fraud, forgery, and identity theft. The Tenth United Nations Congress defines illegal behavior targeting computer system security and data processing, including illegal possession and distribution of information through computer systems or networks, as part of its prevention and treatment of offenses. [18] **The Jordan Cybercrime Law No. 27 of 2015** criminalizes acts resulting from information technology intervention, punishable by law, and all laws in the Kingdom are in effect according to Article 15. [19] **The Jordanian Cybercrime Law No. 17 of 2023** criminalizes unauthorized access to information networks, fake accounts, misinformation, phishing, illegal donations, prostitution promotion, weapon information, possession of electronic data, creation of pornographic material, inciting prostitution, manufacturing weapons, and possessing electronic data without permission. The law also forbids the promotion or incitement of prostitution and immoral sexual behavior, as well as the acquisition of information related to weapons, ammunition, or explosives. The law also prohibits possessing electronic data, passwords, or access codes for committing crimes. [20]

Related Literature Review

A study by Solaka and Topaloglua (2015) found that gathering personal information and leaking it to third parties is a cybercrime, but sharing outdated content is acceptable. Students generally responded positively to privacy concerns and used parental control software to monitor their children's internet use. However, interdisciplinary undergraduate programs such as information technology law fall short, often emphasizing child pornography and cyber fraud. The study suggests that individuals should be aware of cybercrimes as classic crimes and social phenomena. [21]Another study by Ozdamli & Ercag (2019) reveals that adolescents are generally familiar with concepts like child pornography and computer and network security but are unaware of other types. Legal objections and obstacles hinder the definition and determination of cybercrimes. Adolescents are trying to protect themselves by not sharing account information and refraining from online shopping. Training sessions or seminars can help teach unfamiliar informatics concepts and enhance adolescents' protection. Researchers should work across the country to identify cybercrime profiles and determine training needs, allowing for the assessment of adolescents' awareness and organizing relevant activities. [22].

Cybercrime in Jordan is a growing issue, with a rise in cyber fraud, data breaches, online defamation, and financial crimes.Although the Jordanian government has enacted legislation to combat cybercrimes, critics continue to question its effectiveness. One million cases of cybercrime occur in Jordan each year, yet only 5% of these cases receive official reporting. The most common cybercrimes encompass threats, extortion, defamation, slander, and contempt. The incidence of online child abuse has escalated. Experts forecast that worldwide cybercrime expenses will amount to $6 trillion by 2021 and $10.5 trillion by 2025. Students at the University of Jordan exhibited differing degrees of awareness regarding cybercrime principles, legal regulations, and illicit activities. Male students exhibited greater awareness of cyber risks, potentially attributable to personal experiences or expertise. Studies indicate that adolescent boys exhibit diminished self-regulation, resulting in criminal behavior. Socialization affects irresponsible behavior, as Jordanian society permits males to partake in hazardous activities. Women possess a greater awareness of cybercrime legislation compared to men. ([23] [24][25]). Academic research on cyberspace and cybercrimes has been initiated since 2010 (i.e., [26][27][28][29][30][31])[32][33]

A study by Al-Badayneh (2025). The study examines factors affecting cyberbullying, victimization, and perpetration among college students in Jordan and revealed that 26% had experienced cyberbullying, 73% were aware of cyberbullying victimization, 80% were aware of cyberbullying perpetration, and 9% were aware of victims both on and off campus. The results indicated that factors such as gender, college, father's work, exposure to violence, lack of interest in life, suicidal ideation, anger, and low self-control significantly influence general cyberbullying, victimization, and perpetration. Over a quarter (26%) participated in fights and experienced cyberbullying, with a high prevalence of cyberbullying victimization and perpetration (73% and 76%, respectively). Cyberbullying has become a significant social and political issue worldwide, sometimes leading to youth suicide. Governments are concentrating their efforts on educational institutions to create programs aimed at combating cyberbullying in academic settings. Psychological support is crucial for students involved in cyberbullying attacks. Researchers attribute gender differences in general cyberbullying, cyberbullying victimization, cyberbullying perpetration, self-cyberbullying, vicarious cyberbullying, and low self-control to gender. Low self-control is a significant predictor of cyberbullying behavior, and students with low self-control are more likely to engage in cyberbullying than those with high self-control. Offline victimization and perpetration, or greater online time, mediate this association. The widespread prevalence of cyberbullying on campus should prompt university administration to take action on all levels, including policy formation, lawmaking, and preventive and victim programs. Law enforcement on university campuses and beyond is necessary due to the trans-organizational nature of cyberbullying behavior. [34]

METHODOLOGY

Sample. The study sample comprised 494 Jordanian students representing four Jordanian universities. Of these, 215 (43%) were males, and 258 (57%) were females. Students (19%) reported being victims of cybercrimes, and 24% were perpetrators.

Measurement

Students Perceptions Toward Jordanian Cybercrimes Law Scale. This scale is based on the literature review. It consists of 31 items covering all areas of Jordanian Cybercrimes Law. Interval levels 0–5 categorize the questions, with 0 to 5 being the most commonly used range. Reliability as estimated by the scale's Cronbach's α was 0.95, and the validity (correlation between the scale and LSC scale) was 0.309, α = 0.00, F = 11.981, α = 0.00.

Procedure and Data Collection

This quantitative study used the survey method on a sample of undergraduate students. The researchers provided informed consent to all students, requested their voluntary participation, and offered them the option to withdraw from the study at any time. The researchers also collected data by electronically sending the questionnaire to students for their completion.

FINDINGS

Table 1, [2]shows the percent of each item (agree and disagree) of students' perceptions of JCC. A quarter of the sample (26.9%) viewed the law negatively; of them, 10.7% were males and 16.2% were females. [1] Over 10% of the sample holds a negative perception of the cybercrime law, citing factors such as the exaggeration of defamation penalties, the expansion of judicial police officer authorization, the absence of preventive measures, and the neglect of cyberterrorism and cyberbullying. The law focuses on illegal entry

[2] The JCC treats agreement as a negative perception and views disagreement with the statement as a positive perception.

into government websites, neglects personal privacy, and violates freedom of expression. People no longer trust the law to prevent or manage cybercrimes.

Regressing, gender, net use, perpetration, knowledge, cyber extremism, and LSC explained 31% ($R^2 = .313$) of the variance in college students' perceptions toward Jordanian cybercrime laws. Table 2 showed that the overall effect of gender, net use, perpetration, knowledge, cyber extremism, and LSC was significant (F = 37.053, α = .000). Table 3 showed the unique contribution of each variable. Each variable significantly influenced college students' perceptions of Jordanian cybercrime law. except the gender.

Table 1 percent of agree and disagree of students perceptions of JCC

		% Male Agree	%Female Agree	% All Agree	% all Disagree
	Public security authorities can access the information and data.	2.4	2.2	4.7	95.3
	JCL was concerned with criminalizing all forms of expression of opinion	2.4	1.8	4.3	95.7
	Criminalized all forms of permissible criticism of affairs.	2	2	4	96
	The expansion of finding new criminal images that were unknown	3.2	6.7	9.9	90.1
	Conflicts with the strict penal policy of the Jordanian legislator	1.8	2.8	4.7	95.3
	Exaggerated the penalty for crimes of defamation ……	**3.4**	**6.7**	**10.1**	89.9
	Equated the completed crime with the attempted crime …	2.2	3.6	4.7	95.3
	Stipulated the penalty of temporary hard labor for the perpetrator ….	2.2	1.0	3.2	96.8
	Conflicts with the principle of criminal legality ...	2	2	4	96
	JCL has made it possible to charge a person merely for criticizing…	2.4	1.6	4	96
	Stipulates that anyone who commits any crime not provided …	3.2	2.2	5.5	94.5
	Conflicts with the principle of criminal legality	1.2	2.4	3.6	96.4
	JCL punishes mere intervention, participation, or incitement ….	4.5	5.5	9.9	90.1
	Expanded the authorization of judicial police officers…	**3.6**	**6.5**	**10.1**	89.9
	JCL did not rely on preventive and precautionary measures	**4**	**7.5**	**11.5**	88.5
	The Cybercrime Law uses broad, loose, and unspecified legal phrases	**3.6**	**7.3**	**10.9**	89.1
	JCL followed the traditional approach of criminal policy….	3	6.7	9.7	90.3
	Did not include a scientific or legal classification of cybercrimes.	**3.2**	**7.5**	**10.7**	89.3

	Did not distinguish between cybercrimes within the same category.	**4**	**7.3**	**11.3**	88.7
	Did not mention cyberterrorism and cyberbullying.	**3.6**	**6.9**	**10.5**	89.5
	The Cybercrime Law is perceived the basis that cybercrime is one.	**4.5**	**7.5**	**11.9**	88.1
	Focused on illegal entry into government websites and other activities.	**3.8**	**6.7**	**12.3**	89.5
	The Cybercrime Law neglected the breach of personal privacy	**4.7**	**7.7**	**12.3**	87.7
	The Cybercrime Law neglected the rights of victims.	**4.3**	**8.1**	**12.3**	87.7
	Neglected to guarantee and protect freedom of expression.	**4.9**	**7.1**	**11.9**	88.1
	The Cybercrime Law neglected violations of personal rights.	**5.1**	**7.1**	**12.1**	87.9
	Do you think the law has lost public confidence	**4.5**	**6.5**	**10.9**	89.1
	Do you think the law has lost political legitimacy?	**3.4**	**6.5**	**9.9**	90.1
	Do you think the law targeted public freedoms in cyberspace?	**4.5**	**7.5**	**11.9**	88.1
	Do you think the law will curb cybercrimes?	**4.7**	**7.7**	**12.3**	87.7
	Do you think the law will control cybercrimes?	**6.5**	**12.8**	**12.9**	80.8
	All	**10.7**	**16.2**	**26.9**	**73.1**

Table 2 ANOVA table testing the effect of gender, net use, perpetration, knowledge, cyber extremism and LSC on College Students Perceptions Toward Jordanian Cybercrimes Law

Source	Sum of Squares	df	Mean Squares	F	α
Between Groups	153227.384	6	25537.897	37.053	.000
Within Groups	335654.991	487	689.230		
Toala	488882.374	493			

Table 3 Coefficients

model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-7.612	5.517		-1.380	.168
Gender	.461	2.419	.007	.190	.849
Net Use	1.129	.279	.155	4.050	.000
Perpetration	-3.491	1.081	-.127	-3.230	.001

Knowledge	2.612	.667	.161	3.914	.000
Cyber Extremism	.608	.068	.371	8.942	.000
LSC	1.054	.238	.176	4.421	.000

CONCLUSION & DISCUSSION

Jordan's cybercrime rate is increasing, with an estimated one million incidents annually. A 2024 law regulates cybercrimes, but concerns about overcriminalization and politicization persist among college students. This supports humans. Amnesty concerns "Jordanian authorities are weaponizing the new Cybercrimes Law to target and harass journalists, activists, and others for expressing opinions online that are critical of government policies and practices, Amnesty International said today, marking one year since the law's adoption. [35].Another support came from Article: 19 "This law has proven to be a tool for state repression, stifling dissent and curtailing the human rights of individuals online, including the rights to freedom of expression, access to information, and privacy. The law has produced an environment of self-censorship and fear, shutting down one of the few remaining avenues for people in Jordan to engage in public debate and criticize public policies and authorities".[36, p. 1]

The study examines Jordanian college students' views on the Jordanian cybercrimes law, finding that 25% are aware of the law's politicization, 50% observe illegal online activities, and 26.9% view it negatively, with 10.7% males and 16.2% females. One common fact across the literature is that cyberspace is increasingly becoming a place not only for human interactions, but also for cybercrimes and cyber deviance. This goes in line with The space transition theory posits that individuals exhibit distinct behaviors when transitioning between different spaces, and that suppressed criminal behavior in physical space can lead to a greater inclination to commit crimes in cyberspace. Identity flexibility, dissociative anonymity, and the absence of deterrence factors in cyberspace give offenders the option to commit cybercrime. Intermittent ventures and the dynamic nature of cyberspace provide opportunities for escape. Closed society individuals are more likely to commit crimes in cyberspace than open society individuals. [37]. Students experienced victimization face to face or vicarious victimization.

Over 10% of the sample had a negative perception of the cybercrime law, which included exaggerated defamation penalties, expanded authorization for judicial police officers, a lack of preventive measures, and a neglect of cyberterrorism and cyberbullying. The law focuses on illegal entry into government websites, neglects personal privacy, and violates freedom of expression. The public no longer trusts the law to curb or control cybercrimes. Students viewed the law as a political and security tool to control their freedom.

Perception toward JCC was affected by several factors. including net use, perpetration, knowledge, cyber extremism, and low self-control. Together, these factors accounted for 31% of the variance in college students' perceptions of the Jordanian cybercrime law. Each variable was significant in its effect on college students perceptions toward Jordanian cybercrime law. However, gender had no significant effect, meaning that both males and females viewed the JCL the same.

The study recommends an integrated team for cyber lawmaking, which should include cybersecurity specialists, practitioners, criminal law experts, criminologists, and computer scientists. A need to include an evidence-based typology of cyber crimes that includes the most prevalent cyber crimes. Moreover, university students should be informed about technology and cybercrime risks. It suggests incorporating cybercrime concepts into academic activities and enhancing students' awareness of legal procedures. There is evidence that it can enhance prosecution facilitation and reduce criminal incidents. The Jordanian Cybercrimes Law defines cybercrimes like electronic defamation, libel, and slander, requiring a clear definition of what constitutes such an offense. [38]

REFRENCES

[1] Novikov, D. (2015). Cybernetics: from Past to Future. https://www.researchgate.net/publication/287319297_Cybernetics_from_Past_to_Future

[2] Silva, A., Burkhardt C., & Caneppele, S., (2020). Policy Brief No. 4 European Union's Horizon.

[3] European Commission (2024). Cybercrime. https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

[4] Wolf A., (2024). A Brief History of Cybercrime. https://arcticwolf.com/resources/blog/decade-of-cybercrime/

[5] Monroe University (2024). Cybersecurity History: Hacking & Data Breaches. https://www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches

[6] Zaharia, A. (2024). 300+ Terrifying Cybercrime and Cybersecurity Statistics – 2024 EDITION. https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

[7] Zaharia, A. 2024, p.1)

[8] Kantar Belgium (2020). Europeans' attitudes towards cyber security. Special Eurobarometer 499. European Commission, Directorate-General for Migration and Home Affairs and co-ordinated by the Directorate-General for Communication. https://europa.eu/eurobarometer/surveys/detail/2249

[9] Wahl, (2020). Eurobarometer: Europeans Attitudes towards Cyber Security.

[10] European Commission (2024). Cybercrime. https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

[11] Al-Badayneh, D. (2025). Factors Affecting Cyberbullying, Cyberbullying Victimization, and Cyberbullying Perpetration Among College Students. Journal of Legal and Security Studies.

[12] Al-badayneh, D. M. (2014). Cybercrimes: Definition and causes: Research paper for the Conference on New Crimes in Light of Regional and International Changes and Transformations, College of Strategic Sciences, Amman, Jordan.

[13] Al-Badayneh, D. (2025).. Journal of Legal and Security Studies.

[14] Almany, N. (2012). Criminal Investigation, Declining the Rate of Cyber-crimes, Addustour newspaper, Wednesday, March 28, Issue No. 16059, Forty-sixth Year, Amman, Jordan.

[15] Al-Khaza'leh, M., S., Lahiani, H. (2023). Cybercrime and Harassment: The Impact of Blackmailing on Jordanian Society as a Case Study. Journal of Intercultural Communication, 23(3), 116-123. doi.org/10.36923/jicc.v23i3.99

[16] Al-Badayneh, D., Khelifa M. & Aladra, I., (2024). A The Relationship Between Cyberbullying and Depression Among College Students.. 2024, 9(3): 000395. 1-7 https://medwinpublishers.com/article-description.php?artId=12839

[17] Akdemir, N.; Sungur, B.; Basaranel, B.U. (2020) . Examining the Challenges of Policing Economic Cybercrime in the UK. Güvenlik Bilimleri Derg. (Int. Secur. Congr. Spec. Issue) 2020, Özel Sayı, 113–134

[18] United Nations Office on Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime. Retrieved from [UNODC](https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf).

[19] The Jordanian Cybercrimes Law (No. 27 of 2015) page 5631 of the Official Gazette (No. 5343) dated 1 June 2015.

[20] Jordan Open Source Association (JOSA) (2023). Cybercrime Law of (2023). https://www.josa.ngo/publications/33

[21] Solaka D., &Topaloglua, M. (2015).The Perception Analysis of Cyber Crimes In View of Computer Science Students . Procedia - Social and Behavioral Sciences 182 (2015) 590 – 595 4th WORLD Conference On Educational Technology Researches, Wcetr.https://www.sciencedirect.com/science/article/pii/S1877042815030621/pdf?md5=c0a0e96aaedbc97d2e5144423f4daac0&pid=1-s2.0-S1877042815030621-main.pdf

[22] Ozdamli F. & Ercag, E., (2019). Knowledge Levels and Attitudes Toward Cybercrimes of Adolescents in Northern Cyprus. TEM Journal. Volume 8, Issue 4, Pages 1345-1350, ISSN 2217-

8309, DOI: 10.18421/TEM84-35. https://www.temjournal.com/content/84/TEMJournalNovember2019_1345_1350.pdf

[23] Al-Badayneh, D., Khelifa M. & Ben Brik, A. (2024A).

[24] Al-Badayneh, D., Khelifa M. & Ben Brik, A. (2024B). Cyberbullying and Cyberbullicide Ideation Among Jordanian College Students. International Journal of Cyber Criminology. Vol 18 Issue 1 . 58-82 https://www.temjournal.com/content/84/TEMJournalNovember2019_1345_1350.pdf

[25] Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The Influence of Cybercrime and Legal Awareness on the Behavior of University of Jordan Students. Heliyon. 10. e32371. 10.1016/j.heliyon.2024.e32371. https://www.researchgate.net/publication/381243039_The_Influence_of_Cybercrime_and_Legal_Awareness_on_the_Behavior_of_University_of_Jordan_Students

[26] Al-Badayneh, D., Al-Khattar, A. Al-Kresha R., and Al-Hassan, K.,(2012). Bullying victimization among college students (A transnational problem): A test of Agnew's General Strain Theory. The Homeland Security Review. Vol. 6, n2, 83-108

[27] Al-Badayneh, D., Al-Hagry, D., and Ben Brik, A., (2022), Cyberbullying, Victimization, Strains and Delinquency In Qatar. European Journal of Science and Theology, December 2022, Vol.18, No.6, 37-45. http://www.ejst.tuiasi.ro/Files/97/6_Al-Badayneh%20et%20al.pdf

[28] Al-badayneh, D. Al-Assasfeh, R. & Siddik Ekici (2023A). Developing A Robust Legal System Through Scale for Youth Extremism Across Arab Cultures. International Journal of Criminal Justice Science Vol 18 Issue 1, 29-51 https://ijcjs.com/menu-script/index.php/ijcjs/article/view/589

[29] Al-Badayneh, D., Ben Brik, A., and Elwakad, A. (2023b). A partial empirical test of the general strain theory on cyberbullying victimization among expatriate students. Journal Of Criminological Research, Policy And Practice. VOL. 10 NO. 1 2024, pp. 35-52. https://www.emerald.com/insight/content/doi/10.1108/JCRPP-03-2023-0013/full/html

[30] Al-Badayneh, D (2023c) Developing A College Students' Cyberbullying Scale. Open Access Journal of Criminology Investigation & Justice (OAJCIJ). https://medwinpublishers.com/OAJCIJ/developing-a-college-students-cyberbullying-scale.pdf

[31] Al-Badayneh, Diab M. (2024c). "Prevalence, Viewpoints, and Encounters With Cyberterrorism Among College Students". Journal of Ecohumanism 3 (3):1266-78. https://doi.org/10.62754/joe.v3i3.3437 . https://ecohumanism.co.uk/joe/ecohumanism/article/view/3437

[32] AlZeben, G., AlKharabsheh, A., (2021). Cybercrimes and the awareness of its danger field study on Jordanian university youth, Journal of the Islamic University of Human Research 29 (2). http://refhub.elsevier.com/S2405-8440(24)08402-0/sref27

[33] Al-Zoubi, M. (2023). "Crimes of Electronic Defamation, Libel, and Slander under Jordanian Cybercrimes Law", International Review of Law, Volume 12, Regular Issue 1, 2023

[34] Al-Badayneh, D. (2025). Journal of Legal and Security Studies.

[35] Human Amnesty, (2024). Jordan: New Cybercrimes Law stifling freedom of expression one year on.

[36] ARTICLE 19 (2024). Jordan: Marking a year of oppression, fresh calls to scrap Cybercrime Law. https://www.article19.org/resources/jordan-fresh-calls-to-scrap-cybercrime-law/

[37] Jaishankar K., (2007). Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology. Vol 1 Issue 2 July. (IJCC) ISSN: 0974 – 2891 Vol 1 (2): 7–9

[38] Al-Zoubi, M. (2023). "Crimes of Electronic Defamation, Libel, and Slander under Jordanian Cybercrimes Law", International Review of Law, Volume 12, Regular Issue 1, 2023