Social Sciences & Humanity Research Review
ISSN 3007-3170(O), ISSN :3007-3162(P)
Volume 3 issue 1,pp. 626-645
January-March 2025

Received: 25 January 2025 ,Accepted: 05 March 2025
DOI:

THE ROLE OF INTERNATIONAL LAW IN AI DRONE REGULATIONS

[1]*MS Shahzadi Sarwat Noreen*, [2]*Talat Ara*

1. Former Member District Assembly Sargodha Punjab, Former Editor & Lawyer
2. Economist, Educator, & Co-Founder Global Peace & Prosperity Initiative(Think Tank)

Correspondent email: sarwat_talal@hotmail.com

ABSTRACT

The rapid expansion of artificial intelligence (AI) in surveillance and drone technologies has redefined modern security paradigms but has also introduced severe vulnerabilities. AI-driven surveillance systems are increasingly being used for intelligence gathering, cyber espionage, and hybrid warfare. However, weak global regulatory oversight has allowed foreign surveillance manufacturers to infiltrate national security infrastructures. The 2020 India-China border tension at Galwan Valley serves as a critical case study, highlighting the risks of relying on foreign-manufactured surveillance technology. Reports indicate that Zhenhua Data, a Chinese surveillance technology manufacturer, allegedly manipulated and gained access to India's security networks, including sensitive sites, as a show of cyber dominance. This alarming precedent extends beyond India, as many nations, particularly in Europe, Africa, and South America, rely on Chinese-manufactured AI surveillance equipment due to its low cost, putting global privacy and national security at stake. Building on the pioneering work of Hassan Rasheed Siddiqui and Maria Muniza, who have extensively analyzed the regulatory gaps in AI surveillance and drone technology, this paper argues that current regulatory measures—such as selective bans on certain surveillance manufacturers—fail to address the transnational risks posed by AI surveillance. This study proposes a comprehensive global policy framework, including the prohibition of foreign-made AI surveillance technology, stringent licensing for AI surveillance manufacturers, enhanced cybersecurity protocols, and international intelligence-sharing agreements. Without immediate action, nations will remain vulnerable to AI-driven cyber infiltration and surveillance warfare.

KEYWORDS: *Artificial Intelligence (AI), Surveillance Technologies, Cyber Espionage, AI Surveillance Drones, Cyber Warfare, Hybrid Warfare*

1. INTRODUCTION

The integration of artificial intelligence (AI) into surveillance and drone technologies has revolutionized intelligence gathering and security operations worldwide. Governments, law enforcement agencies, and private corporations increasingly deploy AI-driven systems for border control, crime prevention, and military applications. However, the rapid expansion of these technologies has outpaced regulatory measures, leading to significant privacy violations, security risks, and increased susceptibility to cyber warfare (Broeders, 2022).

Recent studies, particularly those by Siddiqui and Muniza (2025), emphasize that AI-powered surveillance is a key element of hybrid warfare, enabling nations to exploit digital vulnerabilities for geopolitical advantage. Their research highlights the lack of comprehensive international regulations, leaving countries exposed to cyber manipulation by foreign actors.

This paper examines the case study of the 2020 Galwan Valley incident, where Chinese surveillance technology manufacturer Zhenhua Data allegedly manipulated India’s security systems to assert cyber dominance. This incident is not an isolated case—it demonstrates a global security crisis, as many nations continue to equip their surveillance infrastructure with foreign-manufactured AI technology, particularly from China. This study builds upon Siddiqui and Muniza’s research to critically analyze the risks posed by foreign AI surveillance technologies and propose urgent global policy interventions to safeguard national security and privacy rights (Buchanan, 2020).

1.1 Background

1.1.1 The Expansion of AI-Equipped Surveillance Technologies

The proliferation of AI-driven drones and surveillance systems has reshaped modern security practices. Governments worldwide have invested in AI-powered technologies that integrate facial recognition, predictive analytics, and real-time monitoring into security networks. However, Siddiqui and Muniza (2025) argue that the absence of global regulations has allowed AI surveillance to become a tool for geopolitical manipulation and cyber warfare.

One of the biggest concerns is the dominance of Chinese surveillance manufacturers in global markets. Companies such as Zhenhua Data, Huawei, and Hikvision provide AI surveillance technologies to various nations at low costs, making them attractive but highly risky investments (Clarke, & Knake, (2019).

1.1.2 The 2020 Galwan Valley Incident: A Case Study in AI Surveillance Warfare

The India-China border conflict at Galwan Valley in 2020 offers a real-world example of how AI-powered surveillance can be exploited in geopolitical tensions. Reports indicate that Zhenhua Data, a Chinese surveillance and data intelligence company, had embedded AI-driven surveillance technology into India's security infrastructure (Lin, & Singer, 2017).

Key Findings from the Incident:

1. Zhenhua Data's AI-powered surveillance systems were integrated into Indian border security networks.
2. During the heightened military standoff, Chinese cyber units allegedly exploited vulnerabilities in these systems to access and manipulate Indian security networks.
3. This act of cyber infiltration was reportedly a deliberate show of power, demonstrating China's ability to override India's security infrastructure.
4. The incident exposed a critical security risk for all nations reliant on foreign-made AI surveillance systems.

This case study highlights the urgent need for regulatory intervention to prevent nations from losing control over their own security networks due to dependence on foreign-manufactured surveillance technology (Ramachandran, 2021).

1.2 Rational of the study

The rapid growth of artificial intelligence (AI) in surveillance and drone technologies has fundamentally altered security paradigms across the world. While AI-driven systems are crucial for intelligence gathering and security operations, they have introduced significant vulnerabilities. The use of foreign-manufactured AI surveillance equipment, such as that from

Chinese manufacturers, has allowed foreign entities to potentially manipulate and access national security infrastructures. This study is driven by the need to understand and address these vulnerabilities and propose a framework to safeguard national security from AI-driven cyber threats.

1.3 Statement of the problem

Current global regulatory measures on AI-equipped drones and surveillance technologies are inadequate in addressing the transnational risks posed by foreign-manufactured systems. A lack of cohesive international regulations has allowed for foreign surveillance equipment, such as those manufactured by Chinese companies, to infiltrate national security networks. The 2020 India-China border tensions at Galwan Valley, wherein Chinese surveillance technology allegedly infiltrated India's security networks, highlights the urgency of addressing these issues. Nations, particularly in Europe, Africa, and South America, continue to use these technologies due to their low cost, exposing them to vulnerabilities related to cyber espionage and surveillance warfare.

1.4 Research Objectives

This research aims to analyze the security, privacy, and ethical risks associated with AI-equipped drones and surveillance technologies. The study builds upon the pioneering work of Hassan Rasheed Siddiqui and Maria Muniza, who have extensively highlighted the regulatory gaps in AI-driven surveillance and its implications for national security.

This paper seeks to:

1. Identify the risks posed by AI-powered drone technology, including espionage, cyber warfare, and privacy violations.
2. Examine how foreign nations use AI-driven drones and surveillance tools to bypass international restrictions.
3. Assess existing regulatory frameworks and their shortcomings in controlling the global misuse of AI-driven surveillance technology.
4. Provide policy recommendations for a globally coordinated regulatory framework to ensure ethical AI governance and national security protections.

1.6 Significance of the study

This study is significant because it identifies the serious risks posed by the growing reliance on AI-driven surveillance technologies that are manufactured abroad, especially by countries with interests that may not align with national security. The findings will contribute to the development of a comprehensive global regulatory framework, which includes measures like the prohibition of foreign-made AI surveillance technologies, stricter licensing procedures, and enhanced cybersecurity protocols. By addressing these concerns, this study will aid in protecting global privacy, preventing cyber espionage, and reducing the risks of surveillance warfare.

2. METHODOLOGY

This study employs a qualitative research approach that combines several methods to comprehensively address the issue of AI-driven surveillance technologies and their regulation. First, Document Analysis is utilized by reviewing key publications by Siddiqui and Muniza (2024, 2025), along with other scholarly works that explore the dynamics of AI surveillance technologies and their associated risks. In addition, Comparative Legal Analysis is conducted to evaluate the effectiveness of existing regulatory frameworks, such as the European Union’s General Data Protection Regulation (GDPR) and U.S. policies on AI surveillance technologies, to determine their adequacy in addressing transnational security threats. The study also incorporates Case Studies, particularly analyzing real-world instances of AI surveillance misuse, including China’s deployment of AI-powered drones and the security implications they have on global stability. Finally, a Policy Review is carried out, assessing how different nations regulate AI-driven drone manufacturing, with a focus on identifying policy gaps and proposing improvements to enhance the security and ethical use of such technologies (U.S. Department of Commerce, 2024).

3. LITERATURE REVIEW

3.1 The Regulatory Void in AI-Equipped Surveillance Technologies

Siddiqui and Muniza (2025) emphasize the regulatory gaps that exist in the rapidly expanding field of AI-driven surveillance technologies, particularly drones. They argue that the lack of comprehensive regulation exposes civil liberties and national sovereignty to significant threats. Their work reveals that while some countries implement selective bans on specific manufacturers, such as those from China, these measures are insufficient. They focus too narrowly on individual companies, failing to address the broader AI surveillance ecosystem that involves complex global supply chains and transnational security risks. This leaves countries vulnerable to foreign influence and cyber espionage through unregulated or inadequately monitored surveillance technologies (Tang, 2024).

3.2 National Security Concerns and Hybrid Warfare

Siddiqui and Muniza (2025) further discuss the critical role of AI-powered drones in modern hybrid warfare, where they are used for intelligence gathering, cyber-attacks, and exerting geopolitical influence. They highlight China's National Intelligence Law (2017/18), which requires Chinese companies to cooperate with government agencies by sharing surveillance data. This law raises serious concerns about espionage and potential data breaches, particularly when Chinese AI surveillance equipment is deployed in foreign nations. The authors argue that such practices could jeopardize national security by providing foreign government's access to sensitive information, thus underscoring the need for stronger international regulatory frameworks to prevent misuse of AI-driven surveillance technologies (Rosenbach, & Mansted, 2019).

3.3 Privacy Violations and Ethical Implications

The ethical implications of AI-driven mass surveillance are thoroughly examined in The Drone's Gaze: Religious Perspectives on Privacy and Human Dignity in the Age of Surveillance (Siddiqui & Muniza, 2024). The study delves into how AI technologies, particularly facial recognition, behavior prediction, and unauthorized data collection, erode individual privacy and compromise human dignity. Siddiqui and Muniza (2024) argue that these technologies, which are increasingly used in surveillance drones, not only infringe upon the right to privacy but also dehumanize individuals by reducing them to data points. The ethical concerns raised in their work underscore the need for a regulatory framework that ensures privacy protections are not sacrificed in the pursuit of national security or technological advancement.

3.4 The Shortcomings of Existing Regulations

Siddiqui and Muniza (2025) also critique existing regulatory measures, highlighting their insufficiency in addressing the broader scope of AI surveillance technologies. They note that while the European Union’s General Data Protection Regulation (GDPR) (2018) places restrictions on data collection, it does not specifically regulate the use of AI-powered drones, leaving a critical gap in safeguarding privacy. Similarly, the U.S. ban on Chinese-manufactured drones (2024) targets only a few companies, failing to address the issue comprehensively. The study points out that despite these selective measures, alternative manufacturers continue to supply AI-driven surveillance technology worldwide, exposing nations to the same security and privacy risks. The authors argue that without a more robust and unified regulatory approach, these regulatory shortcomings will continue to undermine global privacy and national security (Stokes, 2023).

3.5 The Expansion of AI-Equipped Surveillance Technologies

The rapid expansion of AI-driven drones and surveillance systems has been observed across a variety of industries, with notable applications in security, law enforcement, and border control. Both China and the United States have significantly invested in integrating AI-powered surveillance technologies, such as facial recognition, predictive analytics, and real-time monitoring capabilities, into their security infrastructures. These technologies are increasingly seen as essential tools for enhancing national security, surveillance, and law enforcement operations. AI-powered surveillance systems allow for more efficient tracking, identification, and monitoring of individuals, potentially improving security measures and preventing crime (Smith, 2022).

However, Siddiqui and Muniza (2025) argue that the absence of coherent international regulations surrounding these technologies has led to unchecked development and deployment, which opens the door for misuse. They highlight how countries, especially those with less stringent regulations, may utilize AI surveillance systems in ways that compromise privacy and ethical standards. A major concern, particularly with the widespread use of AI surveillance in China, is the country’s National Intelligence Law (2017/18), which compels domestic technology firms to share surveillance data with government agencies. This legislation raises significant concerns about espionage, data manipulation, and the potential for geopolitical influence through

AI surveillance tools. Such practices are not only a threat to privacy but also introduce risks to international relations and the sovereignty of nations that rely on foreign surveillance technology (Taylor, 2023).

3.6 Ethical and Privacy Concerns

The deployment of AI-powered drones and surveillance systems brings forth profound ethical concerns, particularly with regard to privacy and human rights. Siddiqui and Muniza (2024) delve into these issues through a religious and cultural lens, arguing that AI-driven surveillance technologies fundamentally violate principles of human dignity and privacy. Their research, published in Al-Qamar Journal, highlights that AI surveillance, particularly through tools such as facial recognition and biometric tracking, disproportionately affects marginalized communities. These groups are often subjected to invasive monitoring, raising issues of fairness and equality in the application of these technologies. Moreover, the use of AI surveillance technologies can infringe on religious and cultural values, particularly in societies where privacy and personal freedom are seen as integral to human dignity. In such contexts, the use of AI for mass surveillance by governments and corporations is seen as exploitative, with little to no public accountability (Patel, 2022).

Siddiqui and Muniza (2024) argued that these technologies erode public trust, as they are often deployed without consent or transparent oversight. The authors assert that the unchecked rise of AI surveillance systems can lead to a dystopian reality where individuals' private lives are constantly monitored, thus undermining essential human rights and freedoms. This growing trend of AI surveillance technology necessitates a reevaluation of its ethical implications and a more robust regulatory approach to ensure that these technologies do not infringe on fundamental privacy rights.

3.7 The Security Threat of Foreign-Made AI Surveillance Technologies

The growing reliance on foreign-made AI surveillance technologies has raised significant security concerns across many countries. In response to these concerns, several nations, including the United States, have taken steps to limit the use of surveillance technology from foreign manufacturers, particularly those from China. In 2024, the U.S. imposed a limited ban on certain Chinese AI surveillance companies, citing fears of espionage, data breaches, and the potential for geopolitical manipulation. While this move addresses immediate security concerns, Siddiqui and Muniza (2025) argue that such selective bans are inadequate in tackling the larger issue of the unrestricted global proliferation of AI surveillance technologies. They contend that these piecemeal bans only target a few companies, leaving a vast space open for other foreign manufacturers to fill the gap. This fragmented approach does not address the systemic risks posed by the widespread use of AI surveillance technologies, which could be misused for cyber espionage, data theft, and other forms of digital warfare. As these technologies continue to spread across the globe, nations become increasingly vulnerable to external control over their surveillance infrastructure, which could compromise their security and sovereignty (Bhattacharya, 2022).

3.8 Prohibition of Foreign-Made AI Surveillance Technology

To effectively safeguard national security, Siddiqui and Muniza (2025) advocate for a more comprehensive and stringent approach to regulating AI surveillance technologies. They propose that governments should implement an outright ban on AI surveillance technologies manufactured by foreign entities, especially those with ties to adversarial nations. This would prevent the infiltration of foreign surveillance tools that could potentially be used for espionage or other harmful purposes (Nandan, 2021).

Furthermore, Siddiqui and Muniza (2025) emphasize the importance of prioritizing domestic AI development. By fostering the creation and deployment of homegrown AI surveillance technologies, governments can maintain greater control over their security infrastructure, minimizing the risks posed by foreign-made systems. They argue that domestic development not only strengthens national security but also ensures that surveillance technologies are subject to local laws, regulations, and ethical standards, preventing the exploitation of AI for malicious purposes. In this way, countries can mitigate the risks associated with foreign surveillance technologies while promoting innovation and self-reliance in the critical field of AI surveillance.

3.9 Global AI Surveillance Governance Framework

To address the growing challenges posed by AI surveillance technologies, Siddiqui and Muniza (2025) advocate for the creation of a unified international regulatory body dedicated to overseeing the manufacturing, distribution, and deployment of AI surveillance systems. This global governing body would ensure that AI surveillance technologies are developed and used in compliance with international standards of ethics, security, and privacy. A central regulatory body would also help prevent regulatory loopholes that foreign manufacturers could exploit, fostering transparency and cooperation across borders. Additionally, mandatory licensing requirements must be enforced for all AI surveillance technology manufacturers. By imposing strict licensing criteria, governments can ensure that only compliant and vetted companies are allowed to produce and distribute these powerful technologies. These requirements would enforce ethical guidelines, security protocols, and transparency in the development and deployment of AI surveillance tools, ultimately mitigating the risks associated with unchecked surveillance capabilities.

3.10 Strengthening Cybersecurity Measures

Given the critical nature of AI-powered surveillance systems in modern security infrastructure, Siddiqui and Muniza (2025) emphasize the importance of strengthening cybersecurity measures to protect against potential threats. AI surveillance systems should be equipped with end-to-end encryption and robust cybersecurity protocols to prevent unauthorized access and ensure the confidentiality and integrity of data collected by these systems. These systems should be designed to resist cyber-attacks, including hacking and data breaches, which could have disastrous implications for national security. Furthermore, governments should mandate regular cybersecurity audits for all AI-powered surveillance networks to identify vulnerabilities and ensure that these systems are resilient against emerging threats. These audits would serve as an essential tool for detecting potential weaknesses in surveillance infrastructure, allowing for timely corrective actions to be taken before security breaches occur (Wu, 2023).

3.11 Intelligence and Counter-Surveillance Initiatives

In addition to strengthening cybersecurity measures, international collaboration is crucial for addressing the transnational risks associated with AI surveillance technologies. Siddiqui and Muniza (2025) propose the establishment of international intelligence-sharing agreements to monitor and track the use of AI surveillance technologies, particularly in the context of cyber warfare and espionage. These agreements would foster cooperation among nations, enabling them to share intelligence on emerging threats and suspicious activities involving AI-powered surveillance tools. By working together, nations can better protect their security interests and prevent hostile actors from exploiting these technologies for malicious purposes. Additionally, AI surveillance drones should incorporate geofencing and real-time monitoring features to prevent unauthorized intrusions into sensitive areas. Geofencing would allow security agencies to set geographical boundaries for AI surveillance drones, ensuring that these systems cannot be used for unauthorized surveillance or data collection outside designated areas. Real-time monitoring capabilities would further enhance security by allowing operators to track the location and movements of drones in real time, preventing their misuse for espionage or infiltration. These initiatives would create a comprehensive framework for countering the growing threats posed by AI-powered surveillance technologies (Taylor, 2024).

4. CONCLUSION

The 2020 Galwan Valley incident, in which Zhenhua Data allegedly exploited vulnerabilities in India's surveillance network, serves as a stark reminder of the dangers posed by the unregulated proliferation of AI-driven surveillance systems. This event underscores the urgency for global security policymakers to address the risks of cyber manipulation, espionage, and geopolitical instability caused by the increasing reliance on foreign-made surveillance technologies. Building on the foundational work of Siddiqui and Muniza (2025), this study demonstrates that current piecemeal bans on select surveillance manufacturers are insufficient and ineffective in tackling the broader issue of AI surveillance's unchecked global proliferation.

A comprehensive international regulatory framework is essential to mitigate these risks. This framework should include a ban on foreign-made AI surveillance technologies to prevent cyber manipulation and espionage, along with strict licensing requirements for AI surveillance manufacturers to ensure adherence to cybersecurity and ethical standards. Additionally, strengthening cybersecurity protocols to guard against hacking and unauthorized surveillance is crucial, as is the development of robust counter-surveillance initiatives to track and neutralize AI-driven cyber threats. Without immediate and coordinated international action, nations will remain exposed to the growing dangers of AI-driven cyber warfare, espionage, and security infiltration, leaving their privacy, sovereignty, and national security at risk. The time for a unified global response to these threats is now, before the vulnerabilities become unmanageable.

5. DISCUSSION

The rise of AI-equipped surveillance technologies has brought about significant transformations in national security, law enforcement, and privacy policies. However, as outlined in the previous sections, this technological advancement is accompanied by complex challenges, particularly concerning the security, ethical, and privacy implications of AI-driven systems. The rapid proliferation of foreign-made AI surveillance technologies, often lacking adequate regulation, has heightened global vulnerabilities. The discussions that follow will address the core issues arising from the unregulated use of these technologies, the risks they pose, and the urgency of implementing a robust regulatory framework to mitigate potential harm (Kaspersky, 2023).

5.1 The Security Risks of Foreign-Made AI Surveillance Technologies

One of the primary concerns surrounding AI surveillance technologies is their foreign origin, particularly when these technologies are developed by countries with adversarial interests or those that do not prioritize cybersecurity and ethical standards in the same way as others. The case of China’s surveillance technology, for instance, is emblematic of how AI-powered surveillance systems can be weaponized for espionage and geopolitical influence. As mentioned in the context of the 2020 Galwan Valley incident, the use of foreign-made surveillance equipment, such as that provided by Chinese manufacturers, can lead to significant breaches of national security. Foreign-made AI surveillance technologies often come with inherent risks, as seen with companies like Zhenhua Data, whose alleged actions against India’s security networks underscore the potential for exploitation (White, 2023).

The introduction of AI surveillance systems without proper regulatory oversight allows for vulnerabilities that can be exploited by hostile foreign actors. Governments, particularly in nations with geopolitical tensions, are understandably concerned about allowing foreign companies access to their surveillance infrastructure, which could then be used for purposes like data theft, espionage, and cyber-attacks. Given these concerns, it is crucial that countries consider restricting the use of foreign-manufactured AI surveillance technologies, especially from companies tied to adversarial nations. A comprehensive ban on foreign-made surveillance systems would significantly reduce the risk of espionage and protect sensitive national security information (O'Brien, 2023).

5.2 The Limitations of Current Regulatory Approaches

Existing regulatory frameworks, such as the European Union's General Data Protection Regulation (GDPR) and the limited U.S. ban on Chinese surveillance manufacturers, have attempted to address some of the privacy and security risks posed by AI surveillance technologies. However, Siddiqui and Muniza (2025) highlight that these approaches are fundamentally flawed because they focus primarily on specific manufacturers rather than addressing the broader issue of AI surveillance's unregulated global spread. These piecemeal bans do not prevent other manufacturers from filling the void left by one banned company. As a result, the risks of espionage, data breaches, and cyber-attacks remain present as surveillance technologies continue to evolve and proliferate (Dutta, 2021).

Moreover, while the GDPR imposes strict data collection restrictions, it does not specifically address AI-powered drones and other surveillance technologies, leaving a regulatory gap in a rapidly evolving technological landscape. Governments need to move beyond targeting specific companies and adopt a more comprehensive approach that regulates the entire AI surveillance ecosystem. A global regulatory framework is essential to ensure that AI surveillance technologies are developed, distributed, and deployed in a manner that prioritizes security, privacy, and ethical standards, reducing the risks posed by foreign interference and cyber threats.

5.3 Ethical and Privacy Concerns

The ethical implications of AI-powered surveillance technologies cannot be understated. These systems, particularly facial recognition software and behavioral analytics, pose serious threats to individual privacy and human dignity. Siddiqui and Muniza (2024) have pointed out that AI surveillance technologies often disproportionately target marginalized communities, subjecting them to constant monitoring and surveillance. Additionally, the use of biometric tracking and facial recognition technology infringes upon religious and cultural values, where privacy is viewed as a fundamental human right. The unchecked use of AI surveillance technologies by governments and corporations without public accountability or consent can lead to a violation of these rights, often without individuals being aware of the extent to which they are being monitored (Feldstein, 2021).

As AI surveillance systems continue to proliferate globally, governments must prioritize the protection of privacy rights and ethical standards. This involves not only regulating the technology but also ensuring transparency in its use, informing citizens about the scope and purpose of surveillance efforts. Without clear ethical guidelines and accountability measures, AI surveillance technologies risk becoming tools of oppression, undermining public trust in both governments and private corporations (European Parliament, 2018).

5.4 Cybersecurity Challenges and the Need for Stronger Protections

The implementation of AI surveillance technologies must be accompanied by strong cybersecurity measures to ensure the protection of sensitive data. As noted earlier, these systems are highly susceptible to hacking, data breaches, and unauthorized surveillance. In a world where cyber-attacks are becoming increasingly sophisticated, it is essential that AI surveillance systems integrate end-to-end encryption and advanced cybersecurity protocols to prevent unauthorized access. Governments should enforce mandatory cybersecurity audits for all AI-powered surveillance networks to identify potential vulnerabilities and ensure that systems are robust against evolving cyber threats (Singh, 2022).

These audits should not only focus on identifying technical weaknesses but also assess the broader security infrastructure, including how data is stored, transmitted, and accessed. This would help prevent incidents like the massive data breaches that have occurred in other sectors, which have had far-reaching consequences for individuals and nations alike. As surveillance technologies are integrated into critical national security frameworks, securing these systems from cyber threats becomes paramount (Zhao, 2024).

5.5 The Role of International Collaboration in Addressing AI Surveillance Risks

Given the global nature of AI surveillance technology, national efforts alone will not suffice to mitigate the risks posed by these systems. International collaboration and intelligence-sharing are essential components of a comprehensive response to the threat of AI-driven surveillance. By establishing global intelligence-sharing agreements, nations can monitor the deployment of AI surveillance technologies, particularly those used for cyber warfare, espionage, or unlawful surveillance. This would foster greater transparency and enable countries to detect and counter surveillance technologies that pose a threat to their security and sovereignty (Jones, 2023).

Furthermore, the implementation of counter-surveillance measures, such as geofencing and real-time monitoring for AI surveillance drones, would prevent unauthorized intrusion into sensitive airspace and restricted areas. These technologies would allow security agencies to track the movement of AI surveillance drones and neutralize potential threats in real time (Chen, 2024).

The proliferation of AI-driven surveillance systems presents significant challenges to global security, privacy, and ethical standards. As highlighted throughout this discussion, the current regulatory frameworks are inadequate to address the growing risks posed by foreign-made surveillance technologies and their potential for misuse. Governments must take immediate action to restrict foreign-made AI surveillance technologies, enhance cyber security measures, and establish international collaboration to combat the threats of espionage and cyber warfare. By implementing these recommendations, nations can better protect their citizens' privacy, ensure the ethical deployment of surveillance technologies, and safeguard national security in an increasingly interconnected and technologically advanced world (Gupta, 2021).

6. RECOMMENDATIONS

6.1 Restricting Foreign-Made AI Surveillance Technology

To mitigate national security risks and prevent unauthorized data access, governments should implement nationwide bans on foreign-made AI surveillance technologies. This is essential to safeguard sensitive data and protect national infrastructures from potential espionage or cyber-attacks facilitated by foreign entities. By prohibiting these technologies, nations can limit the risks associated with foreign surveillance tools that may have vulnerabilities or be susceptible to exploitation. Additionally, priority should be given to the development of domestic AI surveillance technology to ensure that surveillance systems remain under the control of national regulatory frameworks, promoting both security and ethical standards.

6.2 Global AI Governance Framework

A unified international AI regulatory body should be established to oversee the global manufacturing, distribution, and deployment of AI-powered surveillance systems. This body would create international standards and guidelines to govern the use of AI surveillance technologies, promoting cooperation among nations. Additionally, mandatory licensing requirements should be introduced for all AI surveillance technology manufacturers. These requirements would enforce compliance with security and ethical standards, ensuring that companies adhere to stringent guidelines before their products are deployed globally. By standardizing regulations, nations can prevent the misuse of AI surveillance technologies and ensure that their deployment aligns with international security protocols.

6.3 Strengthening Cybersecurity Measures

AI surveillance systems must be equipped with advanced cybersecurity features, including end-to-end encryption protocols, to prevent hacking and unauthorized data collection. These systems should be designed to resist cyber threats and protect the sensitive information they collect from being accessed by malicious actors. Governments should also enforce strict cybersecurity audits for all AI-powered surveillance technologies to regularly assess vulnerabilities and ensure the ongoing security of surveillance networks. These audits will help identify weaknesses, enabling timely interventions to mitigate risks associated with cyber-attacks.

6.4 Intelligence and Counter-Surveillance Measures

To further enhance national security, international intelligence-sharing agreements should be established to monitor and track AI surveillance technologies that may be used for espionage or other malicious purposes. Such agreements would foster global collaboration and enable nations to share information on emerging threats, strengthening collective security. Additionally, AI surveillance drones should be equipped with geofencing and real-time tracking features to prevent unauthorized airspace breaches. Geofencing would create secure boundaries for AI drones, ensuring they cannot access restricted areas, while real-time tracking would allow authorities to monitor drone movements and prevent them from being used for illicit surveillance or intelligence gathering. By adopting these recommendations, governments and international bodies can significantly reduce the risks associated with AI-driven surveillance technologies, ensuring they are used safely and ethically while safeguarding national security and individual privacy.

REFERENCES

Anderson, P. (2023). Hacking Democracy: Cybersecurity and Foreign Surveillance in Electoral Systems. Digital Policy Studies, 17(3), 251–276.

Bhattacharya, K. (2022). The Politics of AI Surveillance: Nationalism vs. Globalization. Digital Governance Review, 10(1), 89–116.

Braw, E. (2020). Hybrid Warfare: The Weaponization of AI and Cybersecurity. International Journal of Cyber Studies, 6(1), 112–130.

Broeders, D. (2022). The Governance of Surveillance Technologies: Global Risks and National Interests. Cyber Policy Review, 15(3), 301–318.

Buchanan, B. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press.

Chen, L. (2024). AI and the Rise of Smart Warfare: Implications for Global Security. Journal of Global Intelligence, 19(2), 312–340.

Clarke, R. A., & Knake, R. (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin.

Dutta, R. (2021). India’s AI Security Strategy: Lessons from the Galwan Valley Cyberattack. South Asian Security Studies, 5(2), 132–158.

European Parliament (2018). General Data Protection Regulation (GDPR).

Feldstein, S. (2021). The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance. Oxford University Press.

Gupta, R. (2021). India’s Surveillance Infrastructure: Vulnerabilities and Policy Recommendations. South Asian Cybersecurity Review, 4(2), 98–120.

Jones, C. (2023). The Ethics of AI in Warfare: Drones, Surveillance, and Human Rights Concerns. Journal of Military Ethics, 22(1), 45–67.

Kaspersky, E. (2023). Cyber Espionage: A Modern Warfare Tactic. Journal of Cyber Intelligence, 5(1), 210–230.

Klein, A. (2023). The Future of AI in Military Surveillance: Challenges and Solutions. Strategic Defense Policy Review, 6(3), 111–136.

Lin, H., & Singer, P. (2017). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

Nandan, D. (2021). Chinese Hybrid Warfare Strategy: A Threat to India's National Security. ResearchGate. https://www.researchgate.net/publication/351660031_CHINESE_HYBRID_WARFARE_STRATEGY_A_THREAT_TO_INDIA'S_NATIONAL_SECURITY

O’Brien, P. (2023). The Dark Side of AI: How Surveillance Technologies Are Undermining Privacy. Journal of Ethics in AI, 8(3), 56–77.

Patel, N. (2022). The Role of AI in Espionage: Risks and Global Countermeasures. Journal of Advanced Security Studies, 15(2), 178–202.

Ramachandran, S. (2021). The India-China Border Conflict: Cyber and Surveillance Warfare at Galwan Valley. Defence& Security Journal, 9(3), 201–225.

Robinson, N. (2022). AI Warfare: The Future of Military Conflicts in the Digital Age. Journal of Strategic Defense, 10(2), 85–102.

Rosenbach, E., & Mansted, K. (2019). The Geopolitics of Artificial Intelligence and Surveillance. Harvard Kennedy School.

Siddiqui, H. R., & Muniza, M. (2024). The Drone’s Gaze, Religious Perspective on Privacy and Human Dignity in the Age of Surveillance. Al-Qamar Journal, December, 1-12.

Siddiqui, H. R., & Muniza, M. (2024). The Drone’s Gaze, Religious Perspective on Privacy and Human Dignity in the Age of Surveillance Mentioning Security Threats & Regulatory Gaps. Al-Qamar, 7(4), 1-12. https://doi.org/10.53762/alqamar.07.04.e01

Siddiqui, H. R., & Muniza, M. (2025). Hybrid Warfare and the Global Threat of Data Surveillance: The Case for International Standards and Regulation. Pakistan Social Sciences Review, 9(1), 519–531.

Siddiqui, H. R., & Muniza, M. (2025). Regulatory Gaps in Drone Surveillance: Addressing Privacy, Security, and Manufacturing Standards. Annals of Human and Social Sciences, 6(1), 415–428.

Singh, A. (2022). Geopolitical Risks of AI-Driven Surveillance Technologies. Global Policy Journal, 11(4), 355–380.

Smith, J. (2022). AI Ethics and the Future of Surveillance. Oxford University Press.

Stokes, J. (2023). AI-Powered Surveillance and Its Implications for National Security. Journal of Global Security Studies, 8(2), 205–229.

Tang, F. (2024). China's AI and Surveillance Strategy: A New Era of Cyber Espionage. Asian Security Studies, 12(4), 359–378.

Taylor, M. (2023). Cybersecurity Challenges in AI-Driven Surveillance. Cambridge University Pres

Taylor, M. (2024). AI, National Security, and the Ethics of Surveillance. Journal of International Law & Policy, 28(1), 57–78.

U.S. Department of Commerce (2024). Ban on Chinese AI Surveillance Manufacturers.

UN Special Rapporteur on Privacy (2023). AI and Mass Surveillance: Global Concerns and Recommendations.

White, S. (2023). Countering AI-Powered Cyber Threats in Surveillance Technologies. Journal of Cyber Defense Strategies, 14(2), 221–249.

Wu, X. (2023). China's Digital Silk Road: Surveillance, Influence, and Cyberpower. Asian Cyber Studies, 7(1), 144–168.

Zhao, Y. (2024). The Role of Chinese Surveillance Manufacturers in Global Cybersecurity. East Asia Policy Review, 8(3), 112–139.