AL-BIRUNI

Al-Biruni Journal of Humanities and Social Sciences
Vol. 04, No. 06, 2026, pp. 28-41
ISSN 3104-8900
https://al-biruni-journal.jo

Digital Administrative Policing and Its Role in Regulating Cyberspace: A Comparative Study between Jordan and Indonesia

Saleem Asouli[1*]

[1] Assistant Professor, Ajloun National University- Jordan, Corresponding Author's Email: saleem.asouli@anu.edu.jo , ORCID: https://orcid.org/0009-0006-4132-8194

Corresponding Author: Saleem Asouli, saleem.asouli@anu.edu.jo

DOI: https://doi.org/10.64440/BIRUNI/BIR0028

ARTICLE INFO

Article history
Received Feb 06, 2026
Revised Feb 10, 2026
Accepted June 18, 2026

Keywords

Cyber Surveillance;
Cyber law;
Cyber Warfare;
Digital Transformation;
The Hashemite Kingdom of Jordan;
The Republic of Indonesia.

ABSTRACT

This study aims to analyze the concept of electronic administrative policing as a contemporary development of the administrative policing function in light of rapid digital transformation and the migration of threats to public order into cyberspace. The study argues that, despite differing from traditional administrative policing in terms of technological tools and scope of application, electronic administrative policing retains its fundamental preventive function of safeguarding public order and preventing disturbances before they occur. Adopting a juxtaposition legal approach, the research examines the legal framework governing Cyber Surveillance, including cybercrime legislation, personal data protection regulations, and rules issued by competent regulatory authorities in the Hashemite Kingdom of Jordan and the Republic of Indonesia. Particular emphasis is placed on the challenge of balancing the expansion of administrative discretionary powers with the protection of digital rights and fundamental freedoms. The study further explores the legal and technical characteristics of Cyber Surveillance, highlighting its preventive nature, its subjection to the principle of legality, and its reliance on advanced technological instruments such as electronic surveillance systems, artificial intelligence technologies, data analytics, encryption mechanisms, and digital content blocking measures. It also analyzes legal and technical responses to digital violations, including early warning mechanisms, content removal, account suspension, financial penalties, and, where necessary, the potential combination of administrative and criminal liability. The study concludes by addressing implementation mechanisms, as adopted in International best practices for Cyber Regulations arising from unlawful acts in cyberspace, including compensation, restitution, guarantees of non-repetition, international sanctions, mediation, and arbitration, thereby contributing to strengthening the legal governance of the digital environment.

1. Introduction

Twenty-five years after War Games, cyber surveillance remains somewhat of a mystery. Specifically, is Cyber hacking a threat to national security? The answer lies in the history of humanity's conquest of the oceans, skies, and outer space. The first arrivals are explorers, who can hardly be blamed for their actions. But as settlement and commerce begin to flourish, criminals, competitors, and enemies appear, by arrival or by birth. Cyber-space is no different. Political and military adversaries, alliances, and soldiers from every international conflict on Earth already inhabit it. The article provides a brief introduction to

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 06, 2026, pp. 28-41
ISSN 3104-8900

cyber warfare. Introduction to the Issue: Wars frequently leverage new technological advancements. They might be smaller, incremental developments, such as more accurate traditional kinetic weapons like rifles or missiles, or new types or improved vehicles like drones or stealth bombers. However new and improved, these kinds of weapons are basically means of achieving the same goals as before – in many ways, it is trivial whether a missile is launched from a traditional fighter jet, a ship, or an unmanned drone piloted from afar. These developments are rarely uncontroversial, either in a legal or moral sense. Calls of cowardice met the introduction of firearms: instead of bravely meeting and fighting within arm's and sword's length, the musket allowed for inflicting death and damage from a distance [1].

By the late twentieth century, ballistic missiles made it possible to strike targets beyond the horizon, and now much debate revolves around uncrewed aerial vehicles, also known as drones. The laws of war adapt to new technological developments. In 1868, the Saint Petersburg Declaration banned the use of explosive projectiles weighing less than 400 grams. Since then, numerous treaties have been concluded to regulate or completely ban the use of various weapons. Especially modern Western societies are highly networked and reliant on Personal Computers in nearly everything, ranging from hospitals to factories and from banks to nuclear reactors. Lest there be any doubt about the pervasiveness of connected devices, in August 2013 the security company Trustwave issued a security advisory after it found a vulnerability in a toilet seat; because of lax security, a malicious user could use a smartphone to open or close the lid, flush the toilet, or activate air-drying [2]. The connectivity of devices provided an unimaginable attack surface just a couple of decades ago. States have increasingly focused on securing critical infrastructure against cyber-surveillance but have also considered the need for offensive capabilities. A state-run Cyber army carrying out cyber-surveillance with direct consequences in the physical world has come far from the stereotype of the 1990s: an individual malicious Cyber enthusiast or a group writing viruses to claim fame among their peers. Even though Cyber operations have not so far played a major part in any larger conflict, it has been widely claimed that several countries are faced with vulnerable systems and that it might only be a matter of time until an enemy; be it a state or a non-state actor such as a terrorist group – uses its Cyber capabilities either as the primary way of attacking or as a supplementary way to wreak havoc. The consequences of such Cyber-Surveillance are by no means limited to the virtual world and may very well be significant for both civilians and soldiers. Cyber-Surveillance has several characteristics that distinguish it from traditional uses of force, with implications for applying the existing legal framework to it.

A Cyberattack might last only a fraction of a second, and its source might be masked. The legal framework has its roots in the more traditional ways of waging war between nation-states. Some of the problems emanating from Cyber-Surveillance follow the same lines of thought as the issues discussed after the terrorist Cyber-Surveillance of 11 September 2001 (hereafter referred to as the 9/11 Cyber-Surveillance), regarding, among other things, non-state actors and the possibility of pre-emptive self-defense. Cyber warfare has been a hot issue, especially after the events in Estonia in 2007 and the discovery of Stuxnet, both of which will be introduced in the following pages. The dangers of cyber surveillance have

even been compared to the consequences of nuclear war with hyperbolic tones [3]. Although the worst-case cyber scenarios may indeed include consequences comparable to nuclear war, focusing on them tends to misguide the discussion away from the arguably more common and more probable consequences of Cyber operations. The erstwhile Director of the CIA, Michael Hayden, rarely states so clearly; hence, this phenomenon has been communicated with less clarity and less apparent understanding than it warrants [4]. Although the discussion about Cyber-Surveillance has been especially lively recently, Cyber-Surveillance and the threats themselves are not entirely new [5].

In 1993, John Aquila and David Ronfeldt envisioned that information technology would be the technological breakthrough that would bring about the 'next major shift like conflict and warfare'[6]. The laws of war are not the only aspect of law being challenged by technological changes [7]. The possibility of making exact copies of digital media and easily disseminating them has challenged conventional conceptions of copyright, and the possibility of gathering data on an unimaginable scale poses a new kind of test for the protection of privacy, to name two obvious examples. On a broader scale, the diminishing significance of national borders brought about by the internet makes it more difficult to apply the traditional concept of territorial jurisdiction [8].

Whatever the challenges may be, they neither mean that the technology is immune to the legal system nor that the legal system is immune to the technology [9]. The same applies to jus ad bellum – the law concerning the resort to force by states – and Cyber operations: the existing rules apply [10]. Still, they may need to be interpreted in new ways and supplementary new rules may need to be agreed upon. In this book, I will examine the relationship between cyber operations and current international law in terms of jus ad bellum. First, I shall discuss the terminology regarding the subject and present a parallel case which I will later refer to. Hitherto, the history and evolution of the regulation of war will be examined, from the bellum justum doctrine to the current system built around the United Nations Charter [11]. Then the much-debated notions of force and armed attack will be examined, both of which are essential to the question of the legality of military action. There is no agreed-upon definition of either term, and both will be discussed in the context of Cyber operations. The aim is to determine if and when Cyber operations may constitute a use of force or an armed attack.

2. Background

The world today is witnessing a wave of digital transformation, leading to new behavioral patterns and risks in cyberspace. This has compelled public administration to develop its tools and methods to preserve public order. Traditional administrative control alone is no longer sufficient to address the challenges posed by cybercrimes, data breaches, the dissemination of illegal content, and other cybersecurity threats, creating a pressing need to establish a Cyber Surveillance system as a modern extension of administrative powers in the digital domain.

This study aims to clarify the concept of Cyber Surveillance, outline its legal basis, and examine its legal and technical characteristics. It also highlights the mechanisms used by

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 06, 2026, pp. 28-41
ISSN 3104-8900

public authorities to monitor digital activities and curb electronic violations. Furthermore, the research addresses the remedial and punitive measures adopted in response to transgressions within cyberspace, as well as the mechanisms for enforcing international responsibility when unlawful acts have cross-border effects.

Accordingly, this study seeks to provide a comprehensive framework for understanding the role of Cyber Surveillance as one of the most important tools for protecting digital security and public order amid rapid technological development.

Introduction to the Jordanian Cyber Laws

The legal structures governing digital media in the Hashemite Kingdom of Jordan, including aspects of freedom of speech, privacy, and online governance. Hitherto, for the past decade, Jordan has witnessed the development of various laws to address emerging issues such as cybercrime, misinformation, and data protection. The Cybercrime Law No. 17 of 2023 in Jordan is a major reform, as it criminalizes online character assassination. Still, it also reflects a wider regional trend of prioritizing state security at the expense of digital rights [12]. The concept of *"digital rights"* emerged alongside contemporary human rights discourse, as international organizations advocated for their recognition. Henceforth, it is incumbent upon the government in Jordan to acknowledge, protect, and impartially ensure these rights through promulgation. Albeit, digital rights face complex challenges spanning legislative, political, and technical domains. Thus, regulatory mechanisms are crucial in upholding these rights while addressing societal concerns such as public order and morality [13].

Cybersecurity has become vital due to the increased use of modern technology and global connectivity, which has resulted in the infiltration and surveillance of information systems. This has enabled terrorist organizations to exploit relevant information, thereby exposing vulnerabilities in international protection systems. Cyber-surveillance has significant economic and social impacts on nations, affecting their security and social systems. Therefore, the global community must collaborate to safeguard cybersecurity and preserve it. There is a growing interest in cybersecurity in the Hashemite Kingdom of Jordan. This study has also proven impactful, offering significant implications and enhancing its overall effectiveness by motivating policymakers and government officials to develop and enforce robust cybersecurity policies and laws to mitigate cyber-surveillance [14].

Jordan's regulatory framework navigates the tension between international human rights standards, specifically Article 19 of the ICCPR, and domestic security logics. The analysis identifies a paradigm shift towards the protection of digital speech, characterized by: (i) the use of imprecise legal definitions that allow for the criminalization of political criticism; (ii) the imposition of penalties that prioritize state security over individual expression; and (iii) a state-centric interpretation of digital sovereignty. Thus, an analysis of judicial precedents, such as the Court of Cassation Decision No. 6280/2022, reveals that authoritarian regimes use legalistic justifications to manage digital dissent. By positioning Jordan's legislative evolution as a case of Coordinated Digital Governance, we can argue

that authorities are stricter than in neighboring countries, given Jordan's geopolitical landscape [15].

Jordan Court of Cassation Decision No. 6280/2022 is a landmark legal precedent concerning digital dissent and "fake news," the criminalization of fake news under the 2023 Jordanian Cybercrime Law, and the evaluation of its implementation within the broader global canon of fake news law analyses [16]. The court convicted a Twitter user for posting corruption allegations against a public official, concluding that the posting of verifiable public records could still be conflated with false news and punishable as speech [17]. Criminalizing Legitimate Criticism, through this decision, sets a precedent that conflates political criticism and allegations of public corruption with the distribution of "false news." The Legal Ambiguity refers to the fact that, by enforcing Article 15(a) of Jordan's cybercrime framework [18], the court demonstrated how textual ambiguity can be exploited to prosecute citizens for online speech. International Human Rights Concerns were raised through the legal researchers' identification of this decision as a key example of how Jordanian authorities prioritize state security and information control over international standards on freedom of expression [19]. In the broader legal context, this decision is often analyzed alongside Jordan's subsequent legislation to track the criminalization of online speech. The ruling highlights how the Jordanian state manages digital dissent through the judiciary [20].

The Indonesian laws on Cyber surveillance

The Republic of Indonesia is located in the ASEAN region and is a well-developed jurisdiction in terms of cyber law [21]. Indonesia's legal framework, including the 1945 Constitution, the Electronic Information and Transactions Law (ITE Law), and the Personal Data Protection Law (PDPL), allude to the comprehensive Indonesian laws on cyber surveillance which are primarily governed by the Electronic Information and Transactions (EIT) Law (Law No. 11/2008, as amended by Law No. 1/2024) and the Personal Data Protection (PDP) Law (Law No. 27/2022). These frameworks generally prohibit unauthorized interception and data access, but provide major exemptions for state surveillance and law enforcement [22]. Hitherto, while citizen privacy is protected, the government retains broad powers to conduct cyber surveillance for national security and criminal investigations. Law Enforcement Access is under the EIT Law and related Ministry of Communication and Informatics (Kominfo) regulations; Electronic System Providers (ESPs) are legally mandated to grant law enforcement authorities access to electronic data for the investigation of crimes carrying a minimum sentence of two years' imprisonment [23].

Furthermore, Intelligence and Security fall under the jurisdiction of the State Intelligence Law, which grants agencies such as the State Intelligence Agency (BIN) broad authority to intercept and monitor communications to prevent and combat threats to national security [24]. Another form of cyber surveillance is through Wiretapping Agreements, in which the Attorney General's Office (AGO) routinely partners with major telecommunications operators to mandate the installation of direct wiretapping and data-exchange devices to track suspects [25].

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 06, 2026, pp. 28-41
ISSN 3104-8900

If identity theft involves personal data, it also breaches Articles 67(1), 67(2), and 68 of Law No. 27 of 2022 regarding Personal Data Protection ("PDP Law"). The PDP Law prohibits the unlawful collection, use, or falsification of personal data, with criminal sanctions of up to six years' imprisonment and/or a fine of up to IDR 6 billion, along with potential additional penalties such as asset confiscation and compensation payments [26].

In several cases, the courts have imposed sentences ranging from one to two years' imprisonment and/or fines of IDR 10–50 million; however, in Decision No. 479/PID.SUS/2025/PT SMG, the defendant was found guilty under Article 68 of the PDP Law for creating or falsifying personal data to benefit himself and harm others. He was sentenced to four years' imprisonment and fined IDR 1 billion [27].

3. Discussion and Analysis

Ever since Barlow's 1996 article, cyberspace has received enormous applause from the general public. As a result, Cyberspace got a place in Webster's dictionary by the year 1997. Technopedia defines cyber Attack as,

"A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises, and networks. Cyber-surveillance uses malicious code to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. A cyberattack is also known as a computer network attack (CNA)." [28]

"Cyber warfare" has become an ominous catchphrase used especially in the media and in international law, in a variety of contexts, not all of which are appropriate or fitting [29]. It is very often referred to in situations more aptly described as espionage, be that commercial or targeted at military intelligence. Just as often, it is used to describe activities of smaller scale with consequences that have little to do with warfare, as in the case of the Cyber-Surveillance against Estonia in 2007 [30]. We will go through some of the terminology and definitions used in discussing the subject matter, as well as argue for the researcher's strengths and weaknesses. 'Information warfare' has been used to describe Cyber-Surveillance and operations carried out via Cyber networks. However, it seems that lately the term has been more or less replaced by the notion of Cyber-Surveillance. Information warfare more aptly describes the battle of words and images [31]. Hence, the term has more to do with propaganda than with what now is referred to as Cyber operations. This is also how information warfare has previously and widely been understood [32].

According to Checkpoint, a leading IT Observer on the Internet, cyber-surveillance is defined as the following:

"Cyber-Surveillance is a strike against a computer system, network, or internet-enabled application or device. Hackers often use a variety of tools to launch Cyber-Surveillance, including malware, ransomware, exploit kits, and other methods." [33]

Consequently, some of the newer Cyber-Surveillance developments into the concept of information warfare are problematic. It is theoretically possible to stretch the definition of information so that the target of Cyber-Surveillance is indeed the information resident in the memory of Cyberspace, but it is forced and far-fetched [34]. Also, it does not seem practical to group traditional information warfare (such as propaganda) with newer forms of attack, such as those targeting industrial control systems, whose objectives and outcomes are very different. Cyber-Surveillance of the network infrastructure would more readily fall under the concept of information warfare, especially if its ultimate aim is to disrupt the flow of information. Indeed, the communications networks were seen early on as probable targets of Cyber-Surveillance [35]. It has also been argued that Cyber operations and Cyber network Cyber-Surveillance should be understood as one of the main capabilities of information warfare [36]. This is a reasonable claim from the perspective of information warfare, yet it should be clarified that it applies only to Cyber operations whose goals pertain to information warfare. Not all Cyber operations have such goals, and those that do not (such as an attack on the air traffic control system intended to crash aircraft or an attack on industrial control systems intended to cause an explosion) should not be forced into the category of information warfare [37]. The term 'Cyber network attack' (CNA) is also frequently used. This is often an apt term, but in some cases it seems too strict about the network aspect. Some critical infrastructure might be disconnected from the internet or other networks as part of security measures. Yet, these systems can very well be – and have been – targeted by a Cyberattack. For instance, one of the main propagation methods of the Stuxnet malware, which hit an Iranian nuclear facility, was spreading via removable USB drives [38]. The use of the term 'Cyber network attack' also seems to be declining in favor of 'Cyber Surveillance'[39].

A juxtaposed comparative analysis of the cyber surveillance of Jordan and Indonesia

Jordan and Indonesia both have comprehensive cyber law frameworks. Still, Jordan's 2023 Cybercrime Law has drawn criticism for restricting free speech, while Indonesia's ITE Law (2008, amended 2024) emphasizes electronic transactions and data protection with harsher penalties for hacking and phishing [40]. In the case of Indonesia: Stronger focus on digital commerce and personal data protection. The ITE Law provides harsher penalties for hacking and phishing. However, its defamation provisions have also been criticized for misuse against dissent, as Indonesia's cyber laws prioritize digital commerce and personal data and impose harsher cybercrime penalties yet face criticism for restricting freedom of expression [41].

The key difference lies in Jordan's focus on national security and speech regulation versus Indonesia's emphasis on digital commerce and personal data protection [42]. Jordan places strong emphasis on national security and speech regulation. The 2023 Cybercrime Law broadens the range of punishable offenses but risks curtailing freedom of expression, as Jordan's cyber laws prioritize national security and control

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 06, 2026, pp. 28-41
ISSN 3104-8900

over online speech while lagging in personal data protection. Data protection remains underdeveloped (a draft law is pending) [43].

The researcher has drafted the following table to explain the paradoxical relationship of cyber laws between the two jurisdictions:

Table (1) Comparative Analysis of Cybercrime Legal Frameworks in Jordan and Indonesia

Aspect	Jordan	Indonesia
Core Cybercrime Law	Cybercrime Law No. 17 (2023) – replaces the 2015 law. Covers hacking, identity theft, online fraud, defamation, fake news, cyberstalking, and harassment. Penalties: up to **3–5 years imprisonment** and fines.	Electronic Information and Transactions Law (ITE Law) No. 11 (2008), amended by Law No. 1 (2024). Covers hacking, denial-of-service, phishing, and manipulation of electronic data—penalties: up to **12 years imprisonment** and fines up to **IDR 12 billion**.
Data Protection	Draft Data Protection Law (pending since 2021). Modeled on the GDPR, includes consent-based processing, individual rights, and cross-border transfer rules.	Permenkominfo No. 20/2016 on Personal Data Protection in Electronic Systems. Requires organizations to adopt strict security measures.
Electronic Transactions	E-Transactions Law No. 15 (2015). Recognizes e-signatures, digital contracts, and regulates e-commerce.	ITE Law also governs electronic transactions, ensuring validity of e-documents and contracts.
Cybersecurity Framework	Cyber Security Law No. 16 (2019). National Cybersecurity Center (NCSC) oversees defense, incident response, and critical infrastructure protection.	National Cyber and Encryption Agency (BSSN) oversees national cyber defense. Works with ASEAN on regional cooperation.
Free Speech & Controversy	2023 law criticized for vague definitions of defamation and fake news, potentially restricting journalists and activists.	ITE Law criticized for broad defamation and online speech provisions that are often used against critics and activists.
International Cooperation	Aligns with Budapest Convention principles but is not a signatory. Active in UNODC and INTERPOL initiatives.	Member of ASEAN cybersecurity cooperation, promoting regional best practices.

Findings

1 . The study confirms that Cyber Surveillance has become an urgent necessity in light of digital transformation and the growing prevalence of cyber risks, as traditional control mechanisms are no longer sufficient to address challenges arising within cyberspace.

2 . Jordan is primarily focused on enhancing its security measures and implementing strict speech control regulations. This approach aims to ensure national stability and control the flow of information within the country. In contrast, Indonesia prioritizes promoting commerce while emphasizing data protection. The country aims to foster economic growth through trade while safeguarding its citizens' personal information and privacy in an increasingly digital world. The legal framework governing Cyber Surveillance in Jordan remains in a developmental phase. Despite the existence of significant legislation, such as the Cybercrime Law and the Personal Data Protection Law, practical application demonstrates the need for organization.

3 . Cyber Surveillance is characterized by a clear preventive nature, aiming primarily at preventing digital violations through electronic monitoring, content blocking measures, and early-warning systems, in both jurisdictions.

4 . Public administration enjoys broad discretionary powers in exercising electronic control, granting flexibility in addressing digital risks while simultaneously raising concerns relating to excessive surveillance and potential infringement of users' rights.

Technological tools play a central role in strengthening administrative capacity to detect violations.

5 . Digital monitoring systems, encryption technologies, artificial intelligence applications, and data analytics.

6 . A continuing challenge exists in achieving equilibrium between protecting public order and safeguarding digital rights and freedoms, especially with the expansion of electronic monitoring and content restriction practices.

7 . International responsibility increasingly intersects with Cyber Surveillance, particularly where unlawful digital activities extend across borders, making compensation, restoration, and guarantees of non-repetition essential mechanisms for addressing digital harm.

Recommendations

1 . Developing a more comprehensive legislative framework governing Cyber Surveillance that clearly defines administrative powers, prevents abuse, and guarantees protection of citizens' digital rights.

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 06, 2026, pp. 28-41
ISSN 3104-8900

2 . Strengthening judicial oversight over electronic administrative decisions, particularly those relating to surveillance and website blocking, to ensure compliance with the principle of legality.

3 . Enhancing the technical capabilities of administrative authorities through continuous professional training in digital monitoring and analytical technologies to improve preventive effectiveness.

4 . Adopting clear policies for digital privacy protection by defining the categories of data that administrative authorities may lawfully collect, process, and retain, in accordance with proportionality and necessity principles.

5 . Promoting international cooperation in combating cross-border cyber risks through information exchange agreements and coordinated regulatory mechanisms.

6 . Expanding digital awareness programs aimed at individuals and institutions to foster a culture of cybersecurity and responsible digital behavior.

7 . Encouraging the integration of artificial intelligence governance standards within administrative practice to ensure transparency, accountability, and protection against algorithmic bias in electronic control decisions.

Conclusion

This study has demonstrated that Cyber Surveillance has become an organizational necessity imposed by the nature of cyberspace and the risks it generates, which exceed the capacity of traditional administrative control mechanisms. The findings reveal that the effectiveness of Cyber Surveillance depends primarily on the existence of a clear legal framework and on the administration’s reliance on advanced technological tools capable of ensuring preventive and efficient protection of digital public order.

Through a comparative analysis of the Cyber Laws of Jordan and Indonesia, we recognize the need to strike a careful balance between administrative supervisory powers in the digital sphere and the protection of individuals’ digital rights and freedoms, particularly in light of the expanding scope of electronic surveillance. The recommendations emphasize the importance of legislative development, strengthening judicial oversight, enhancing technical capacities within administrative institutions, increasing international cooperation, and promoting digital awareness.

Accordingly, Cyber Surveillance represents a modern regulatory framework in which law and technology intersect, requiring precise legal regulation to safeguard public order in a secure digital environment without undermining individual rights and freedoms.

Acknowledgements

None

Author Contribution:

All authors contributed equally to the main contributor to this paper. All authors reviewed and approved the final version of the manuscript prior to submission.

Declaration of generative AI and AI-assisted technologies in the writing process

The authors hereby declare that no generative artificial intelligence or AI-assisted technologies were used at any stage during the preparation of this manuscript, including language editing, proofreading, or content development. The authors take full responsibility for the originality and integrity of the work presented in this publication.

Funding:

None

Conflicts of Interest:

“The authors declare no conflict of interest.”

References

[1] Felix Reichmann, 'The Pennsylvania Rifle: A Social Interpretation of Changing Military Techniques', The Pennsylvania Magazine of History and Biography, January 1945 at 6

[2] Sean Gallagher, 'Smart Toilet Vulnerable to Bluetooth Flushing Hack', Wired, 5 August 2013 www.wired.co.uk/news/archive/2013-08/05/toilet-hack-attack . References to online sources are accurate as of 6 January 2014.

[3] For an overview of the problems with Cold War metaphors regarding Cyber war, see Noah Shachtman and Peter W. Singer, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive', Brookings Institution, 15 August 2011, www.brookings.edu/research/articles/2011/08/15-Cybersecurity-singer-shachtman

[4] Michael V. Hayden, 'The Future of Things "Cyber"', 5 Strategic Studies Quarterly (1/2011) 3–7 at 3

[5] In fact, September 2013 marked the release of the first history of Cyber conflict: Jason Healey and Karl Grindal (eds), A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Cyber Conflict Studies Association: Arlington, 2013).

[6] John Arquilla and David Ronfeldt, 'Cyberwar is Coming!', in John Arquilla and David Ronfeldt (eds), In Athena's Camp – Preparing for Conflict in the Information Age (Rand Corporation: Santa Monica, 1997), 23–60 at 24–25, reprinted from 12 Comparative Strategy (1993) 141–165.

[7] For an overview of the implications of the development of technology to legal systems see Noel Cox, Technology and Legal Systems (Ashgate: Farnham, 2006)

[8] Cox, Technology and Legal Systems, supra note 8 at 172–173.

[9] Cox, Technology and Legal Systems, supra note 8 at 217.

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 04, No. 06, 2026, pp. 28-41
ISSN 3104-8900

[10] Thanvi, Irfan Ali, THE IMPACT OF THE BRUSSELS EFFECT ON THE EU GDPR: A LEGAL ANOMALY (May 10, 2026). Available at SSRN: https://ssrn.com/abstract=6743300

[11] Charter of the United Nations, 26 June 1945, in force 24 October 1945, 1 UNTS XVI.

[12] Al-Mashaqbeh, Yousef Awad. "Legislative Framework Regulating Digital Media In Jordan And Arab Countries: A Study On The Legal Dimensions." Lex Localis 23, no. 10 (2025): 1-20.

[13] Al-Kasassbeh, Fahad Yousef, Sadam Mohammad Awaisheh, Mohammad Atef Odeibat, Salah Mohammad Aboudi Awaesheh, Lana Al-Khalaileh, and Manal Al-Braizat. "Digital human rights in Jordanian legislation and international agreement." International Journal of Cyber Criminology 18, no. 1 (2024): 37-57.

[14] Al-Kasassbeh, Fahad Yousef, and Ali Mohammad Abu Ghazleh. "International and National Efforts to Protect Cyber Security: Jordan Case Study." International Journal of Cyber Criminology 17, no. 2 (2023): 350-363.

[15] Khwaileh, Khaled Mohammad, and Naheda Mohammad Makhadmeh. "Criminal liability for spreading fake news: a study of Jordanian law in light of international standards." Frontiers in Sociology 11 (2026): 1815400.

[16] Airout, Mohammad. "Criminal Protection Against Cybercrime: A Comparative Legal Analysis of Jordanian, Arab, and International Legislations." Journal of Posthumanism 5, no. 4 (2025): 1459-1472.

[17] Ghandour, Ahmad, and Brendon J. Woodford. "Guidelines to develop a cybersecurity policy in schools, perspectives informed from Jordanian Cybercrime Law." In 2024 25th International Arab Conference on Information Technology (ACIT), pp. 1-6. IEEE, 2024.

[18] Albustanji, Huthaifa, and Paulovics Anita. "A Critical Review of The Jordanian Legal Frameworks on International Cooperation in Combating Cybercrime." AAU Journal of Business and Law 10, no. 1 (2026).

[19] Al-Sarayreh, Riyad Mahmoud. "Jordanian cybercrime law No.(17) of 2023 between regulating social media sites and restricting freedom of opinion." Scholars International Journal of Law, Crime and Justice 7, no. 09 (2024): 339-351.

[20] Muneeb, Firas. "Extent of harmonization of Jordan's Cybercrime Act No. 17 of 2023 with international legislation on freedom of opinion and expression."

[21] Natamiharja, Rudi, Febryani Sabatira, Desia Rakhma Banjarani, Orima Melati Davey, and Ikhsan Setiawan. "Balancing Two Conflicting Perspectives on Wiretapping Act: Rights to Privacy and Law Enforcement." In Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan, vol. 22, no. 1, pp. 18-30. 2022.

[22] Zebua, Memo Alta. "Legal Challenges in Handling Non-Consensual Intimate Image Threats Under Indonesian Law: A Practitioner's Perspective." Available at SSRN 6485380 (2026).

[23] Suci, Evan Andhika. "Video Game Content Regulation and the Politics of Implementation: The Indonesia Game Rating System, 2016–2026." Journal of Political Innovation and Analysis 3, no. 1 (2026): 67-88.

[24] Adi, Bimo Prasetyo, Arthur Josias Simon Runturambi, and Sylvia Prisca Delima. "Strategic Planning of Intelligence and Security Agency of the Indonesian National Police in Maintaining Public Security and Order: The Case of the 2020 Omnibus Law Demonstrations." International Journal of Social Science and Community Service 4, no. 1 (2026): 26-35.

[25] Widjaja, Gunawan, and Adrian Bima Putra. "SURVEILLANCE AND IMPLICATIONS OF WIRETAPPING IN INTERNATIONAL AND NATIONAL LAW: A COMPARATIVE STUDY OF ARRANGEMENTS AND PRACTICES." Jurnal Komunikasi 3, no. 2 (2025): 264-276.

[26] Tobing, Agustinus Nicholas L., and Annisa Fitria. "LEGAL JURISDICTION AND PLACE OF OCCURENCE IN TRANSNATIONAL CYBERCRIME: A NORMATIVE ANALYSIS OF GLOBAL LAW AND INDONESIAN TELECOMMUNICATIONS REGULATIONS." Awang Long Law Review 8, no. 2 (2026): 530-538.

[27] Usman, Noval. "LEGAL PROTECTION OF PERSONAL DATA AND AUTHORITY ACCOUNTABILITY FOR CYBER SECURITY: PDP LAW REVIEW." Law Research Review Quarterly 10, no. 1 (2024).

[28] https://www.techopedia.com/definition/24748/cyberattack

[29] Katharina Ziolkowski, 'Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force' in C. Czosseck, R. Ottis and K. Ziolkowski (eds), 2012 4th International Conference on Cyber Conflict Proceedings (NATO CCD COE Publications: Tallinn, 2012), 295–309 at 296.

[30] Infra discusses it in greater detail

[31] Jari Rantapelkonen, 'Informaatiosodan monet kasvot' in Jyri Raitasalo & Joonas Sipilä (eds), Sota – teoria ja todellisuus: Näkökulmia sodan muutokseen (National Defence University: Helsinki, 2008) at 65.

[32] Finnish Security and Defense Policy 2026, at 162

[33] https://www.checkpoint.com/definition/cyber-attack/

[34] Thanvi, Irfan Ali, The Legal Challenges in Securing Critical Information Infrastructure Protection (CIIP) (March 12, 2026). Available at SSRN: https://ssrn.com/abstract=6399799 or http://dx.doi.org/10.2139/ssrn.6399799

[35] Nicolas Falliere, Liam O Murchu and Eric Chien, 'W32.Stuxnet Dossier', Symantec Security Response Whitepaper, Version 1.4, 11 February 2026, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossi er.pdf at 29. For a more detailed description of Stuxnet see infra at 14.

[36] An obvious example is the use of the term by Michael Schmitt, who used the term 'computer network attacks' in a 1999 article (infra note Error: Reference source not found) but has since used the terms 'cyber operations', 'cyber attacks' and 'cyber war(fare)' (see e.g. infra note 190).

[37] Thanvi, Irfan Ali. "TALLINN MANUAL Application in Real Time Cases." International Journal of Cyberlaw and Cybercrime (IJCLCC) 3, no. 1 (2026): 8–22.

[38] This was an Israeli propaganda

[39] The first cyber-attack was done on the US bank Meryll Lynch. And then the ball got rolling.

[40] Judijanto, L., Suwarna, A. I., & Putra, I. (2025). Juridical Analysis of Data Sovereignty in the Era of Digital Economy in Indonesia. The Easta Journal Law and Human Rights , 3(02), 138–146. https://doi.org/10.58812/eslhr.v3i02.468

[41] Rahman, Irsan, Mohamad Hidayat Muhtar, Novita M. Mongdong, Rahmat Setiawan, Beni Setiawan, and Henry Kristian Siburian. "Harmonization of Digital laws and Adaptation Strategies in Indonesia focusing on E-Commerce and Digital transactions." Innovative: Journal Of Social Science Research 4, no. 1 (2024): 4314-4327.

[42] Al-Brim, Abeer, Lubna Krishan, Khaled Al-jbour, and Omar Almakhzoumi. "Freedom of Opinion and Expression in the Jordanian Legislation." Pakistan Journal of Criminology 16, no. 2 (2024): 1107.

[43] Maghaireh, Alaeldin Mansour. "Cybercrime laws in Jordan and freedom of expression: a critical examination of the electronic crimes act 2023." International Journal of Cyber Criminology 18, no. 1 (2024): 15-36.