P-ISSN : 2721-186X, E-ISSN : 2721-365X

FiTUA : JURNAL STUDI ISLAM
Journal Homepage : https://ejournal.stitbima.ac.id/index.php/fitua

Preventing Cyber Espionage for Social Security Stability: A Ḥadīth and Maqāṣid al-Sharīʿah Perspective

Hendri Waluyo Lensa[1], Marwan Mas'ud[2], Teguh Dwi Prayoga[3]

[1,2] Sekolah Tinggi Dirasat Islamiyah Imam Syafi'i, Jember – Indonesia
[2] Booking Ninjas Company, Florida – United States of America
*Corresponding author : masudmarwan14@gmail.com
DOI : https://doi.org/10.47625/fitua.v7i1.1314

Article

Article History :
Received : May 01, 2026
Reviewed : May 20, 2026
Accepted : June 18, 2026
Published : June 28, 2026

Keywords:

Cyber espionage;
Social Security Stability;
Prophet's Hadith;
Maqāṣid al-Sharīʿah.

Abstract

Cyber espionage, referring to efforts by certain parties to illegally obtain strategic information through digital means, poses a serious threat to human survival and social stability. This issue can be objectively examined from the perspective of the Prophet's Hadith and *maqāṣid al-sharīʿah*. This study employs a qualitative approach using a library research method. The data utilized are secondary and analyzed through descriptive analysis. The theoretical framework applied includes Critical Discourse Analysis (CDA) and the theory of *maqāṣid al-sharīʿah*, with conclusions drawn using a deductive approach. The results indicate that, from the perspective of *maqāṣid al-sharīʿah*, cyber espionage undermines societal welfare and violates the five essential objectives: religion, life, intellect, progeny, and wealth. This practice threatens safety, causes economic losses, disrupts education and public services, and diminishes moral and ethical values in society, making its prevention a collective obligation. Prevention can be carried out through the application of Hadith, which emphasizes trustworthiness, commitment to promises, and protection of rights, as well as through CDA to build moral awareness, strengthen digital governance, promote ethical education, and enforce just laws, thereby maintaining social stability and public welfare in the digital era.

INTRODUCTION

The rapid development of information and communication technology has transformed social interactions, economic activities, and public governance by improving efficiency, connectivity, and access to digital services.(Mubasit et al., 2025; Rahman & Firdaus, 2021; Yusuf et al., 2025) However, this digital transformation has simultaneously expanded the global cyber threat landscape, making cyber espionage one of the most significant security challenges confronting governments, corporations, and critical infrastructure. According to the IBM X-Force Threat Intelligence Index 2025, identity abuse remained the most common initial attack vector, accounting for approximately 30% of cybersecurity incidents, while 70% of the incidents handled by IBM involved organizations operating critical infrastructure, demonstrating that attackers increasingly target strategic digital assets rather than merely causing operational disruption. Likewise, the Verizon 2025 Data Breach Investigations Report analyzed more than 22,000 security incidents and 12,195 confirmed data breaches across 139 countries, revealing a substantial increase in system intrusions and vulnerability exploitation as major causes of security breaches, particularly in the Asia-Pacific region (Caridi, 2025). These findings indicate that cyber espionage is no longer an isolated technical issue but a rapidly escalating global threat with serious implications for national security, economic resilience, institutional trust, and societal stability. Cyber espionage refers to the unauthorized acquisition of strategic or confidential information through digital means by state or non-state actors, potentially compromising national security, individual privacy, and the broader welfare of society. (Cremer et al., 2022)

Cyber espionage causes a wide range of harmful consequences, including unauthorized access to confidential information, violations of individual privacy, substantial economic losses, institutional

instability, and threats to human security.(Cremer et al., 2022a; Ulven & Wangen, 2021) These consequences extend far beyond technical or cybersecurity concerns, affecting public trust, social order, and the overall welfare of society. Therefore, cyber espionage should be understood not merely as a technological problem but also as an ethical and social issue that requires normative evaluation. From the perspective of classical *Maqāṣid al-Sharīʿah*, any action that threatens the safety, security, and welfare of society constitutes a violation of the objectives of Islamic law (Dakhoir et al., 2022; H. Osman et al., 2021; Sayudi & Parmujianto, 2023). *Maqāṣid al-Sharīʿah* emphasizes the protection of five fundamental objectives: religion (*dīn*), life (*nafs*), intellect (*ʿaql*), progeny (*nasl*), and property (*māl*), all of which may be adversely affected by cyber espionage.((Corresponding Author) et al., 2023; Subhani, 2023). For example, unauthorized disclosure of confidential information jeopardizes property rights and individual safety, erodes trust in public institutions, disrupts decision-making processes, and ultimately undermines social stability.

Classical studies of the Hadith of Prophet Muhammad SAW also emphasize the importance of safeguarding the security, dignity, and rights of both individuals and society. These principles serve as a moral and ethical foundation for addressing destructive digital threats.(Korbatieh, 2020) Accordingly, classical perspectives such as the Hadith and *Maqāṣid al-Sharīʿah* offer a normative framework that can be utilized to prevent and comprehensively mitigate the practice of cyber espionage.

Despite the growing body of research on cybersecurity and cyber espionage, previous studies have primarily focused on technological, legal, geopolitical, and governance perspectives, with limited attention given to the ethical and normative dimensions offered by Islamic scholarship. In particular, little research has integrated Prophetic Hadith, *Maqāṣid al-Sharīʿah*, and Critical Discourse Analysis (CDA) into a comprehensive framework for evaluating and preventing cyber espionage while promoting social security stability. This gap highlights the need for an interdisciplinary approach that connects contemporary cybersecurity challenges with the normative objectives of Islamic law.

Accordingly, this study seeks to answer the following research questions: (1) How is cyber espionage understood and evaluated from the perspective of *Maqāṣid al-Sharīʿah*? (2) To what extent does cyber espionage affect social security stability at both the individual and societal levels? and (3) How can cyber espionage be prevented through the application of Prophetic Hadith and *Maqāṣid al-Sharīʿah*? By addressing these questions, this study aims to contribute to the growing discourse on cybersecurity by proposing an Islamic ethical framework that integrates Hadith, *Maqāṣid al-Sharīʿah*, and Critical Discourse Analysis as complementary approaches for strengthening cybersecurity governance, protecting public welfare, and maintaining social security stability in the digital era.

Previous research addressing similar themes includes the article titled "*Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era*" by Aisha Adeyeri and Hossein Abroshan.(Adeyeri & Abroshan, 2024) The study's findings indicate that, as the digital environment develops, cyber threats become increasingly complex, including aggressive attacks and sophisticated cyber espionage. The research highlights the role of non-state actors, such as terrorist organizations and armed groups, in leveraging cyberspace for strategic purposes and their impact on global security. Various threats, including supply chain attacks, ransomware, and IoT vulnerabilities, demonstrate the limitations of security approaches that focus solely on states. Additionally, the study emphasizes the importance of informal governance and cooperation between governmental and non-governmental entities to build strong and flexible cybersecurity mechanisms. These findings encourage stakeholders to understand the complex relationship between geopolitics, governance, and cyber threats in order to strengthen global digital resilience.

Another study titled "*Cyber Espionage in National and Global Perspective: How Indonesia Deals with this Issue?*" by Maharani Chandra Dewi shows that,(Dewi, 2022) in the era of rapid technological advancement, cybercrime has become a serious threat to individual and institutional privacy. Mobile technology and advanced communication networks, while beneficial, can pose risks if misused. Preventing cybercrime requires self-awareness, ethical behavior, and adequate technological

literacy, as excessive or careless actions may create opportunities for cyber offenses. By maintaining proper conduct and wise use of technology, the risks of cybercrime can be minimized.

The previous studies, such as "*Geopolitical Ramifications of Cybersecurity Threats" by Adeyeri and Abroshan and "Cyber Espionage in National and Global Perspective*" by Maharani Chandra Dewi, share similarities with the research "*Preventing Cyber Espionage for Social Security Stability: A Ḥadīth and Maqāṣid al-Sharīʿah Perspective*" in highlighting cyber espionage as a complex digital phenomenon with potential harm to both individuals and institutions. Both studies emphasize the importance of technological understanding, self-awareness, ethical behavior, and cooperation among various stakeholders—both between nations and between governmental and non-governmental entities—to mitigate cyber risks. The threats discussed, such as aggressive cyberattacks, ransomware, supply chain attacks, and vulnerabilities in the Internet of Things, are central due to their broad impact on security stability and privacy.

However, the research "*Preventing Cyber Espionage for Social Security Stability: A Ḥadīth and Maqāṣid al-Sharīʿah Perspective*" presents significant differences compared to the previous studies. First, it emphasizes a classical Islamic perspective, using the Hadith and *Maqāṣid al-Sharīʿah* as the analytical framework. This focus adds a normative and ethical dimension that has not been widely explored in previous literature, which mostly concentrates on technical, geopolitical, and modern governance aspects. Second, this study emphasizes social security stability as the consequence of cyber espionage, rather than solely national security or individual privacy. This positions the protection of society and public welfare at the center of the analysis, in line with the principles of *Maqāṣid al-Sharīʿah*, which stress the protection of life, property, intellect, religion, and progeny.

RESEARCH METHOD

This research adopts a qualitative approach, a framework centered on grasping and interpreting social phenomena from the personal viewpoints of participants. Originating from the fields of Anthropology and Sociology, qualitative research rests on the belief that social reality can be examined in a systematic and scholarly way.(Lensa et al., 2026; Mas' ud, Lensa, et al., 2026; Mohajan, 2018; Nasrulloh et al., n.d.) The main approach used to gather data in this research is library research. This method is defined by specific traits, such as working directly with documentary sources, relying on data that is already accessible, not being constrained by time or location, and essentially depending on secondary information sources (Husaini et al., 2026; La Harisi et al., 2026; Muhtadin et al., 2026; Tajedini et al., 2019).

The way data is managed in this study depends on secondary information, meaning it uses data that were gathered by others rather than by the researchers themselves (Cheong et al., 2023; Mas'ud et al., 2025; Mas'ud, Wicaksono, et al., 2026; Saleh & Mas'ud, 2025). The materials used in this research consist of academic journal articles, recent scholarly books, and traditional collections of Hadith. This investigation uses a thematic Hadith analysis as its research framework, which in Hadith scholarship entails systematically gathering and critically reviewing all Prophetic traditions associated with a particular topic. After compiling the relevant Hadiths, they are examined to form a unified, well-contextualized, and thorough understanding of the issue being studied (Mas' ud et al., 2025; Mas' ud, Rizqi, et al., 2026; MAS'UD, 2021; Mas'ud, Penataran, et al., 2026; Rohman et al., 2020).

In this study, Critical Discourse Analysis (CDA) and the theory of Maqāṣid al-Sharīʿah are used as the main analytical tools. CDA views language not just as a communicative tool but as a type of social practice that is deeply connected to power relations, ideology, and broader social frameworks.(Boulahnane, 2019; Fairclough, 2023) CDA begins with the understanding that language is never neutral, so it moves beyond simple linguistic interpretation to critically explore the social, political, and historical contexts behind how texts are produced. This method emphasizes how language helps shape meaning, influences collective thought patterns, and brings certain perspectives to the forefront while obscuring others. The goal of CDA is to reveal the often-hidden ideologies within texts and to evaluate how these texts help construct social realities. The analysis is carried out on three connected levels: the micro-level, which focuses on specific linguistic features and word choices; the

meso-level, which looks at how discourses are produced, distributed, and received; and the macro-level, which considers the wider social conditions and power structures that inform the discourse.

On the other hand, the theory of *Maqāṣid al-Sharīʿah* is a concept in *uṣūl al-fiqh* that identifies the core aims of Islamic law, which are intended to promote human well-being (*maṣlaḥah*) and prevent harm (*mafsadah*). According to classical scholars such as al-Shāṭibī, the objectives of *Sharīʿah* are organized into three hierarchical categories: *ḍarūriyyāt* (fundamental necessities like protecting religion, life, intellect, lineage, and wealth), *ḥājiyyāt* (important needs that ease hardship), and *taḥsīniyyāt* (desirable refinements that enhance moral and social life). These *maqāṣid* serve as a framework for evaluating laws and policies, making sure that *Sharīʿah* rulings are applied ethically, appropriately for their context, and in ways that support the welfare (*falāḥ*) of the community.(Zaprulkhan, 2018) For analyzing the data, this research uses descriptive analysis, a method that focuses on systematically describing the characteristics and features of the collected data rather than testing hypotheses or making predictions. After the initial description, the results are then integrated and interpreted through deductive reasoning to draw logical conclusions based on established principles,(Amirudin et al., 2025; Azungah, 2018; Marwan Mas'ud et al., 2025; Mas' ud, Asy'ari, et al., 2026; Mas' ud, Tujang, et al., 2026; Mas' ud & Rizqi, 2025; Masud et al., 2025; Ramadhansyah et al., 2025) whereby general observations are analyzed first and then refined into specific, evidence-based conclusions.

RESULT AND DISCUSSION

Cyber Espionage from the Perspective of *Maqāṣid al-Sharīʿah*

In the current digital era, cyber espionage, or the illegal acquisition of strategic and confidential digital information, has emerged as one of the most pressing security concerns confronting individuals, institutions, and states alike (Broeders, 2024). Cyber espionage refers to the unauthorized collection of sensitive data through digital means, whether carried out by individuals, organized groups, or state and non-state actors, for political, economic, or strategic purposes. Its targets range from government agencies, corporations, and financial institutions to the personal data of private citizens (Salim et al., 2023). As digital infrastructure becomes increasingly sophisticated, perpetrators are able to penetrate complex information-security systems, posing serious threats to national security, individual privacy, and the broader stability of society.

Evaluating this phenomenon solely through a technical or legal lens, however, is insufficient, because cyber espionage is fundamentally a violation of trust and a threat to collective well-being (Shulruff, 2024). It is precisely at this point that the framework of *maqāṣid al-sharīʿah* becomes relevant. As a branch of *uṣūl al-fiqh, maqāṣid al-sharīʿah* identifies the overarching objectives of Islamic law, namely the promotion of human welfare (*maṣlaḥah*) and the prevention of harm (*mafsadah*) (Saydullayevich, 2025). Classical scholars such as al-Shāṭibī classify these objectives hierarchically into *ḍarūriyyāt* (fundamental necessities), *ḥājiyyāt* (complementary needs), and *taḥsīniyyāt* (refinements that enhance moral and social life). At the core of the *ḍarūriyyāt* lie five essential objectives known as *al-ḍarūriyyāt al-khams*: the protection of religion (*ḥifẓ al-dīn*), life (*ḥifẓ al-nafs*), intellect (*ḥifẓ al-ʿaql*), progeny (*ḥifẓ al-nasl*), and property (*ḥifẓ al-māl*) (Fahrurrozi et al., 2026; Hasan et al., 2026; Mohammed, 2024). Any action that undermines one or more of these five objectives is, by definition, contrary to the purposes of *sharīʿah*, regardless of whether it is explicitly mentioned in a specific legal text.

Cyber espionage can be shown to contravene all five of these objectives simultaneously, which is precisely what distinguishes it from an ordinary technical infraction and elevates it to the status of a *sharʿī* violation. First, in relation to *ḥifẓ al-nafs*, the unauthorized exposure of personal or institutional data frequently generates psychological distress, anxiety, and, in more severe cases, physical danger when sensitive information is exploited for coercion, blackmail, or targeted attacks (Sears & Cunningham, 2024). Second, concerning *ḥifẓ al-māl*, digital data, intellectual property, and strategic information constitute contemporary forms of wealth; their theft causes direct financial harm to individuals, corporations, and states, paralleling the harm caused by the unlawful seizure of tangible

property (Liu & Babar, 2024). Third, with respect to *ḥifẓ al-ʿaql*, cyber espionage corrodes the integrity of information upon which sound judgment depends; when data can no longer be trusted, decision-making at both the individual and institutional level is impaired, and public confidence in digital systems erodes (Snider et al., 2021). Fourth, in terms of *ḥifẓ al-nasl*, attacks on the digital infrastructure underpinning education, healthcare, and public administration jeopardize the continuity of services on which the welfare of future generations depends (Ewoh & Vartiainen, 2024). Fifth, in relation to *ḥifẓ al-dīn*, cyber espionage represents a fundamental breach of *amānah* (trustworthiness) and ethical responsibility, two values that Islam regards as inseparable from religious commitment (Meerangani et al., 2022); a society in which deception and betrayal of trust become normalized suffers a corresponding erosion of its moral and religious fabric.

Viewed through this lens, cyber espionage is not merely a technological or security problem to be resolved through firewalls and encryption alone. It is, more fundamentally, an act that undermines *maṣlaḥah ʿāmmah* (public welfare) and generates *mafsadah* (harm) across all five dimensions that *sharīʿah* seeks to protect. This conclusion provides the normative foundation for the discussion in the following sections: if cyber espionage threatens the *ḍarūriyyāt al-khams*, then its prevention is not optional but constitutes a *sharʿī* obligation aimed at preserving social security and collective stability.

The Impact of Cyber Espionage on Social Security Stability

Having established that cyber espionage contradicts the objectives of *maqāṣid al-sharīʿah* in principle, this section examines how that contradiction materializes concretely across different levels of social life: the individual, the institutional, the state, and society at large. Organizing the discussion according to the locus of impact, rather than according to isolated case studies, makes it possible to trace systematically how each category of harm corresponds to a specific dimension of the *al-ḍarūriyyāt al-khams*, thereby connecting empirical impact with normative evaluation.

1. Impact on Individuals

At the individual level, cyber espionage manifests primarily as a violation of privacy through the unauthorized collection, surveillance, or exposure of personal data (Mulahuwaish et al., 2025). Victims often experience direct psychological consequences, including anxiety, fear, and loss of a sense of safety, particularly when leaked information is used for blackmail, harassment, or identity-related fraud (Borwell et al., 2025). These consequences correspond directly to *ḥifẓ al-nafs*, since the protection of life encompasses not only physical safety but also psychological well-being and freedom from intimidation (Bawono et al., 2025). In addition, when financial data or digital assets are compromised, individuals suffer material loss, which constitutes a violation of *ḥifẓ al-māl* (Shevchenko et al., 2023). The individual-level impact thus illustrates how a seemingly technical intrusion translates into tangible harm to a person's safety and property.

2. Impact on Institutions

At the institutional level, cyber espionage disrupts organizational integrity and erodes the trust that institutions, whether corporate, educational, or administrative, depend upon to function (Perera et al., 2022). The theft of proprietary information, trade secrets, or internal communications can paralyze decision-making processes, damage an institution's reputation, and weaken coordination both within the organization and with its partners (Cheng et al., 2024). This corresponds to *ḥifẓ al-ʿaql*, since the reliability of information is a precondition for sound institutional judgment; when that reliability is compromised, the capacity of an institution to reason, plan, and respond effectively is correspondingly diminished (Habib, 2025). Financial losses arising from data breaches additionally implicate *ḥifẓ al-māl* at an organizational scale, often with consequences that extend to employees, shareholders, and the wider public who depend on the institution's services (Azizov et al., 2025). Cyber espionage weakens institutional integrity by undermining information reliability, financial security, and public trust, thereby violating the objectives of *ḥifẓ al-ʿaql* and *ḥifẓ al-māl*.

3. Impact on the State

At the level of the state, cyber espionage acquires an explicitly political and strategic dimension. The infiltration of government systems or critical infrastructure can be used to manipulate public opinion, disrupt governmental processes, compromise national defense, or even provoke international

tension when conducted by foreign actors (Rosli, 2025). Such acts threaten *ḥifẓ al-nasl* insofar as the continuity of public services, including administration, healthcare, and education systems operated by the state, is essential to safeguarding the welfare of future generations (Muhammadong, 2025). At the same time, state-level cyber espionage threatens *ḥifẓ al-dīn* in a broader civilizational sense, because it undermines the ethical and moral order that *sharīʿah* seeks to preserve within a polity, replacing trust between governing institutions and citizens with suspicion and instability (Shandler & Gomez, 2022). From the perspective of *Maqāṣid al-Sharīʿah*, cyber espionage undermines state stability by threatening public welfare, institutional legitimacy, and the ethical order of society.

4. Impact on Society

At the societal level, the cumulative effect of individual, institutional, and state-level breaches is a generalized erosion of public trust (Imran et al., 2024). When sensitive information is repeatedly exposed or misused, communities grow increasingly anxious about the safety of their data, skeptical of digital institutions, and fragmented in their willingness to cooperate with public systems (Pool et al., 2024). This generalized erosion of trust represents a direct threat to social cohesion, the very foundation that *maqāṣid al-sharīʿah* seeks to protect through its emphasis on collective welfare (Aruqaj, 2023). In economic terms, the leakage of corporate or financial data destabilizes markets and threatens the broader economic security on which public welfare depends, again implicating *ḥifẓ al-māl*, but now at the level of society as a whole rather than a single individual or institution (Zhou & Huang, 2024).

Taken together, these four levels of impact demonstrate that the harm caused by cyber espionage is not confined to a single dimension of the *ḍarūriyyāt al-khams* but instead radiates outward from the individual to society, accumulating in severity as it moves from the personal to the collective sphere. This progression confirms that cyber espionage is, at its core, a multidimensional threat to social security stability, one that cannot be adequately addressed through technical countermeasures alone but requires a normative and ethical response, which is the subject of the following section.

Preventing Cyber Espionage through *Hadith*

If the preceding sections established why cyber espionage constitutes a violation of *maqāṣid al-sharīʿah* and how its harm manifests across different levels of social life, the present section turns to the normative resources within the Hadith literature that ground the obligation to prevent it. Rather than treating each Hadith as an isolated textual unit, the discussion below groups the relevant traditions according to three thematic clusters, namely the protection of property, the protection of trust, and the protection of brotherhood and human dignity. This thematic organization allows the analysis to move beyond a mere catalogue of texts toward an integrated discourse, in line with the analytical aims of Critical Discourse Analysis (CDA), which treats language as a form of social practice rather than an inert string of words.

1. Protection of Property (*Ḥifẓ al-Māl*)

The first thematic cluster concerns the protection of property, drawing on two complementary Hadith. The first is the tradition narrated by Abū Hurayrah (r.a.), in which the Prophet SAW said: “May Allah curse the thief who steals an egg, so that his hand is cut off, and who steals a rope, so that his hand is cut off” (Agreed upon) **).**(al-Ḍiyā’, 2016 Vol. 6, p. 539.). The second is the tradition, also narrated by Abū Hurayrah, in which the Messenger of Allah SAW said: “Whoever cheats us is not one of us” (Narrated by Muslim) (al-Ḍiyā’, 2016 Vol. 5, p. 563.).

Read together, these two traditions establish a unified ethical principle: any unlawful appropriation of another's property, whether through outright theft or through deceit and fraud (*ghashsh*), constitutes a serious violation of public order, regardless of the apparent magnitude of the object taken. The first *Hadith* emphasizes that even a seemingly trivial item, such as an egg or a rope, is sufficient to warrant severe condemnation, underscoring that the prohibition concerns the principle of unlawful taking itself rather than the monetary value involved. The second *Hadith* extends this principle from overt theft to covert deception, establishing that fraud and manipulation are equally condemned even when no physical object changes hands.

Applied to the digital context, cyber espionage represents a contemporary convergence of both forms of violation identified in these *Hadith*. The unauthorized extraction of data, the interception of

confidential communications, and the hacking of secured systems are functionally equivalent to theft, since they involve the unlawful appropriation of an asset that, in the digital era, takes the form of information rather than physical property. At the same time, many cyber-espionage operations rely on manipulation, social engineering, or the impersonation of trusted parties, placing them squarely within the prohibition against *ghashsh*. Using Critical Discourse Analysis, it can be observed that at the micro level, lexical choices such as "curse" and "hand cut off" signal the gravity with which Islamic legal discourse treats violations of property rights, while at the macro level, both *Hadith* function as a critique of any social or technological structure that enables unlawful appropriation, whether through brute force or deception. Normatively, this cluster establishes that cyber espionage, insofar as it constitutes digital theft and fraud, directly contravenes *ḥifẓ al-māl* and the broader prohibition against unlawful taking that the Hadith of theft and the Hadith of fraud jointly articulate.

2. Protection of Trust (*Amānah*)

The second thematic cluster centers on the principle of *amānah*, drawing on the *Hadith* reported from Anas, who said: "Rarely did the Messenger of Allah SAW deliver a sermon without saying: 'There is no faith for one who has no trustworthiness, and there is no religion for one who has no commitment to promises'" (Reported by Aḥmad; graded ḥasan by al-Dhiyā') (al-Ḍiyā', 2016 Vol. 11, p. 117.).

This Hadith situates *amānah* (trustworthiness) and *wafā' al-'ahd* (fulfillment of commitments) not as peripheral virtues but as conditions so fundamental that their absence is equated with the absence of faith and religion themselves. The severity of this equivalence signals that trust is not merely a social convenience but a constitutive element of religious and moral integrity.

In the context of cyber espionage, this principle is directly implicated, because nearly every act of digital espionage presupposes a prior breach of trust, whether trust placed in a system, an institution, an employee with privileged access, or a counterpart in digital communication. Cyber espionage frequently exploits relationships of presumed reliability: an insider who abuses authorized access, a vendor who exceeds the scope of granted permissions, or a state actor who violates diplomatic norms of confidentiality. Applying Critical Discourse Analysis, the repeated negation "there is no…there is no…" at the micro level constructs an uncompromising discursive boundary around the value of trustworthiness, admitting no exception. At the meso level, the *Hadith's* placement as a recurring element of the Prophet's sermons reflects the centrality of *amānah* to communal life, while at the macro level, it functions as a standing critique of any social or institutional structure, including digital ones, that normalizes the betrayal of granted trust. Normatively, this cluster establishes that the prevention of cyber espionage is inseparable from the cultivation of *amānah* at every level, from individual digital conduct to institutional data governance, since cyber espionage is, at its root, a violation of trust rather than merely a technical failure.

3. Protection of Brotherhood and Human Dignity

The third thematic cluster concerns the protection of brotherhood and human dignity, drawing on the Hadith narrated by Abū Hurayrah (r.a.), in which the Prophet SAW said: "Do not envy one another, do not cheat in trade, do not hate one another, do not turn away from one another, and do not sell one over the sale of another. Be the servants of Allah as brothers. A Muslim is the brother of another Muslim; he does not oppress him, abandon him, or belittle him. Piety is right here," and he pointed to his chest three times. "It is sufficient evil for a person to belittle his Muslim brother. For every Muslim, the blood, property, and honor of another Muslim are sacred" (Narrated by Muslim) (al-Ḍiyā', 2016 Vol. 11, p. 117.).

This Hadith establishes *ukhuwwah* (brotherhood) as a relational ethic that prohibits not only direct harm but also subtler forms of disregard for another person's standing, including oppression, abandonment, and belittlement. Its concluding declaration, that the blood, property, and honor of a fellow Muslim are sacred, broadens the scope of protection beyond physical safety to encompass property and dignity as inseparable elements of the same ethical injunction.

Cyber espionage stands in direct tension with this ethic, since the unauthorized surveillance, exposure, or exploitation of another person's or institution's digital information is, in substance, a violation of their honor (*ʿirḍ*) and dignity as much as it is a violation of their property. The covert nature

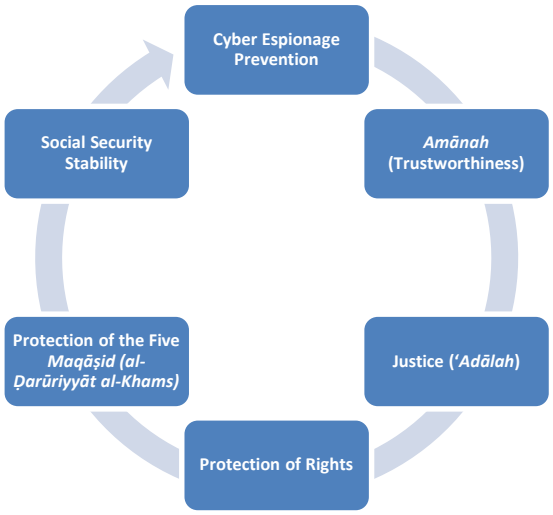
of cyber espionage further compounds the harm, as the targeted party is typically denied even the awareness that a violation has occurred, a circumstance that intensifies the breach of trust and dignity described in the Hadith. Using Critical Discourse Analysis, the repeated negative imperatives at the micro level ("do not envy," "do not cheat," "do not hate") construct a cumulative discourse of relational boundaries, while the meso-level structure, moving from prohibition to positive injunction ("be the servants of Allah as brothers") to a culminating declaration of sanctity, models a complete ethical architecture rather than a single isolated rule. At the macro level, this Hadith critiques any social order, digital environments included, in which the dignity of the other is treated as negotiable or exploitable for strategic advantage. Normatively, this cluster establishes that the prevention of cyber espionage is also a matter of upholding *ukhuwwah* and human dignity in digital interaction, since the harm caused by espionage extends beyond material loss to an assault on the honor and standing of its victims.

Integration of Hadith and *Maqāṣid al-Sharīʿah* in Preventing Cyber Espionage

The discussion thus far has proceeded along two parallel tracks: the normative evaluation of cyber espionage through the lens of *maqāṣid al-sharīʿah*, and the thematic analysis of relevant Hadith organized around property, trust, and brotherhood. The principal conceptual contribution of this study lies in integrating these two tracks into a single coherent framework, rather than leaving them as separate analytical layers.

The analysis demonstrates that the prevention of cyber espionage within an Islamic ethical framework is built upon three foundational principles that emerge consistently across the Hadith examined above: *amānah* (trustworthiness), justice (*ʻadālah*), and the protection of public welfare (*maṣlaḥah ʻāmmah*). *Amānah*, as established through the Hadith of Anas, requires that every party with access to data, systems, or confidential information uphold the trust placed in them rather than exploit it for unauthorized gain. Justice requires that the rights of individuals, institutions, and states to the security of their information be respected and that violations, whether through theft, fraud, or covert surveillance, be subject to fair and consistent accountability, as reflected in the *Hadith* condemning theft and deception. The protection of public welfare requires that the cumulative impact of digital conduct on the safety, dignity, and stability of the broader community be treated as a primary consideration, in line with the Hadith affirming the sanctity of a fellow believer's blood, property, and honor.

These three principles do not operate independently; rather, they converge to support the protection of rights at large, which in turn corresponds directly to the five objectives of maqāṣid al-sharīʿah identified in the first section of this discussion, namely *ḥifẓ al-dīn, ḥifẓ al-nafs, ḥifẓ al-ʿaql, ḥifẓ al-nasl, and ḥifẓ al-māl*. When amānah, justice, and the protection of public welfare are upheld in digital conduct, the five essential objectives are correspondingly preserved, and the cumulative result is the stability of social security described in the second section of this discussion. The relationship among these elements can be represented as a sequential conceptual flow, moving from the prevention of cyber espionage through the foundational ethical principles toward the ultimate goal of social security stability.



This conceptual flow illustrates that the prevention of cyber espionage is not reducible to a single legal prohibition or a single technical safeguard, but rather emerges from the layered operation of ethical principles that originate in the Hadith and culminate in the objectives safeguarded *by maqāṣid al-sharīʿah. Amānah* provides the internal ethical disposition that discourages the temptation to exploit access to information; justice provides the normative standard by which violations are judged and addressed; and the protection of public welfare provides the orientation toward the collective good that elevates the discussion beyond individual wrongdoing to a matter of communal responsibility. Together, these principles operationalize the protection of rights, which in turn sustains the five essential objectives of *sharīʿah*, and it is precisely the sustained protection of these five objectives that constitutes social security stability in the digital era.

This integrated framework represents the central conceptual contribution of the present study. Whereas previous research on cybersecurity has tended to treat technical, legal, and geopolitical dimensions of cyber espionage as separate from religious-ethical considerations, this study demonstrates that Hadith-derived principles of *amānah*, justice, and public welfare can be systematically connected to *maqāṣid al-sharīʿah* to produce a unified normative model for understanding why cyber espionage must be prevented and what ethical foundations such prevention should rest upon. This model offers a basis for future research to develop more concrete policy recommendations, ethical guidelines, and educational strategies grounded in Islamic legal theory while remaining responsive to the technical realities of the digital era

CONCLUSION

From the perspective of *maqāṣid al-sharīʿah*, cyber espionage is regarded as an act that undermines public welfare and contradicts the five essential objectives (*al-ḍarūriyyāt al-khams*): religion (*dīn*), life (*nafs*), intellect (*ʻaql*), progeny (*nasl*), and wealth (*māl*). This practice threatens human safety, harms the economy, weakens decision-making, disrupts education and public services, and diminishes the moral and ethical values of society. Thus, cyber espionage is not merely a technical threat but also a moral and social violation, making its prevention a collective obligation to safeguard social security, stability, and welfare comprehensively.

Efforts to prevent cyber espionage can be undertaken through the application of classical studies, namely Hadith, which emphasize *amanah* (trustworthiness), *wafā' al-ʻahd* (fulfillment of promises), and the protection of individual and societal rights. Hadith strongly prohibit theft, fraud, and actions that harm others, which in the modern context are applicable to illegal acts such as digital data theft or manipulation. Through the lens of Critical Discourse Analysis (CDA), Hadith can be understood as normative discourse that builds collective moral awareness, highlights individual and institutional responsibility, and guides strategies for preventing cyber espionage through ethical education, strengthened digital governance, and just law enforcement. This approach ensures social security, stability, and the protection of societal welfare in the digital era.

REFERENCES

Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information, 15*(11), 682. https://doi.org/10.3390/info15110682

al-Ḍiyā', M. 'Abd A. (2016). *Al-Jāmiʻ al-Kāmil fī al-Ḥadīth al-Ṣaḥīḥ al-Shāmil al-Murattab ʻalā Abwāb al-Fiqh* (1st ed.). Dār al-Salām lil-Nashr wa-al-Tawzīʻ.

Amirudin, H., Ihcsan, C. M., Fathoni, M., Ramadhansyah, A., & Mas'ud, M. (2025). تحليل حماية البيئة من التلوث الهوائي في ضوء الحديث النبوي: دراسة موضوعية من خلال أحاديث الصحيحين: An Analytical Study on Environmental Protection from Air Pollution in the Light of Prophetic Hadiths: A Thematic Study Based on the Hadiths of al-Ṣaḥīḥayn. *Maʿālim Al-Qurʾān Wa al-Sunnah, 21*(2), 405–426. https://doi.org/10.33102/jmqs.v21i2.545

Aruqaj, B. (2023). An Integrated Approach to the Conceptualisation and Measurement of Social Cohesion. *Social Indicators Research, 168*(1–3), 227–263. https://doi.org/10.1007/s11205-023-03110-z

Azizov, E., Azizov, A., Azizli, A., & Babayev, A. A. (2025). A Maqasid al-Shariah Framework for Fintech and Digital Asset Regulation in Muslim Jurisdictions. *Journal of Islamic Law and Legal Studies*, *2*(2), 96–113. https://doi.org/10.70063/jills.v2i2.119

Azungah, T. (2018). Qualitative research: Deductive and inductive approaches to data analysis. *Qualitative Research Journal*, *18*(4), 383–400. https://doi.org/10.1108/QRJ-D-18-00035

Bawono, B. T., Huda, M. N., Prayitno, A. H., & Siswanto, M. A. (2025). Human Trafficking and the Relevance of Hifz al-nafs and Hifz al-'ird in Contemporary Islamic Legal Ethics. *MILRev: Metro Islamic Law Review*, *4*(1), 597–618. https://doi.org/10.32332/milrev.v4i1.10694

Borwell, J., Jansen, J., & Stol, W. (2025). The psychological impact of cybercrime victimization: The importance of personal and circumstantial factors. *European Journal of Criminology*, *22*(4), 603–624. https://doi.org/10.1177/14773708241312506

Boulahnane, S. (Corresponding A. (2019). Homophobia and 'Un-Americanness' as Rising Facets of Islamophobia: an Analysis Of Orlando Shooting Media Transcripts. *Journal of Al-Tamaddun*, *14*(2), 143–152. https://doi.org/10.22452/jat.vol14no2.11

Broeders, D. (2024). Cyber intelligence and international security: Breaking the legal and diplomatic silence? *Intelligence and National Security*, *39*(7), 1213–1229. https://doi.org/10.1080/02684527.2024.2398077

Caridi, C. (2025, April 17). *X-Force Threat Intelligence Index 2025 highlights attackers steal, and sell, user identities at scale | IBM*. https://www.ibm.com/think/x-force/x-force-threat-intelligence-index-2025-attackers-steal-sell-user-identities

Cheng, C. S. A., Jiang, L., & Song, W.-L. (2024). Media coverage and debt financing choice. *Journal of Accounting and Public Policy*, *44*, 107181. https://doi.org/10.1016/j.jaccpubpol.2024.107181

Cheong, H., Lyons, A., Houghton, R., & Majumdar, A. (2023). Secondary Qualitative Research Methodology Using Online Data within the Context of Social Sciences. *International Journal of Qualitative Methods*, *22*. https://doi.org/10.1177/16094069231180160

(Corresponding Author), M. A. N., Jamaludin, M. H., Mohd Nawawi, M. S. A., Ahmad Zaki, N., & Abdul Wahab, R. (2023). Astronomy Development since Antiquity to Islamic Civilization from the Perspective of Islamic Historiography. *Journal of Al-Tamaddun*, *18*(1), 169–177. https://doi.org/10.22452/jat.vol18no1.14

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Dakhoir, A., Tarantang, J., & Rahman, G. (2022). Bankers' Attitudes to the Legal Position of Bank Interest: New Insights for the Development of Fiqh Wasatiyah Maliyah. *Akademika : Jurnal Pemikiran Islam*, *27*(1), 47. https://doi.org/10.32332/akademika.v27i1.4085

Dewi, M. C. (2022). Cyber Espionage in National and Global Perspective: How Indonesia Deal with This Issue? *International Law Discourse in Southeast Asia*, *1*(1), 1–22.

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. *Journal of Medical Internet Research*, *26*, e46904. https://doi.org/10.2196/46904

Fahrurrozi, M., Mas'ud, M., Raihan, Z., Putra, D. H., & Prayoga, T. D. (2026). Prophetic Supplications and Economic Stability: A Ḥadīth-Based Analysis through al-Shāṭibī's Maqāṣid al-Sharīʿah Framework. *Solo International Collaboration and Publication of Social Sciences and Humanities*, *4*(02), 647–660. https://doi.org/10.61455/sicopus.v4i02.533

Fairclough, N. (2023). Critical discourse analysis. In *The Routledge Handbook of Discourse Analysis* (2nd ed.). Routledge.

H. Osman, R. A., Zakariyah, L., Zakariyah, H., & Ahmad Dahlan, A. R. (2021). Cyber Security and Maqasid Al- Shariah: A Case Of Facebook Application. *International Research Journal of Shariah, Muamalat and Islam*, *3*(6), 12–25. https://doi.org/10.35631/irjsmi.36002

Habib, Z. (2025). Ethics of Artificial Intelligence in Maqāṣid Al-Sharīa's Perspective. *KARSA Journal of Social and Islamic Culture*, *33*(1), 105–134.

Hasan, I., Mas' ud, M., & Prayoga, T. D. (2026). Preventing Bullying in Pesantren: A Maqāṣid al-Sharī 'ah and Hadith Perspective on the Role of the Sakinah Family. *Al-Insyiroh: Jurnal Studi Keislaman*, *12*(1), 1–17. https://doi.org/10.35309/alinsyiroh.v12i1.633

Husaini, A., Mas'ud, M., Cahyadi, G., & Aji Pratama, S. W. (2026). Vasectomy as Social Assistance Policy Discourse: A Normative Juridical Analysis from Ibn ʿUthaymīn's Fatwa. *AT-TURAS: Jurnal Studi Keislaman*, *13*(1), 1–14. https://doi.org/10.33650/at-turas.v13i1.13486

Imran, M. F., Gunawan, H., & Asmoro, D. (2024). Addressing The Hurdles: Enhancing Better Policies In Indonesia Cyber Security Management Amidst Uncertainty. *Jurnal Manajemen Pelayanan Publik*, *8*(2), 275–290. https://doi.org/10.24198/jmpp.v8i2.52212

Korbatieh, S. (2020). Evidence Laws in Sharia and the Impact of Modern Technology and DNA Testing. *Australian Journal of Islamic Studies*, *5*(3), 4–29. https://doi.org/10.55831/ajis.v5i3.303

La Harisi, I., Mas'ud, M., Imran, A., & Amien, M. Y. (2026). Algorithms, Religious Authority, and Digital Da'wah: A Qualitative Study of Social Media in Indonesia. *Journal of Mathematics Instruction, Social Research and Opinion*, *5*(1). https://doi.org/10.58421/misro.v5i1.1322

Lensa, H. W., Mas'ud, M., Solehuddin, S., & Atsal, D. (2026). The Authority of Ḥadīth in Tafsīr bi al-Maʾthūr: A Critical Study of Fabricated Narrations on the Virtues of Sūrat Yāsīn in al-Durr al-Manthūr. *Tut Wuri Handayani: Jurnal Keguruan Dan Ilmu Pendidikan*, *5*(1), 9–17.

Liu, C., & Babar, M. A. (2024). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*, *51*(1), 62–92. https://doi.org/10.1177/03128962241293658

Marwan Mas'ud, Muhid, Isnaini Lu'lu' Atim Muthoharoh, & Mohammed Alghiffar Alwalid. (2025). تحليل حكم "أصحُّ شيء" في كتاب التلخيص الحبير: دراسة حول درجة الحديث الضعيف. *Maʿālim*, *21*(1), 82–106. https://doi.org/10.33102/jmqs.v21i1.526

Mas' ud, M., Asy'ari, E. H. N., La Harisi, I., & Arceri, M. (2026). بولتيرآبند في منظور فقه النكاح الإسلامي. *An-Nikah: Jurnal Pernikahan Islam*, *1*(2), 146–160.

Mas' ud, M., Lensa, H. W., & Azizi, N. H. (2025). دور فن الطهي وقيمه من خلال الحديث النبوي: دراسة موضوعية (في ضوء أحاديث الصحيحين). *As-Sunnah: Jurnal Ilmu Dirayah*, *1*(1), 128–174.

Mas' ud, M., Lensa, H. W., Laksana, A. B. S., & Maarif, S. (2026). أهمية الوعي بالآخرة في تحقيق استقرار الأمن الأسري في ضوء الحديث النبوي (دراسة موضوعية من خلال أحاديث الصحيحين). *Tahdis: Jurnal Kajian Ilmu Al-Hadis*, *17*(01). https://doi.org/10.24252/tahdis.v17i01.62670

Mas' ud, M., & Rizqi, N. A. (2025). الموكويُوشي والهوية النَّسَبيَّة:(دراسة فقهية في الأحوال الشخصية حول ظاهرة التبنِّي الرَّشِيد للرجال البالغين في اليابان). *Al-Mawaddah: Jurnal Hukum Dan Ekonomi Keluarga Islam*, *1*(2), 131–148.

Mas' ud, M., Rizqi, N. A., & others. (2026). تحليل الرواة المحكوم عليهم بالمطروح في كتاب ميزان الاعتدال للذهبي (دراسة استقرائية مقارنة): An Analysis of Narrators Judged as Maṭrūḥ in al-Dhahabī's Mīzān al-Iʿtidāl (A Comparative Inductive Study). *Ulūm Al-Sunnah*, *4*(01), 01–11. https://doi.org/10.5281/zenodo.19652544

Mas' ud, M., Tujang, B., Fadhil, M., & Prayoga, T. D. (2026). تحليل الرواة الذين حُكِمَ عليهم بالمطروح في كتاب سير أعلام النبلاء (دراسة استقرائية مقارنة). *AL-ATSAR: Jurnal Ilmu Hadits*, *4*(1). https://doi.org/10.37397/al-atsarjurnalilmuhadits.v4i1.1365

MAS'UD, M. (2021). *[illegible]* [PhD Thesis]. Sekolah Tinggi Dirasat Islamiyah Imam Syafi'i Jember.

Masud, M., Amien, M. Y., & Ihcsan, C. M. (2025). المفاضلة بين الرواة عند أبي نعيم الفضل بن دكين: دراسة نظرية تطبيقية. *Al-Khabar: Jurnal Ilmu Riwayah*, *1*(1), 58–80.

Mas'ud, M., Penataran, R. G., & Putra, D. H. (2026). The urgency of preventing online gambling in realizing family security stability in the perspective of the prophetic hadith (A Thematic Study Based on the Hadiths in al-Kutub al-Sittah): A Thematic Study Based on the Hadiths in Al-Kutub al-Sittah. *As-Sunnah: Jurnal Ilmu Dirayah*, *1*(2), 25–48.

Mas'ud, M., Said, I. G., & Alwalid, M. A. (2025). Ḍaʿīf jiddan vs. Mawḍūʿ: a Comparative Assessment of Ḥadīth by Ibn al-Jawzī in al-Mawḍūʿāt and al-ʿirāqī in al-Mughnī ʿan Ḥaml al-Asfār fī al-Asfār. *Al-Majaalis : Jurnal Dirasat Islamiyah*, *13*(1), 107–129. https://doi.org/10.37397/al-majaalis.v13i1.1130

Mas'ud, M., Wicaksono, T., & Cahyadi, T. D. (2026). A Thematic Study of the Book Maʿrifah ʿulum Al-Ḥadith: An Analysis of the Classification of 'Illah from Al-Ḥākim's Perspective. *IJUS| International Journal of Umranic Studies*, *9*(1), 13–32.

Meerangani, K. A., Ibrahim, A. F., Omar Mukhtar, M. Y., Mat Johar, M. H., Badhrulhisham, A., & Ahmad Termimi, M. A. (2022). Cybercrime and its Violation of Digital Platform Security: An Islamic Law Perspective. *International Journal of Academic Research in Progressive Education and Development*, *11*(3). https://doi.org/10.6007/ijarped/v11-i3/14564

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), 23–48.

Mohammed, T. A. S. (2024). A scientometric study of Maqasid al-shariah research: Trending issues, hotspot research, and co-citation analysis. *Frontiers in Research Metrics and Analytics*, *9*. https://doi.org/10.3389/frma.2024.1439407

Muhammadong, M. (2025). The Role of Maqāṣid Al-Sharī'ah in Promoting Sustainable Development: A Study Within Islamic Legal Framework. *Jurnal Budi Pekerti Agama Islam*, *3*(5), 136–146. https://doi.org/10.61132/jbpai.v3i5.1508

Muhtadin, S., Abd.Muthalib, Mas'ud, M., Yassir, M., & Sidiq, R. M. (2026). Integrating Islamic Legal Literacy and Family Support in Shaping Marriage Readiness: A Structural Equation Modeling Approach: Integrasi Literasi Hukum Islam dan Dukungan Keluarga dalam Membentuk Kesiapan Menikah: Pendekatan Model Persamaan Struktural. *Jurnal Ilmu Keluarga Dan Konsumen*, *19*(1), 15–26. https://doi.org/10.24156/jikk.2026.19.1.15

Mulahuwaish, A., Qolomany, B., Gyorick, K., Abdo, J. B., Aledhari, M., Qadir, J., Carley, K., & Al-Fuqaha, A. (2025). A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects. *Computers in Human Behavior Reports*, *18*, 100668. https://doi.org/10.1016/j.chbr.2025.100668

Nasrulloh, E. H., Mas' ud, M., & Harsaputra, T. K. (n.d.). *The Concept of Forgiveness in the Qur'an: A Qur'anic Approach to Mental Health*.

Perera, S., Jin, X., Maurushat, A., & Opoku, D.-G. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics*, *9*(1), 28. https://doi.org/10.3390/informatics9010028

Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. *International Journal of Information Management*, *74*, 102719. https://doi.org/10.1016/j.ijinfomgt.2023.102719

Ramadhansyah, A., Mas'ud, M., & Lensa, H. W. (2025). المفاضلة بين الرواة عند عبد الله بن المبارك (دراسة نظرية تطبيقية): The Preferential Evaluation Among Narrators According to Abdullah bin al-Mubārak: A Theoretical and Applied Study. *Journal Of Hadith Studies*, 51–70. https://doi.org/10.33102/johs.v10i2.392

Rohman, T., Huda, U., & Hartono, H. (2020). Methodology of Hadith Research: The Study of Hadith Criticism. *Journal of Hadith Studies*, *2*(1), 73–84. https://doi.org/10.32506/johs.v2i1.26

Rosli, W. R. W. (2025). Waging warfare against states: The deployment of artificial intelligence in cyber espionage. *AI and Ethics*, *5*(1), 47–53. https://doi.org/10.1007/s43681-024-00628-x

Saleh, A., & Mas'ud, M. (2025). Anomali Istidlal Perang Jamal terhadap Bolehnya Kepemimpinan Wanita. *AL-ATSAR: Jurnal Ilmu Hadits*, *2*(2), 38–51. https://doi.org/10.37397/al-atsarjurnalilmuhadits.v2i2.431

Salim, D. T., Singh, M. M., & Keikhosrokiani, P. (2023). A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model. *Heliyon*, *9*(7), e17156. https://doi.org/10.1016/j.heliyon.2023.e17156

Saydullayevich, B. Z. (2025). The role of the social state in enhancing civic responsibility in society. *Journal of Multidisciplinary Academic and Practice Studies*, *3*(2), 149–158. https://doi.org/10.35912/jomaps.v3i2.3260

Sayudi, M., & Parmujianto, P. (2023). Taxpayer Compliance Behavior on Muslim Micro, Small, and Medium Enterprise Actors in Pasuruan City Indonesia. *Akademika : Jurnal Pemikiran Islam*, *28*(2), 179. https://doi.org/10.32332/akademika.v28i2.7711

Sears, C. R., & Cunningham, D. R. (2024). Individual Differences in Psychological Stress Associated with Data Breach Experiences. *Journal of Cybersecurity and Privacy*, *4*(3), 594–614. https://doi.org/10.3390/jcp4030028

Shandler, R., & Gomez, M. A. (2022). The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics*, *20*(4), 359–374. https://doi.org/10.1080/19331681.2022.2112796

Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., & Trück, S. (2023). The nature of losses from cyber-related events: Risk categories and business sectors. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyac016

Shulruff, T. (2024). Trust and Safety work: Internal governance of technology risks and harms. *Journal of Integrated Global STEM*, *1*(2), 95–105. https://doi.org/10.1515/jigs-2024-0003

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab019

Subhani, Z. H. (2023). Jasser Auda (2021). Re-Envisioning Islamic Scholarship: Maqasid Methodology as a New Approach. UK: Claritas Books & Maqasid Institute. 282 Pages. [ISBN: 978-1-80011-977-2]. *Journal of Al-Tamaddun*, *18*(2), 299–303.

Tajedini, O., Khasseh, A. A., Afzali, M., & Sadatmoosavi, A. (2019). How to increase the loyalty of public library users? A qualitative study. *Journal of Librarianship and Information Science*, *52*(2), 317–330. https://doi.org/10.1177/0961000619856081

Zaprulkhan, Z. (2018). Maqāṣid Al-Shariah in the Contemporary Islamic Legal Discourse: Perspective of Jasser Auda. *Walisongo: Jurnal Penelitian Sosial Keagamaan*, *26*(2), 445. https://doi.org/10.21580/ws.26.2.3231

Zhou, F., & Huang, J. (2024). Cybersecurity data breaches and internal control. *International Review of Financial Analysis*, *93*, 103174. https://doi.org/10.1016/j.irfa.2024.103174