OPEN ACCESS

Scholars International Journal of Law, Crime and Justice

Abbreviated Key Title: Sch Int J Law Crime Justice
ISSN 2616-7956 (Print) |ISSN 2617-3484 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Differences in Students' Attitudes Towards Jordanian and Qatari Cybercrime Laws

Diab M. Al-Badayne[1]*, Hussen Alkubaisi[1], Abdulla Alsulaiti[1], Saleh Alkhowar[1], Ali Alkildi[1], Salman Almohannadi[1]

[1]Department of Security Studies, Graduate College, Police Academy, MOI, Qatar & KCRS, Amman, Jordan

DOI: https://doi.org/10.36348/sijlcj.2025.v08i05.002 | **Received:** 06.04.2025 | **Accepted:** 12.05.2025 | **Published:** 15.05.2025

***Corresponding author:** Diab M. Al-Badayne
Department of Security Studies, Graduate College, Police Academy, MOI, Qatar & KCRS, Amman, Jordan

Abstract

The study examines country and gender differences in attitudes toward Jordanian and Qatari cybercrime laws. The study sample comprised 704 participants from Jordan and Qatar, with 494 (70%) Jordanian and 210 (30%) Qatari. Of them, 377 (53.6%) were males, and 327 (46.4%) were females. Participants (143, 20%) reported being victims of cybercrimes, and 37 (5%) were perpetrators. The study developed a research questionnaire as its tool. As estimated by Cronbach's α, reliability was 0.956 for all scales. The validity, measured by the correlation between the attitude scale and knowledge index, was r = 0.180, α = 0.00. The ANOVA analysis comparing attitudes toward cybercrime law (ATCL) showed that students from Qatar had more negative views than those from Jordan (66 compared to 30); there were significant differences in ATCL between Jordan and Qatar (F = 237.579, α = .036). An ANOVA analysis of the mean gender differences in ATCL revealed that males were more negative about it than females (45 vs. 35). Significant differences were found between males and females in ATCL (F = 14.917, α < .000).

Keywords. Cybercrimes, law, Jordan, Qatar, Attitudes.

INTRODUCTION

Jordan and Qatar have a combined population of 10 million, primarily consisting of Arabs. Qatar's population includes 2.9 million Qatari nationals, predominantly Sunni Muslims, alongside a diverse expatriate community. Societies emphasize family values, hospitality, and religious coexistence (CIA World Factbook—Jordan, 2024; Wikipedia—Demographics of Jordan, 2024). With the rapid advancement of digital transformation in the Middle East, nations such as Jordan and Qatar are confronting an escalating threat from cybercrime. Both nations have advanced in adopting digital infrastructure, e-government services, and fintech; however, this advancement has also rendered them vulnerable to various cyber threats, including financial fraud, data breaches, cyber espionage, and online extremism. (CIA World Factbook—Qatar, 2024; Wikipedia, Demographics of Qatar, 2024).

In Jordan, the increase in internet penetration and smartphone usage has coincided with a significant rise in cyber-related offenses. The Jordanian government has implemented legal reforms, including the Cybercrime Law of 2015 (amended in 2018), which addresses online defamation, hacking, and identity theft. The legislation has faced criticism from human rights organizations for its potential to restrict freedom of expression. Qatar has established itself as a digital hub in the Gulf, particularly considering its preparations for global events such as the 2022 FIFA World Cup. The government has emphasized cybersecurity by establishing institutions such as the Qatar Computer Emergency Response Team (Q-CERT) and enacting the 2014 Cybercrime Prevention Law. Despite implementing various measures, Qatar faces threats, including phishing attacks, financial scams, and politically motivated cyber intrusions. Both nations build capacity and collaborate internationally to improve their cyber resilience. Challenges persist regarding public awareness, legal clarity, and the equilibrium between security and civil liberties. (Al-Badayneh, *et al*., 2024a, 2024b).

Cybercrime legislation in Jordan and Qatar reflects each country's approach to balancing digital security with civil liberties. Table 2 compares

cybercrimes in Jordan and Qatar. Cybercrime is a serious and severe problem in Jordan and Qatar, and further research is required to estimate its prevalence and causal factors. However, concerns about freedom of expression have led to the controversial Cybercrimes Act, which has sparked criticism. Analyzing the law's relationship with individual rights is crucial for navigating cybersecurity while upholding democratic values (Al-badayneh *et al*., 2024a, 2024b).

Table 1: Cybercrimes comparison between Jordan and Qatar

Aspect	Jordan (Cybercrime Law No. 17 of 2023)	Qatar (Cybercrime Prevention Law of 2014)
Year Enacted	2023	2014
Main Objectives	Combat online crimes, including hate speech, defamation, and false news.	Protect personal data, social values, and national security
Key Provisions	Criminalize false accounts. - Hate speech—defamation, Misinformation—Insulting religion - Pornography—promoting prostitution Publishing weapons -making info.	The law criminalizes publishing private information, even if it is true, spreading false news, and posing threats to national security.
Penalties	1 week to 3 years in prison—fines from JD 300 to 75,000 (approx. $423–$105,000)	Up to 3 years in prison—fines up to QR 500,000 (approx. $137,000)
Controversies	Vague terms affecting freedom of expression—LGBTQ+ rights concerns—used against protestors	Limits on press freedom—media censorship—chilling effect on journalists
Criticism From	UN, Human Rights Watch, EU	Gulf Centre for Human Rights, international media, NGOs
Use in Practice	Arrests for social media content, including pro-Palestinian activism	Used to suppress dissent, control media coverage, and restrict online speech
Total cases (2022)	16027	NA*
Incidents (2023)	2455	NA
Financial Losses (2023)	JD 150-200 million ($211-282 million USD	NA
Attacks (2023)	124	NA
Cases (2922)	133	NA

NA*=not publicly available

LITERATURE REVIEW

Jordan's Cyberattacks and Definition of Cybercrime Law

Jordan saw an 80% increase in cybersecurity incidents in 2023, with around 2,455 reported, compared to 1,362 in 2022. The National Cyber Security Center reported an 80% rise in incidents, attributed to enhanced threat detection capabilities, rapid digital transformation, and global cyberattacks. The cybersecurity landscape was dominated by financially motivated organized cybercrime and state-affiliated espionage activities. Jordan has made significant strides in digital transformation. The Cybersecurity Law was enacted in 2019, the establishment of the National Cybersecurity Center in 2021, and the formation of the National Cybersecurity Council. The center's responsibilities include licensing cybersecurity services, ensuring adherence to national standards, accrediting cybersecurity products, and setting guidelines for government-enterprise engagement. (Jordan News Agency, 2023). Jordan's Cybercrimes Law, enacted on 13 August 2023, broadens offenses and grants public prosecutors the power to prosecute individuals without personal complaints about governmental figures or entities. The law introduces harsh penalties for broad offenses. (Amnesty International, 2024). Cybercrime Law 17, 2023, defines cybercrimes as follows: The Cybercrime Law criminalizes various activities, such as gaining unauthorized access to information networks, creating fake accounts, spreading misinformation and phishing schemes, collecting donations without a license, promoting competitions without a license, creating pornographic material, inciting prostitution, manufacturing weapons, and possessing electronic data without permission. It also prohibits promoting or inciting prostitution, engaging in immoral sexual behavior, and obtaining information on weapons, ammunition, or explosives. The law also prohibits possessing electronic data, passwords, or access codes to commit crimes. (Jordan Open-Source Association (JOSA), 2023).

The law has progressed, but gaps exist in alignment with international standards like GDPR. Public perception shows mixed confidence in the law's effectiveness, suggesting improvements in legislative alignment and public awareness could enhance it. (Khwaileh, 2025). Research recommends that Jordanian legislators reconsider unfair legal texts for internet users, adopting balanced texts compatible with basic rights like information exchange, opinion expression, and privacy, as the Jordanian Constitution guarantees. (Al-Sarayreh, 2024).

Qatar's Cyber Threats and Definition of Cybercrime Law

Malicious groups are increasing the volume of cyberattacks, diversifying their types, and using

sophisticated tools. The global cyber threat landscape is unpredictable, with ransomware attack costs estimated at US in 2022 and data breach costs at US 4.35 million. Phishing and business email compromise are the costliest initial attack vectors. Qatar's increasing importance on the global stage makes it an attractive target for cyber threats, necessitating continuous enhancement of national cybersecurity capabilities and reducing exposure to potential cyberattacks or disruptions. According to the Qatar National Cyber Security Strategy, a cybercrime is "conduct or crime committed using technology. Examples of cybercrime may include illegal access to systems or information, fraud, identity theft, or content-related offenses such as spam.". Qatar has implemented several cybercrime laws, including the Cybercrime Prevention Law No. 14 of 2014 and the Personal Data Privacy Protection Law No. 13 of 2016. The country has also established policies and frameworks, such as the National Data Classification Policy and the National Information Assurance Standards, to ensure a robust Information Security Management System. Additionally, Qatar has developed the National Information Security Compliance Framework (NISCF) to enhance cybersecurity. (Qatar National Cyber Security Strategy 2024-2030).

METHODOLOGY

Sample

The study sample comprised 704 Jordanian and Qatari participants. Of these, 494 (70%) were Jordanian participants and 210 (30%) were Qatari participants. Of them, 377 (53.6%) were males, and 327 (46.4%) were females. Participants 143 (20%) reported being victims of cybercrimes, and 37 (5%) were perpetrators.

Measurement

Attitude toward Cybercrime Law Scale (ATCLS).

This scale is based on the literature review. It consists of 31 items covering all dimensions of cybercrime laws. The questions are measured on interval levels 0–5; the most common range is 0 to 5. As estimated by Cronbach's α, reliability was 0.956 for all scales. The validity, measured by the correlation between the attitude scale and knowledge index, was r = 0.180, α = 0.00.

FINDINGS

Table 2 compares attitudes toward cybercrime law between Jordan and Qatar. Qataris have a higher mean in criticizing cybercrime law than Jordanians in all items. The highest item was "*The Cybercrime Law was primarily concerned with ensuring that public security authorities have access to the information and data they require (3.2 vs. 0.82), and "The Cybercrime Law criminalized all forms of expression of opinion and permissible criticism of public affairs" (2.8 vs. 0.72).*

Table 2: Comparison of Attitudes toward Cybercrime Law between Jordan and Qatar

Item	Jordan		Qatar	
	mean	Sd	mean	Sd
The Cybercrime Law was primarily concerned with ensuring that public security authorities have access to the information and data they require.	0.82	1.3	3.2	1.6
The Cybercrime law criminalized all forms of expression of opinion and permissible criticism of public affairs.	0.72	1.2	2.8	1.7
The Cybercrime Law criminalized all forms of permissible criticism of affairs.	0.64	1.1	2.6	1.6
The Cybercrimes Law addresses the expansion of finding new criminal images that were previously unknown, aiming to restrict freedom of opinion and expression on the Internet.	1.0	1.5	2.7	1.6
The Cybercrimes Law exaggerated the penalty for crimes of defamation, slander, contempt, and character assassination, with a fine of up to 50,000 dinars.	1.0	1.4	2.1	1.6
The Cybercrimes Law equated the completed crime with the attempted crime in terms of punishment, which was severe for the person who committed the cybercrimes.	0.75	1.3	2.6	1.5
The Cybercrimes Law stipulated the penalty of temporary hard labor for the perpetrator of this crime.	0.56	1.1	2.6	1.5
The Cybercrimes Law conflicts with the principle of criminal legality in that it does not expand the interpretation of criminal texts against the interest of the accused.	0.64	1.2	2.3	1.5
Cybercrime law has made it possible to charge a person merely for criticizing the government or public authorities within the framework of permissible general criticism of public authorities.	0.54	1.1	2.5	1.6
The Cybercrimes Law mandates punishment for crimes involving information networks, technology, systems, or websites or for participating in or inciting their commission.	0.72	1.3	2.6	1.5
The Cybercrimes Law contradicts the principle of criminal legality by limiting criminalization to specific provisions and not making analogies or expanding interpretations that would be against the accused's interests.	0.86	1.1	2.5	1.5
The Cybercrime Law punishes mere intervention, participation, or incitement to commit cybercrime even if the crime does not occur.	1.2	1.5	2.5	1.5

Table 2: Comparison of Attitudes toward Cybercrime Law between Jordan and Qatar

Item	Jordan		Qatar	
	mean	Sd	mean	Sd
The Cybercrime Law increased the authority of judicial police officers to exercise judicial powers, thereby enhancing security but compromising judicial protection.	1.3	1.5	2.4	1.4
The Cybercrime Law did not rely on preventive and precautionary measures or alternative penalties, instead opting for custodial sentences.	1.3	1.5	2.2	1.5
The Cybercrime Law uses broad, loose, and unspecified legal phrases and terms.	1.3	1.5	2.4	1.4
The Cybercrime Law followed the traditional approach of criminal policy, based on expanding criminalization and severe, strict penalties.	1.4	1.5	2.3	1.5
The Cybercrime Law did not include a scientific or legal classification of cybercrimes.	1.3	1.5	3.3	1.5
The Cybercrime Law did not distinguish between cybercrimes within the same category.	1.4	1.6	2.4	1.5
The Cybercrime Law did not mention common crimes such as cyberterrorism and cyberbullying.	1.3	1.5	2.3	1.5
The Cybercrime Law is perceived the basis that cybercrime is one.	1.4	1.6	2.4	1.5
The Cybercrime Law focused on illegal entry into government websites and other activities.	1.3	1.5	2.5	1.5
The Cybercrime Law neglected the breach of personal privacy by others and government agencies.	1.4	1.6	2.1	1.5
Cybercrime Law neglected the rights of victims.	1.4	1.6	2.1	1.6
Cybercrime Law neglected to guarantee and protect freedom of expression.	1.3	1.5	2.1	1.5
The Cybercrime Law neglected violations of personal rights.	1.4	1.5	2.1	1.5
Do you think the law will curb cybercrimes?	1.4	1.5	2.3	1.4
Do you think the law will control cybercrimes?	1.7	1.7	2.7	1.5

Country Differences in Attitudes Towards Cybercrime Law

Tables 2 and 3 show Qatar's higher mean than Jordan and significant mean country differences in Attitudes Toward Cybercrime Law (F = 237.579, α =.000).

Table 3: Comparison between Jordan and Qatar in ATCL

Scale		N	Mean	SD
Attitudes	Jordan	494	30.1154	27.46550
	Qatar	210	66.2048	30.56143
	Total	**704**	**40.8807**	**32.85876**

Table 4: ANOVA analyses the mean country differences in Attitudes Toward Cybercrime Law

	Source of Variance	Sum of Squares	df	Mean Square	F	Sig.
Attitudes	Between Groups	191925.359	1	191925.359	237.579	.000
	Within Groups	567102.618	702	807.838		
	Total	**759027.977**	**703**			

Gender Differences in Attitudes Towards Cybercrime Law

Tables 5 and 6 represent ANOVA analyses of the mean gender differences in Attitudes Towards Cybercrime Law. Females were more supportive of CCL than males. Table 3 shows significant differences between males and females in CCL (F = 14.917, α =.000).

Table 5: Gender Descriptive statistics

Groups	N	Mean	sd
Males	377	45.2918	34.34570
Females	327	35.7951	30.32014
Total	**704**	**40.8807**	**32.85876**

Table 6: ANOVA table for the Gender Difference in Attitudes Towards Cybercrime Law

Source	Sum of Squares	df	Mean Squares	F	α
Between Groups	15792.801	1	15792.801	14.917	.000
Within Groups	743235.177	702	1058.740		
Total	**759027.977**	**703**			

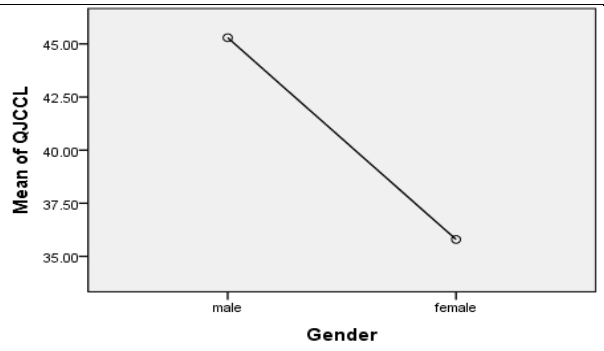

Figure 1: Gender difference in QJCCL

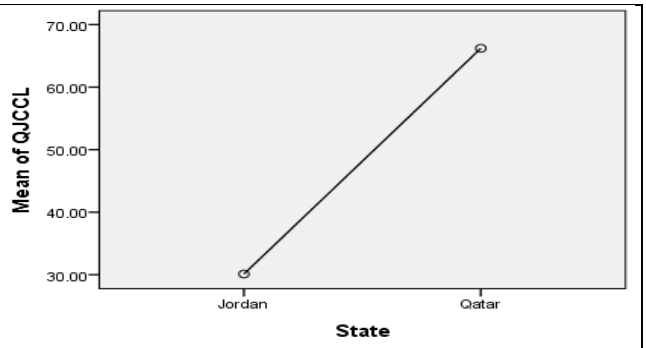

Figure 2: Country difference in QJCCL

CONCLUSION & DISCUSSION

The study examines countries (Jordan and Qatar) and gender differences in attitudes toward Jordanian and Qatari cybercrime laws. Participants (143, 20%) reported being victims of cybercrimes, and 37 (5%) were perpetrators. This finding indicates that cybercrime is a serious and severe problem in Jordan and Qatar, and further research is required to estimate its prevalence and causal factors.

The ANOVA analysis comparing attitudes toward cybercrime law (ATCL) showed that students from Qatar had more negative views than those from Jordan (66 compared to 30). Moreover, there were significant differences in ATCL between Jordan and Qatar in each single item. Qatari students view the law as restricting expression, while Jordanians may view its application as protecting security and stability. Qatari students are increasingly influenced by international universities that promote critical thinking and freedom of expression, leading to an increased inclination to criticize restrictive laws. The country's rapid technological advancements, hosting major global events, and cyberattacks have increased the circle of criticism and freedom of expression. Due to awareness campaigns and media attention, Qatari students are becoming more familiar with cybersecurity laws. However, Jordan's Cybercrimes Law, enacted in August 2023, has been used by authorities to target journalists and activists for critical online opinions. The law expands the scope of offenses and allows public prosecutors to initiate prosecutions without personal complaints. The law criminalizes forms of expression protected under international law (Amnesty International, 2024).

Students may be more reserved due to censorship or social restrictions, and there are shortcomings in the organization of obligations and penalties, delayed educational curricula, and institutional obstacles, resulting in a lack of student criticism of these laws. Smith *et al*. (2019) highlighted the importance of factoring in cultural and sociological contexts when considering gender and cyberbullying.

An ANOVA analysis of the mean gender differences in ATCL revealed that females were more supportive of cybercrime law than males. Significant differences were found between males and females in ATCL. The findings can be interpreted in the light of women's position and status in Jordanian and Qatari society. Females are more likely than males to be involved in cyberbullying as a victim (Foody *et al*., 2019; Marcum *et al*., 2012; Beckman *et al*., 2013; Heiman & Olenik-Shemesh, 2015; Smith *et al*., 2019; Al-badayneh *et al*., 2024a, 2024b). Cybercrime measurement is crucial for response, but variations in conceptualization, definitions, and legislation complicate the issue. We need a systematic approach to address evolving cybercrime. (Al-Badayneh, 2014; Phillips, 2022; Wall, 2010; Sarre, Lau, & Chang, 2018).

REFRENCES

- 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.
- Al-Badayneh, D. M. ., Dosari, H. M. A. ., Qahtani, H. M. A. ., Alkhater, J. A. ., & Mehawesh, S. S. . (2024a). College Students' Attributional Differences in Knowledge Awareness about Cybercrime Law . Journal of Ecohumanism, 3(6), 773–786. https://doi.org/10.62754/joe.v3i6.4046
- Al-Badayneh, D. M. ., Mehawesh, S. S. . Dosari, H. M. A. .& Qahtani H., (2024b). The Relationship between Knowledge Awareness about Qatari Cybersecurity Law, Victimization, and Perpetration Experience: Some Applications of Routine Activities Theory. Contemporary Readings in Law and Social Justice ISSN: 1948-9137, e-ISSN: 2162-2752Vol 16 (1), 2024pp. 1115-1128https://www.crlsj.com/index.php/journal/article/view/272/127
- Al-Sarayreh, R. (2024). Jordanian Cybercrime Law No. (17) of 2023 between Regulating Social Media Sites and Restricting Freedom of Opinion. Sch Int J Law Crime Justice, 7(9): 339-351.
- Amnesty International (2024). Jordan: New Cybercrimes Law stifling freedom of expression one year on.
- Beckman, L., Hagquist, C., and Hellström, L. (2013). Discrepant gender patterns for cyberbullying

and traditional bullying-An analysis of swedish adolescent data. Comput. Hum. Behav. 29, 1896–1903. doi: 10.1016/j.chb.2013.03.010

- CIA World Factbook – Jordan (2024). https://www.cia.gov/the-world-factbook/countries/jordan/
- CIA World Factbook – Qatar (2024). https://www.cia.gov/the-world-factbook/countries/qatar/
- Foody M, McGuire L, Kuldas S and O'Higgins Norman J (2019) Friendship Quality and Gender Differences in Association With Cyberbullying Involvement and Psychological Well-Being. Front. Psychol. 10:1723. doi: 10.3389/fpsyg.2019.01723
- Heiman, T., and Olenik-Shemesh, D. (2015). Cyberbullying experience and gender differences among adolescents in different educational settings. J. Lear. Disabil. 48, 146–155. doi: 10.1177/0022219413492855
- Jordan News Agency (2024). Cybersecurity Incidents in Jordan Surge by 80% in 2023.
- Jordan Open Source Association (JOSA), (2023). Full Text in English of the Cybercrime Law of 2023. https://www.josa.ngo/publications/33
- Khwaileh, K. (2025). Public Perceptions of Jordan's Cybercrime Law: Protecting Social Media Data and Aligning with International Standards. Pakistan Journal of Life and Social Sciences. 23(1): 2947-2955. https://doi.org/10.57239/PJLSS-2025-23.1.00233
- Marcum, C. D., Higgins, G. E., Freiburger, T. L., and Ricketts, M. L. (2012). Battle of the sexes: an examination of male and female cyberbullying. *Int. J. Cyber Criminol.* 6, 904–911.
- McGuire, M. It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In The Human Factor of Cybercrime; Leukfeldt, R., Holt, T.J., Eds.; Routledge: New York, NY, USA, 2020; pp. 3–28.
- National Cyber Crime Reporting Portal. (2019). Retrieved November 24, 2023, from https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1703509
- Phillips, K., *et al*. (20220. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sci.* 2022, *2*(2), 379 398; https://doi.org/10.3390/forensicsci2020028. https://www.mdpi.com/2673-6756/2/2/28
- Sarre, R.; Lau, L.Y.C.; Chang, L.Y. Responding to cybercrime: Current trends. Police Pract. Res. 2018, 19, 515–518
- Smith, P. K., López-Castro, L., Robinson, S., and Görzig, A. (2019). Consistency of gender differences in bullying in cross-cultural surveys. Aggress. Violent Behav. 45, 33–40. doi: 10.1016/j.avb.2018.04.006
- Wall, D.S. The Internet as a Conduit for Criminals. In Information Technology and the Criminal Justice System; Pattavina, A., Ed.; Sage: Thousand Oaks, CA, USA, 2005; pp. 77–98, (Chapter revised March 2010).
- Wall, D.S.(2001). Introduction: Cybercrime and the Internet. In Crime and the Internet; Wall, D.S., Ed.; Routledge: New York, NY, USA, pp. 1–17.
- Wikipedia - Demographics of Jordan (2024). https://en.wikipedia.org/wiki/Demographics_of_Jordan
- Wikipedia -Demographics of Qatar (2024). https://en.wikipedia.org/wiki/Demographics_of_Qatar