Journal of Contemporary Issues in Business and Government Vol. 31, No. 02, 2025
https://cibgp.com P-ISSN :2204-1990; E-ISSN: 1323-6903

EVALUATING THE NATIONAL SECURITY AND ECONOMIC CONSEQUENCES OF U.S. RESTRICTIONS ON FOREIGN DRONES

[1*]Naveed Hussain
[1*]Gold Medalist In L.L.B. International Islamic University Islamabad. Deputy District Prosecutor, Islamabad. Pakistan, Adv.rajanaveed@gmail.com

To Cite This Article: Hussain, N. . (2025). EVALUATING THE NATIONAL SECURITY AND ECONOMIC CONSEQUENCES OF U.S. RESTRICTIONS ON FOREIGN DRONES. The Journal of Contemporary Issues in Business and Government, 31(2), 1–14. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2881

Received: 03/2025 **Published:05/2025**

ABSTRACT
This work investigates not only about the increasing use of overseas produced drones (especially of Chinese and Russian companies) in the U.S., but also the potential consequences on the national security, sectors and economic strength. The Commerce Department has restricted these drones on the grounds of spying threats, vulnerability to cyber-security risks as well as the integration of AI (Artificial Intelligence) chips inside them. These risks involve things like data exfiltration, AI model poisoning and firmware backdoors that could all impact sensitive data and national security. But the ban has also presented extensive operational and economic hardships, particularly in sectors that depend on drones, including agriculture, emergency response and infrastructure inspections. These are companies that rely on low-cost foreign drones such as DJI and this need for affordable local alternatives has hampered the fortunes for them leading to higher operational costs and inefficiencies. The paper goes on to argue that these issues prompt a consideration of an equilibrium approach to regulation. A total ban on all foreign drones may be unwise, but a more selective policy that focuses on models we know represent a risk to our national security could be used to neutralize these threats without damaging vital areas of the economy. The research also suggest that there should be investment for manufacturing of drones domestically, robust cyber security for AI managed drones and public-private partnership to promote innovation in domestic UAV sector. Doing so will allow the U.S. government to protect national security while minimizing economic dislocation and maintaining forward momentum in areas that rely on drone technology.

Keywords: U.S. drone ban, AI surveillance security, national security, foreign-manufactured drones, cyber security vulnerabilities, MAC address tracking, policy alternatives.

INTRODUCTION
The exponential rise in the global deployment of foreign-manufactured surveillance technologies—particularly drones and AI-powered systems—has intensified concerns over cybersecurity vulnerabilities, espionage threats, and growing economic reliance on overseas suppliers. Mr. Hassan Rasheed Siddiqui and Ms. Maria Muniza have been at the forefront of highlighting these issues, offering critical legal and policy insights into the risks posed by unregulated surveillance technologies, especially those originating from China and Russia. Through a series of influential publications, they have drawn early attention to China's National Intelligence Law, the strategic implications of the Zehna case in the Galwan Valley, and the growing global dependence on Chinese-manufactured surveillance systems due to their competitive pricing and mass production capabilities.

In their joint works—Regulatory Gaps in Drone Surveillance: Addressing Privacy, Security, and Manufacturing Standards (Annals of Human and Social Sciences, 2025), Hybrid Warfare and the Global Threat of Data Surveillance (Pakistan Social Sciences Review, 2025), and The Drone's Gaze: Religious Perspective on Privacy and Human Dignity (Al-Qamar, 2024)—Siddiqui and Muniza analyze the multifaceted threats posed by these technologies. Their articles published in CRLSJ (1, 2) and JSSR further delve into the legal, ethical, and geopolitical dimensions of foreign surveillance tools infiltrating critical domestic sectors.

Their concerns have been validated by recent policy actions in the United States. In response to the growing threats, the U.S. Department of Commerce restricted drones from Foreign companies, citing national security risks as the primary motivation. These restrictions stem from fears that such drones could serve as instruments of espionage, with technology capable of collecting, storing, and transmitting data that may be accessed by unauthorized entities—including foreign governments in adversarial positions or cybercriminal networks. As Russell (2023) notes, this has triggered a broader

national reassessment of the dangers posed by foreign-made surveillance equipment, especially in the hands of states that seek strategic advantage through technological penetration.

Beyond security concerns, there is also significant debate surrounding the economic implications of such restrictions. Critical sectors such as agriculture, emergency response, and infrastructure monitoring have warned that limiting access to low-cost foreign drones could drive up operational costs and hinder growth. Farmers, for example, rely on drones to assess crop conditions, while emergency responders depend on real-time aerial surveillance during disaster recovery operations. As Siddiqui and Muniza (2025) point out, the affordability and availability of Foreign drone hardware have made them indispensable in various industries. Should these be banned or restricted, a significant gap could emerge—one that current alternatives may be unable to fill economically or technologically.

Together, Siddiqui and Muniza's scholarship offers a prescient analysis of these intersecting challenges, making a compelling case for urgent international regulation, the development of independent manufacturing capabilities, and the adoption of robust legal standards to safeguard privacy, national interests, and critical infrastructure in the digital era.

MARKET VACUUM AND ECONOMIC CONSEQUENCES

IMPACT ON AGRICULTURE

Agriculture Sector is one of the industries that is dependent on drones for various tasks like precision farming, crop monitoring, pesticide spraying and soil assessment. As if that's not enough, drones, in particular those produced by DJI, are fundamental to the U.S. agriculture industry by providing a way for farmers to efficiently do these things at a fraction of the cost. One of the giants in this domain, DJI – and their drones worth $35,000 and more – together with their technology, enable farmers to closely track their crop health and soil conditions and spray pesticides with the least amount of waste, thus boosting overall productivity as well as sustainability (U.S. Department of Commerce, 2024).

That changes, though, when we examine domestic rivals from U.S.-made brands. These alternatives are significantly more costly, starting with prices that may be as low as $250,000 for systems that provide similar capabilities." As this wide price differential suggests, the barrier that American farmers could be forced to clear if they lose access to affordable drones manufactured beyond our shores like DJI's is a substantial one and 'If there is no local supply of these cheap drones then our farmers will be forced to use expensive Indian versions, leading to huge spike in cost of operations (Hassan, & Maria, 2024).

This rise in operating cost could ripple across the farm sector. And if prices are high for this expensive (at least relatively), top-of-the-line drone tech, prices could mean expense for farming overall and possibly act as a COVID-19 tax on food products. Even worse, such financial strain might stifle agricultural productivity, because farmers might not be able to afford the technology to produce better crops or to work their farms efficiently. This in turn could affect the cost and availability of food to farmers and to consumers. So, the void in the market created by the foreign drones exiting the business could have far-reaching economic repercussions in agriculture, food prices and productivity (Hassan, Maria, 2025).

IMPACT ON EMERGENCY SERVICES AND INFRASTRUCTURE

Drones have become invaluable tools for emergency services — they are used for search and rescue missions and can be equipped with thermal imaging equipment and fly supplies into disaster zones. They offer disaster relief workers instantaneous bird's-eye views of ravaged sites, allowing them to survey damage, find victims and deploy resources more efficiently. Police also use drones to watch over crowds and keep the peace. The possibility of rapid, covert surveillance of extensive areas is an important aspect for the maintenance of public safety (Florida Legislature, 2023).

"Similarly, in areas such as energy, telecoms and infrastructure management, drones are invaluable in inspecting and monitoring critical infrastructure. Drones, for example, are used to inspect power lines, communication towers, bridges and pipelines, and are often able to do so more efficiently and safer than humans. Those industries use drones in the inspections to avoid spending a lot of time and money and to catch issues before they become a big problem (House Armed Services Committee, 2024).

The prohibition on foreign-made drones — especially drones from countries such as China and Russia — could deal a devastating blow to these initiatives. If first responders, police, and infrastructure response teams lose their ability to access low-cost, high-quality drones, their only remaining choice may be more expensive systems. This change could raise operating costs, diverting funds from essential activities.COVID-19 could affect CAP operations by causing staff shortages, limiting medical supplies, or increasing the cost of services. Even in the instance of an emergency scenario, the absence of low-cost drone technology could result in loss of response timeliness due to delays in the time taken to obtain and be trained up in the use of a new unit, or be hampered by the functions available on the more expensive units. In managing infrastructures, this may lead to reduced effort / time in performing maintenance and repairs, which in turn,

may delay the functionality and the safety of time-critical and/or safety-critical infrastructures. At worst, these delays could delay disaster response times, cost lives and slow recovery. So a prohibition on foreign drones could potentially create major public-safety and infrastructure nightmares, increasing costs, shrinking efficiency, and adding delay (UK Parliament Science and Technology Committee, 2023).

IMPACT ON RESEARCH AND DEVELOPMENT

The prohibition of foreign-made drones has been a heavy blow to the research community, academic and commercial. Agencies and researchers beyond just the military have drawn on drones produced overseas, especially by companies such as DJI, for many studies and pilot programs in multiple disciplines. These systems were well-known and low cost, making them available to a wide variety of investigators. Because they are relatively inexpensive and provide sophisticated functionality, they have become powerful tools in environmental monitoring, agriculture, wildlife conservation, and robotics (ENISA, 2024).

These foreign drones have served as a convenient, inexpensive way for many researchers to collect data, run experiments, and test out new technologies. Drones, in other words, are especially necessary for such tasks as aerial imaging and data collection from hard-to-reach places — or from very far, in the case of large-scale projects like monitoring crops or ecosystems. The researchers face new obstacles after the ban on the foreign drones. Loss of access to these commonly used platforms could disrupt ongoing projects and impede new research as scientists are forced to switch to more costly systems or retool their study designs without access to the drones they are dependent on (Texas State Government, 2023).

And even the development of the UAV technology itself could be pushed back by such an upset. Significant amount of research in academia and industry endeavors to enhance drone technology or creates new applications of UAVs. There has been extensive borrowing by foreign drones to develop much of this innovation, and without it, technological advancement may well grind to a halt. Plus, domestic equivalents may be slow to develop if foreign drones are out of reach. U.S.-based companies would also need to quickly produce their own drones on the cheap that are on par with those made overseas. Developing alternatives, on the other hand, would take years and require a great deal of effort and creativity and in the meantime cause a slowdown in technology development. Consequently, the barring of foreign drones does not influence only current research but may also lead to delays in the development of UAV technology and UAV-relevant innovations (U.S. Department of Homeland Security, 2023).

Commentators such as Hassan Rasheed Siddiqui and Maria Muniza Talat Ara have noted that there is a dearth of balanced regulations concerning new AI-powered surveillance systems and drones. Although the bans on foreign drones may appear as a quick fix to the question of national security, according to Siddiqui and Ara but has not taken into consideration of a much nuanced issue. The urgent growth of AI and its insertion in surveillance systems signals an obligatory regulation. In their 2025 reports, they are clear that without changes in existing laws related to drones and artificial intelligence surveillance tools, the U.S. could become ensnared in a cycle of reactionary policymaking that lags the technological landscape. They support a more well-rounded regulatory approach that accounts for security risks associated with foreign-made devices, in addition to establishing clear, enforceable laws that will safeguard industries and help to grow important sectors such as agriculture, healthcare and emergency management. So the difficult question being debated so fiercely these days is where to strike the balance: how much can we tilt the playing field to promote innovation while still keeping our national security and the economic survival of industries that depend on this foreign-made technology (Siddiqui, & Muniza, 2025).

STATEMENT OF THE PROBLEM

The greater use of foreign-made drones, in particular those made in China and Russia, has also provoked concerns over national security, cyber vulnerabilities and espionage risks. Although these drones offer low-cost solutions that allow the agriculture, emergency response and infrastructure sectors ways to work more efficiently, the federal government ban has resulted in economic and operational struggles. And there are no domestic inexpensive alternatives to these material problems, which could become a major impediment to vital industries. Moreover, the use of AI by foreign drones on the other side of the globe complicates matters, with potential of risks ranging from data stealing, surveillance manipulations, and system takeovers." There is a critical need for even-handed regulation to deal with security considerations and protect the further development and ability to function of critically important parts of the economy."

OBJECTIVES OF THE STUDY:

1. To analyze the market vacuum resulting from the ban on drones manufactured by Foreign companies.
2. To assess the effects of price competition and the availability of alternative drone technologies in the market.
3. To investigate the technical vulnerabilities associated with AI-enabled surveillance systems integrated into foreign-manufactured drones.
4. To propose strategies and solutions to ensure that essential industries, such as agriculture, emergency response, and infrastructure management, are not disrupted by restricted access to affordable drone technologies.

5. To recommend policy frameworks that address cyber security risks while fostering technological innovation within the U.S. drone and AI surveillance industries.

LITERATURE REVIEW

DEFINING STANDARDS FOR MANUFACTURERS: A PHASED APPROACH TO REGULATION

Large scale applications to which the technology applies: Regulation and Development of UAVs, particularly AI and Cyber Security aspects UAVs as a technology has taken great heights, and is now an intrinsic part of commercial as well as military operations. The emerging literature on UAV governance underscores the necessity of a holistic governance approach that encompasses the operational capability of UAV and that these devices comply with a resilient cyber context and AI ethical standards. Some experts have stressed the need to set transparent rules that manufacturers must follow as part of the standards, and reflected that foreign-built drones could pose a potential security risk (China Daily, 2024).

ESTABLISHING CLEAR AI AND CYBER SECURITY STANDARDS FOR UAVS

One of the key areas of interest in the literature is the establishment of AI and cyber security standards for formally designing, building, and employing UAVs. At present, the innovative application of UAV is drawing closer to different fields, which makes it necessary to establish figuring out mechanisms. And it needs to be mindful of the sensitive data manufactured by drones as well—surveillance material, geographic data, and personal information, among other things—and regulate them under a principle of "AI transparency." Good News, Bad News: Good, because it reminds us of the general problems of flying robots and the ways virtual paradigms are not neutral when put to “use.” It’s bad news because it’s suggesting the wrong kind of response: the position is “cleaning up the battleground”, where the real issue is drawing and redrawing the lines that make a battleground (Okpaleke, et al., 2023).

There are several proposals in the literature where the most important proposals is the idea of a cyber security audits. Experts further contend that it is important to conduct standard verification and strict cyberspace review of overseas UAV manufacturers to verify these aircrafts meet the set cyber security standards. Such tests would uncover weaknesses in the devices that could be used for espionage, to steal data or in other forms of cyber operations. Such audits should consist not only of a detailed hardware and software analysis but also the security of the communication link as well as the security of recovered data. Given the everchanging landscape of cyber security threats, many experts argue that such audits ought to be performed on a regular basis to ensure timely detection and preventing any new threats (Rao, et al., 2020).

A further consideration is the call for transparency reports on AI. The reports would force manufacturers to provide detailed information about the AI in their drones, especially about the AI used specifically for tracking, surveillance and data analysis. The transparency reports would help regulators determine whether the algorithms meet ethical standards, and function in accordance with national security goals and privacy practices. For instance, the AI used in facial recognition or a drone that is tracking can lead to concerns over invasions of privacy and abuse. It thus has been recommended that vendors issue regular updates regarding how these AI systems work and make decisions. By making AI algorithms transparent, regulators would able to oversee the risks of abuse and guard against such technology violating civil liberties (Rossiter, 2018).

In addition, the existing literatures highlight the necessity of firmware integrity verification. As UAVs are firmware dependent, it is important for regulators to include a mechanism to verify firmware is not updated with backdoors or other exploitable features which would compromise the security of the drone. Firmware updates sometimes improve functionality, fix bugs, and add new features. But they can be used against drone systems by bad actors as well. Industry speak suggests that full checking should be performed on any firmware update prior to deployment to make sure it is not harbouring any hidden security weaknesses. It includes the likes of digital signatures, encryption, secure delivery methods (to ensure updates can’t be tampered with), and much more(Savage, & Schmitt, 2017).

In summary, the available literature implies that the drafting of a phased regulation framework with these features—cyber security audits, AI transparency reports, and firmware integrity checks—would go a long way towards ensuring the security and ethics of UAVs. Such actions not only have the potential to protect national security interests, but also individual privacy and civil rights, and could allow for the responsible and safe use of UAV technology in multiple industries. Although there are some existing regulations on UAVs, the literature suggests they are in need of enhancement and updating to confront new technologies (namely AI and cyber security) that are driving the future uses of drones(Savage, & Schmitt, 2017).

GRADUAL TRANSITION TO SECURE UAV ALTERNATIVES

“Experts have proposed a phased transition to secure alternative domestic or partnering nation unmanned aerial vehicle sources in response to mounting concerns over use of foreign-manufactured drones, particularly in register of cyber and national security considerations.” The phased and innovative regulation of the factory production test serves to ensure the

careful balance between national security, industry requirements, and the development of technology, while avoiding undue disruption. The method consists of three phases: short-term, mid-term, and long-term actions. Each phase corresponds to risks addressed versus foreign drones and the creation and adoption of secure domestic alternatives (Wezman, et al., 2019).

SHORT-TERM: IDENTIFY AND BAN SPECIFIC DRONE MODELS WITH KNOWN SECURITY VULNERABILITIES

Near-term: Near-term plan for addressing known vulnerabilities of unmanned aircraft systems.– Work with industry quickly identify and remediate specific UAS models with known cyber security issues. This would address the most immediate risks presented by drones already in use or on the market. Regulators would perform comprehensive security evaluations to decide which foreign-made drones pose obvious threats — like those with unlocked security holes, back doors or flaws in their communications protocols. Their drones, when discovered, should be blacklisted from both commerce and from being flown within the United States. This rapid solution would reduce the threat of data-leaks, spying or hacking, from a compromised drone network. Targeting high-risk models, the short-term strategy enables the U.S. to act rapidly and decisively to protect sensitive sectors — government, law enforcement and critical infrastructure industries — without causing broader disruptions (Wong, et al., 2020).

MID-TERM: ENCOURAGE DOMESTIC MANUFACTURERS TO RAMP UP PRODUCTION THROUGH FINANCIAL INCENTIVES

Further in the mid-term phase, it is intended to close the interim period f the short-term prohibition of foreign drones to the long-term supply of secure national alternatives. In these early days, the government would be pushing domestic growth on the UAV industry through some sort of financial incentives to domestic U.S. companies. Those incentives might be grants, tax credits or low-interest loans that could help fund the research, development and production of drones that adhere to high cyber security and AI standards. By offering financial assistance the government would allow domestic manufacturers to produce more and enhance the capabilities of indigenous drone technologies. This phase would then serve to build market growth for those in-country produced drones, too, at prices, with functionality, and available to be competitive with what the drone industries, like agribusiness, emergency services, and infrastructure maintenance, can realize without massive cost increases. The ‘mid-term’ plan would see the U.S. to stop relying on foreign drones and boost innovation in the home grown UAV industry (Wu, 2020).

LONG-TERM: PHASE OUT HIGH-RISK FOREIGN DRONES ONCE SECURE DOMESTIC ALTERNATIVES ARE AVAILABLE

In the long run, the plan is for the high risk in foreign drones to be gradually eliminated as safe and competitive domestic offers become available. At this point, the US would have a mature homegrown domestic UAV industry that can be curtailed to multiple industries and is in line with the rigorous cyber security and AI regulations. A shift to safe, domestic replacements would be done in a manner that causes minimal impact on the industries supported by drones, so these industries are not left with no alternatives. This phase would also include continual assessments of the domestic systems compared to their foreign counterparts, with the goal of ensuring that national security, privacy, and operational performance are not harmed. The third and last phase in the transition would involve the controlled and gradual elimination of outside drones, making room for domestic UAVs in certain priority sectors in order to protect national security while promoting technology (Teal Group, 2020).

And by doing so incrementally, the United States would be able to deal with the pressing security concerns posed by foreign drones, encourage the expansion of a domestic UAV industry and be able to wean itself off reliance of high-risk foreign tech over time. This phased shift will allow the U.S. to preserve its technological and national security superiority, foster economic growth, and minimize disruption to industries reliant on drone technology (Zenko, 2017a).

AI-ENABLED SURVEILLANCE SYSTEMS: TECHNICAL VULNERABILITIES AND SECURITY RISKS

With the infusion of AI technology to surveillance and drone world, the functional capacity of unmanned aerial vehicle such as drone and surveillance device have been increased in terms of autonomy, precision and efficiency. But that advance in technology also comes with its own set of potential threats, especially those related to foreign-made drones and surveillance equipment. These principally originate from the weaknesses of the AI systems and to possible exploitation of software and firmware vulnerabilities on these devices (Zenko, 2013).

AI MODEL EXPLOITS: ADVERSARIAL MANIPULATION OF AI-DRIVEN TRACKING SYSTEMS

Adversarial manipulation of AI models is one of the most serious security threats in AI-based surveillance systems. AI-based platforms for tracking individuals or objects, by contrast, work on sophisticated algorithms that parse through large volumes of data to discern patterns and take decisions. But these systems can be gamed, and made to fall foul of their creators by malicious tactics that exploit the AI's decision making. Adversarial attacks occur when small, often small and imperceptible; perturbations are introduced into input data and serve to distort a model's classification or prediction. For example, manipulating visual data feed from drones (for example changing appearance of objects or conditions of scene-lighting etc.) can lead AI-based tracking systems to lose track and suffer failure in surveillance operations. These are exploits that could result in misdiagnosis of special operations, which might give attackers a way to hide, or intervene in critical business processes. The potential to trick AI-based tracking systems has especially troubling implications for border security, military engagements or surveillance work by law enforcement where precision in tracking is important (Tripp, 2020).

FIRMWARE BACKDOORS: UNAUTHORIZED ACCESS TO SURVEILLANCE DATA

Another major vulnerability of AI surveillance products is the fact there are always firmware backdoors. The firmware is a form of low-level software that organizes the hardware of a drone or surveillance system and also must be present for a system to function. Such a backdoor might be exploited by hackers or other hostile actors looking to subvert the drone or surveillance technology. This is particularly dangerous for national security issues, since monitoring by drones is more indiscriminate than that conducted through traditional means and drone surveillance tapes are usually kept and "seized" in secret. Supposing that our adversaries actually are exploiting these firmware backdoors, it would mean that they have access to not just sensitive intelligence, but also to monitoring being done on active surveillance targets that they may be able to disrupt, compromising security and privacy (Zenko, 2017b).

AI-ASSISTED DEVICE HIJACKING: HACKERS OVERRIDING AUTONOMOUS SURVEILLANCE SYSTEMS

The AI-powered surveillance systems can run by themselves and this reduces human involvement and makes it more efficient. But this independence comes with a nuisance: AI-based device hijacking. In this instance, adversaries could hack into an autonomous drone system using the AI algorithms used to pilot the drones, or perhaps the communication between drones and soldiers who run them. From there, if a hacker were able to break in, they could shut down the drone's surveillance capabilities, direct it to potentially unlawful areas or interfere with the system's threat identification processes. For example, a hijacker might alter the way in which the system distinguishes between potential threats, circumventing security countermeasures, or falsely triggering an alarm. In the worst case, AI supported surveillance hijacking can cause catastrophic 1events, especially in mission critical domains such as military operations, law enforcement and critical infrastructure security. Its' ability to hijack a surveillance drone or remotely take over systems has a great appeal for cybercriminals or state-sponsored hacking groups, especially the drone for they are autonomous. Generally, embedding AI capabilities in surveillance or drone devices offers numerous advantages in efficiency and autonomy, at the cost of security. The risks associated with AI model tampering, firmware backdoors, and AI-assisted device compromises indicate that agencies should consider the driver of flash storage devices a critical cyber security asset and use strict monitoring tools to safeguard AI-driven technologies. Addressing these weaknesses is necessary to transform AI-enabled surveillance systems from liability to effective and secure tools for national defense, law enforcement, and other mission-critical purposes (Zoli, 2017).

CASE STUDY

AHMEDABAD SURVEILLANCE INFRASTRUCTURE & FOREIGN ESPIONAGE RISKS

In this Review, we describe the recent technology and the market need, in which countries around the world are beginning to use artificial intelligence (AI)-based observation systems for monitoring safety, security, traffic, and other public areas. For example, until the recent, the Ahmedabad Municipal Corporation (AMC), India, relied on AI-based CCTVs (foreign origin) installed throughout the city to scrutinize mobility. There were such fancy features that came with these technologies – facial recognition, real time tracking and also the provision to analyze huge data sets for security and safety reasons but they also raised issues regarding data security and vulnerability to espionage (Posen, 2018).

DEPLOYMENT OF AI-POWERED SURVEILLANCE CAMERAS BY AMC

The AMC launched the massive surveillance drive to enhance security in the city, especially in crowded places such as markets, bus and railway stations, and gardens. The cameras used were installed with sophisticated AI analytics capabilities to undertake functions like surveillance of public areas to look for suspicious activities as well as match identifying facial recognition algorithms. The cameras, which are not domestic but from overseas, were selected as the best and most cost-effective that the AMC could select to have a camera to enhance the security in the city (Chávez, & Swed, 2020b).

CONCERNS OVER DATA SECURITY AND ESPIONAGE

The use of AI-driven surveillance systems also introduced significant risks arising from data security and foreign espionage, even though it had been implemented to enhance public safety. The fear was that the surveillance data harvested by these foreign cameras could be easily tapped by unauthorized individuals. The information being collected by these scanners was personal and included details on the movements and schedules of individuals, facial recognition data and other personal details. As the cameras were produced by foreign firms, fears were raised about whether these systems might have been used as a way of snooping on the nation (Chávez, & Swed, 2020a).

In interviews, experts Considered The Prospect That The foreign manufacturers of the cameras themselves could have built backdoors or similar access points into their software that would allow outsiders — like foreign governments or cybercriminals — into the very systems that were supposed to be providing security. If the systems were breached, it could expose sensitive data or even disrupt essential infrastructure. For instance, an enemy state may obtain the data as a means to track key players, discover law enforcement tactics or collect information behind public and private sectors. And the AI systems that underpin the cameras could potentially be used for more than just data theft: They could enable tampering. Bad actors also could manipulate the system's algorithms to generate false alarms, disable important surveillance capabilities or taint the data being collected, creating confusion, fear or security risks (Cummings, et al., 2017).

Supply chain risks were another cause for concern. The cameras were linked to central databases and control systems as part of a larger network that meant if one part of the system was disrupted, the entire network could be affected. And if investigators learned that the cameras had in fact been compromised, the city-wide security system would have been crippled, and the safety of the public areas of the city would have been compromised in matters ranging from criminal activities to terrorist threats (Okpaleke, 2021).

IMPACT ON CRITICAL INFRASTRUCTURE AND PUBLIC TRUST

The dangers of Ahmedabad's surveillance system extended beyond data theft. Disruption of crucial city services such as traffic supervision, public safety surveillance or crime alerting may result if a hacker were to gain entry to the surveillance network. For instance, if video surveillance were found to have intentionally missed illegal or critical activity, this might affect law enforcement's ability to learn about specific events in a way that influenced security and public order. As ordinary citizens became more conscious of potential menaces posed by overseas surveillance systems, they became increasingly concerned that their personal data not only may be employed for purposes other than public safety such as by foreign governments or rogue individuals. This lack of trust could potentially work against the aims of the surveillance program, as the public might think that their privacy was being invaded in the name of security and rise up in protests or demand more oversight and regulation (Nagl, et al., 2016).

Such is the situation at Ahmedabad Municipal Corporation but it's not quite so established elsewhere, and the pitfalls over the weeks have been many. While these systems can offer everything from security to efficiency and productivity to metropolitan centers, they are also vulnerable to hacking and to spying — especially where hardware is sourced from overseas (Castelino, 2018).

To mitigate these risks, experts advise the imposition of strict regulation on the buying, selling, and use of internet surveillance tools, the enforcement of cyber security best practices so that systems are protected from compromise, and the establishment and enforcement of data protection requirements for the data collected by these systems. Transparency about the source of surveillance technologies and the development of local alternatives could also help mitigate security risks. With the risk of spying and sensitive, even critical date being stolen, cities like Ahmedabad must weigh the advantages of AI-enhanced surveillance systems against the potential detriments from foreign-made devices, and take wherever possible measures to secure both national security and the trust of the public. This case highlights the need to ensure a holistic integration of AI solutions into public infrastructure that upholds both innovation and security (Carafano, 2020).

DISCUSSION

SECURITY THREATS POSED BY FOREIGN AI-POWERED DRONES

National security concerns are prevalent regarding the emergent and widespread use of artificially intelligent drones — particularly those made by foreign manufacturers including China's DJI and Russia ZALA Aero. These "smart" drones are being used in an ever growing number of situations (in both civilian and military realms), for their relatively low cost, efficiency and tech-heavy capabilities. As their number increases, however, so does the possibility of drones being turned against us and used for nefarious purposes (in espionage, secret monitoring and data theft, for example) (Carter, 2021).

DATA EXFILTRATION

Among the most alarming threats presented by foreign AI drones is data exfiltration. As modern-day drones with sophisticated AI carry out their operations, they can capture and transfer vast swaths of information, from sensitive details like surveillance footage, GPS coordinates, and environmental details like the temperature and air quality of a neighborhood to personal information. The problem is when those drones are produced by businesses in nations with competing national interests (Journal of National Security Studies, 2024). In this case, the data collected by these drones might be surreptitiously returned to enemy governments or intelligence services. It was also the kind of information that can be used to collect intelligence on national security resources, military operations, infrastructure, or private citizens, making it ripe for foreign enemies, he said. "The fact that an American citizen can have private data about their property without consent beamed to a server in China or elsewhere is absolutely mindboggling," Malkin said. "The potential for loss of privacy and national security is terrifying."

FIRMWARE BACKDOORS

A major vulnerability there are firmware doors. The firmware is the software that the drone's hardware depends on in order to work. Drones manufactured outside the US can have unadvertised vulnerabilities baked into the firmware or injected during the manufacturing process. These backdoors could be exploited by cybercriminals, hackers, or even by state actors to remotely access the drones, override security mechanisms, and take control of it. If these drones are employed in sensitive fields — for law enforcement, infrastructure management or defense, for example — hackers could use these vulnerabilities to steal sensitive data, meddle with drone operations or even disrupt core services. For instance, a foreign government might use backdoor access to shut off surveillance systems when they are most needed, to manipulate drone video feeds or to logarithmically alter data collection in order to deceive analysts (Harvard Law Review, 2023).

AI MODEL EXPLOITS

The use of AI in drones presents a new type of security threats—exploiting the AI models. AI drones make use of sophisticated algorithms for such activities as image recognition, tracking, navigation and decision-making. These AI models are susceptible to what are called adversarial attacks, where attackers subtly modify input data—like images—one tiny bit at a time, in a way that causes the drone's AI to make a bad decision. An adversary, for example, may change images or environmental data that is input to an AI system, so that the drone would then rub their own eyes and miss something important. In surveillance applications, such tampering may result in wrong tracking (e.g., letting people or objects untracked) or in incorrect activity indication (i.e., reporting normal activities as suspicious). These AI-model-based attacks whilst compromising the drone functionality, can limit its performance drastically in civilian and military applications, under both authorized as well as adversary's commands(IEEE Transactions on Cyber security, 2023).

SUPPLY CHAIN VULNERABILITIES

Then there is the less-glamorous supply chain threat associated with drones and their parts, which is often forgotten. Drones, including some made by foreign companies, tend to be made with parts from suppliers around the world. Most of these suppliers are indisputably benign, but the fact that they use parts from adversary countries endangers them. There's also malware that enemies embed in hardware or some kind of cyber insecurity in the guts of a drone while it's being built. Even if it is not detected during the assembly or deployment of these drones that they are tampered, the malware implanted in components can be activated later when the drones start running, enabling the user to launch a cyberattack or leakage. For instance, a compromised microchip or communication modem can be used for granting unauthorized access to the drone systems that could result in commanding the drone to hijack the drone or exploiting sensitive information. A supply chain at risk these supply chain vulnerabilities could complicate the job of security experts trying to identify the source of a cyber attack, especially if they are exposed at deep levels in the drone ecosystem (MIT Technology Review, 2024).

BROADER NATIONAL SECURITY IMPLICATIONS

In unison, these threats are a greater threat to national security. Drones — especially those combined with artificial intelligence and surveillance gear — are increasingly used in delicate operations, from border surveillance to protecting main infrastructure. Putting these foreign-made drones in a position to serve as instruments of espionage, surveillance disruption, or sabotage, jeopardizes the security of these operations. In a worst-case scenario, foreign drones might be used to impair a nation's ability to defend itself through surveillance or its intel networks, by which adversarial states could compromise key parts of a country's overall security posture. Indeed, the massive rollout of AI-driven drones raises the question of how well we can secure these systems: How when the AI models running them are opaque or resistant to audit (RAND Corporation, 2024).

With all of these securities threats afoot, it is long past time for robust regulatory regime intended to address the risks posed by foreign drones. And especially those with AI. This should include a condition that drones are subject to strong cyber security standards that information gathered by affected drones is all reported transparently, and that manufacturers

and their supply chains are routinely audited. There's also the imperative to: Put in place processes to decode and mitigate firmware backdoors and supply chain weaknesses that can be exploited in ways that compromise national security (Boussios, 2017).

Economic and Operational Impact of Bans

The decision to ban foreign drones like those from companies like DJI has wreaked havoc on numerous industries that rely heavily on these drones. The city police forces and public safety units that once depended on DJI drones for everything from breaking up big groups of people, to spying on them, to conducting search and rescue operations and responding to emergencies get the raspberries. These drones were said to be very cheaply made and effective at this kind of work, allowing such agencies to obtain cutting edge technology at cut-rate prices. Now forced to rely on domestic drones, these groups will be burdened with increased operating costs, a reduction in capability and response time in emergencies (Boyle, et al., 2018).

And they too are scrambling to find affordable solutions, with farmers and infrastructure directors increasingly using drones for jobs such as precision mapping, monitoring crops and inspecting infrastructure. In agriculture, drones are critical farm equipment for farmers who have to monitor sprawling fields of crops, gauge soil health and water-field data

with irrigation equipment. Infrastructure managers as well call on drones to inspect vital assets, such as power lines, pipelines and bridges. But the barring of foreign drones has left room for affordable, effective solutions. Domestic substitutes exist, but they are many times more costly and price these sectors further out of most local consumers' reach. Accordingly, industry is being burdened by higher costs and is becoming less efficient, which may result in an operational slowdown, or worse, a slowdown in productivity throughout key sectors of the economy (Congressional Research Service, 2024).

Such challenges are only compounded by a lack of alternatives at home. The domestic market for UAVs is expanding, but still falling short of the size and cost competitiveness of foreign drones. The absence of competition leads to expensive goods and drones that fail to meet the performance criteria (in terms of range, distance measurement, etc.) required by key industries. This results in a linear time-to-market of new drone technologies (swapping investment for longer delivery times), and acts as a speed brake for investments themselves (U.S. Department of Defense, 2024).

SHOULD ALL FOREIGN DRONES BE BANNED, OR ONLY MODELS WITH SECURITY RISKS?

Why some in India have a drone itch?Although the antagonism towards foreign drones is largely due to genuine concern on for national security and fears of AI-empowered surveillance and espionage, a complete blanket ban on all foreign drones might not be the most prudent option. Alternatively, a more tailored rule could be adopted that would apply only to specific makes and models of drones that were known to have particular security vulnerabilities. This would enable the U.S. to maintain the advantage of employing foreign drones in which the security holes cannot be easily exploited and remove the threat that would come with compromised model.

A more selective policy would enable U.S. businesses to still operate foreign drones that pass the most rigorous security protocols or have been subject to extensive scrutiny for cyber security vulnerabilities. By targeting individual models with known risks, such as backdoors, malware, or vulnerabilities in AI algorithms, the U.S. could help ensure that drones are not being exploited by enemy actors for spying, or cyber-attacks and would mitigate the need for unnecessary interference in an industry heavily reliant on drone technology. For instance drones that monitor crops in agriculture, will not pose a significant a threat to your national security, they can carry on being used safely, businesses and farmers and infrastructure managers will be able to continue their operations without having to pay over the odds for more expensive domestic options.) It would also reduce impact on industries such as law enforcement and emergency response, which rely heavily on inexpensive drone solutions. (These industries would still have the drones they need to perform the essential tasks, but they wouldn't be burdened with learning whole new product lineups or inflated costs.

This is in difference to India, which has gone for a blanket ban on external drones because there are no local options. India opted for the move due to unavailability of indigenised UAVs with similar monetary burden and capabilities being offered by foreign drones. The U.S., however, has the capacity and resources to caution certain models based on security assessments and not the kind of blanket response that places national security risks on companies of vital national interest. By narrowing the policy scope, the U.S. can strike a balance between national security and industry's economic and operational requirements for drones. So in the end a ban may not be the most effective solution but rather focused regulation on high-risk types of models. This would enable the U.S. to defend against espionage and cyber security threats while still allowing essential industries and in an age when threats are global and the industry is transnational with American drone firms buying foreign made drones.

CONCLUSION

The (bipartisan) American ban of Foreign drones, based on rational national security concerns that address threats of espionage, data leakage and, eventually, foreign drones as weapons in future cyber warfare, is what the world should hope for. But it has also come with tremendous economic and operational pain. It used to be cheaper drones produced elsewhere were not easily attainable at a good price for businesses that lent on them heavily, like agriculture, emergency response and infrastructure service. And those industries rely on cheap, practical drone hardware to monitor crops, respond to disasters and inspect infrastructure are struggling to make the expensive leap to domestic alternatives.

And there are the security implications surrounding AI-equipped foreign drones. The threat of espionage, intelligence theft, and cyber warfare looms large, particularly given the deployment of progressively more power AI-enabled surveillance-suitable drones. These weapons are dangerous, which is just the point. However, these same weapons also open the door to large vulnerabilities that adversaries may exploit. The rapid pace of developing and deploying these capabilities underscores the need for a regulatory posture that balances threats to national security with the operational needs of industry.

To meet these challenges, the federal government must also move proactively to galvanize the domestic drone industry and cyber security. One, bringing drone manufacturing home is more critical than we realize: We need to be able to rely on our own domestic capabilities to produce drones, rather than depending on offshore suppliers, to ensure that the

American economy has a secure, cost-efficient substitute for Chinese or any other drones. Second, AI-enhanced drones require strong cyber security measures to minimize vulnerabilities in hardware and software of UAVs. This would ensure these machines are secure enough to help prevent unauthorized access and protecting personal data. And the United States will need to adopt a graduated policy approach to accommodate a transition from foreign-made drones to secure American alternatives. This would allow industries to carry on as normal while domestic manufacturer's ramp up production of high quality drones that meet security and operational requirements. Last but not least, it is necessary to establish public-private partnerships to promote innovation in the domestic UAV industries. By promoting government-enterprise collaboration, we can spur the development of advanced drone technologies to meet our security needs while boosting U.S. competitiveness.

By adopting a comprehensive, tiered approach to these problems, the U.S. can protect national security interests and the continued health of necessary industries. A safe, well-regulated, and innovative domestic UAV sector will serve to keep the country from exposure to security threats and fend-off industry disruption, enabling the thriving and advancement of critical sectors that depend on low-cost drone technologies.

RECOMMENDATION

Public policy implications Given the ban on foreign drones, and to avoid hampering national security, the U.S. should implement a selective regulation that focuses on those drones of certain types who have known security risks, instead of a wide and general ban on all foreign drones. That would let the industries that have latched onto drones — agriculture, emergency response, infrastructure inspection — keep using cheap, foreign-made models that work far better than domestic alternatives without posing serious security risks. At the same time, the U.S. should make investments to bolster domestic manufacturing of drones, so that safe and affordable alternatives can be ready for critical industries. Rigorous cyber security protocols for AI based drones are also important, including security audits and transparency reports by manufacturers, to reduce the risks from data exfiltration, firmware backdoors and AI tampering. Furthermore, the development of public-private partnerships can facile ate in ramping up innovation in the domestic unmanned aerial vehicle (UAV) industry, which can go a long way in addressing technology security requirement with access to cost-effective alternatives. Through a systematic phased approach, taking in capacity for national security alongside operational requirements of leading sectors, the U.S. can still allow the UAV sector to grow while it continues to safeguard its critical infrastructure from new threats.

REFERENCE

[1] Association for Unmanned Vehicle Systems International (AUVSI) (2023). Market Trends in AI-Powered Drones.
[2] Boussios, E. (2017). Drones in war: The controversies surrounding the United States' expanded use of drones. Contemporary Voices: St Andrews Journal of International Relations, 8(4), 48–52.
[3] Boyle, M. J., Horowitz, M. C., Kreps, S. E., & Fuhrmann, M. (2018). Debating drone proliferation. International Security, 42(3), 178–181.
[4] Carafano, J. J. (2020). Technology and great power competition: 5 top challenges for the next decade. https://www.heritage.org/technology/commentary/technology-and-great-power-competition-5-top-challenges-the-next-decade

[5] Carter, K. L. (2021). Coming soon to a theater (of war) near you: Drones of all shapes and sizes. In Drones and global order (pp. 191–208). Routledge.
[6] Castelino, T. (2018). An action plan on US drone policy: Recommendations for the Trump Administration. Arms Control Today, 48(6), 37–39.
[7] Chávez, K., & Swed, O. (2020a). Off the shelf: The violent nonstate actor drone threat. Air & Space Power Journal, 29(9), 237.
[8] Chávez, K., & Swed, O. (2020b). The proliferation of drones to violent non-state actors. Defense Studies, 13(5), 1–9.
[9] China Daily (2024). DJI's Response to U.S. Drone Ban: Economic and Policy Implications.
[10] Congressional Research Service (2024). Comparative Analysis of U.S. and Global Drone Security Policies.
[11] Cummings, A. R., McKee, A., Kulkarni, K., & Markandey, N. (2017). The rise of UAVs. Photogrammetric Engineering & Remote Sensing, 83(4), 317–325.
[12] Cyber security & Infrastructure Security Agency (CISA) (2023). Threat Assessment of AI-Integrated Foreign Surveillance Drones.
[13] European Union Agency for Cyber security (ENISA) (2024). AI and Cyber security Threats in Surveillance Drones.
[14] Federal Aviation Administration (FAA) (2024). Cyber security Guidelines for AI-Enabled Surveillance Drones.
[15] Florida Legislature (2023). Ban on Foreign-Made Drones in Government Operations.
[16] Harvard Law Review (2023). Legal Challenges of Banning Foreign AI-Powered Surveillance Drones.
[17] Hassan Rasheed Siddiqui, and Ms. Maria Muniza. (2024). "The Drone's Gaze: Religious Perspective on Privacy and Human Dignity in the Age of Surveillance." Al-Qamar.
[18] Hassan Rasheed Siddiqui, Maria Muniza. (2025). Analyzing the Shortfalls of the U.S. Countering CCP Drones Act in Light of China's National Intelligence Law. Social Sciences & Humanity Research Review.
[19] House Armed Services Committee (2024). National Defense Authorization Act and Foreign Drone Restrictions.
[20] IEEE Transactions on Cyber security (2023). Firmware Backdoors in AI-Integrated UAVs.
[21] Journal of International Security (2023). The Role of AI in Modern Espionage and Cyber Warfare.
[22] Journal of National Security Studies (2024). Supply Chain Risks in Foreign-Manufactured AI Surveillance Systems.
[23] MIT Technology Review (2024). Adversarial AI Attacks on Autonomous Drone Systems.
[24] Nagl, J., cited in Bregen, P. (2016). United States of Jihad: Investigating America's homegrown terrorists. Proceedings, 142, 72–73.
[25] National Institute of Standards and Technology (NIST) (2024). AI Security and Data Protection in UAV Technology.
[26] Okpaleke, F. N. (2021). The implications of unchecked armed drone proliferation for global security. African Strategic Review, 4(1).
[27] Okpaleke, F. N., Nwosu, B. U., Okoli, C. R., & Olumba, E. E. (2023). The case for drones in counter-insurgency operations in West African Sahel. African Security Review, 32, 351–367.
[28] Posen, B. R. (2018, March 28). The rise of illiberal hegemony: Trump's surprising grand strategy. Foreign Affairs. https://www.foreignaffairs.com/articles/2018-02-13/rise-illiberal-hegemony
[29] RAND Corporation (2024). Assessing the Risks of AI in Military-Grade UAVs.
[30] Rao, B., Harrison, A. J., & Mulloth, B. (2020). Defense technological innovation: Issues and challenges in an era of converging technologies. Edward Elgar Publishing.
[31] Rogers, A., & Hill, J. (2014). Unmanned: Drone warfare and global security. Between the Lines.
[32] Rogers, J. (2021). Future threats: Military UAS, terrorist drones, and the dangers of the second drone age. In Drone warfare: Trends and emerging issues (pp. 481–505). The Joint Air Power Competence Centre.
[33] Rossiter, A. (2018). Drone usage by militant groups: Exploring variation in adoption. Defense & Security Analysis, 34(2), 113–126.
[34] Russell, S. (2023). AI weapons: Russia's war in Ukraine shows why the world must enact a ban. Nature, 614(7949), 620–623.
[35] Savage, C., & Schmitt, E. (2017). Trump poised to drop some limits on drone strikes and commando raids. International New York Times, NA–NA.
[36] 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.
[37] Siddiqui, H. R., & Muniza, M. (2025). Regulatory Gaps in Drone Surveillance: Addressing Privacy, Security, and Manufacturing Standards. Annals of Human and Social Sciences.
[38] Teal Group. (2020). Teal Group predicts worldwide military production of drones of over $99 billion in the next decade. https://www.tealgroup.com/index.php/pages/press-releases/64-teal-group-predicts-worldwide-military-uav-production-of-almost-99-billion-over-the-next-decade-in-its-2019-2020-uav-market-profile-and-forecast
[39] Texas State Government (2023). Legislation on Restricting Foreign Drone Use in Public Infrastructure Monitoring.

[40] Tripp, B. (2020). Deterrence and drones: Are militaries becoming addicted, and what is the prognosis? In A. Filippidou (Ed.), Deterrence: Concepts and approaches for current and emerging threats. Springer.
[41] U.S. Department of Commerce (2024). National Security Concerns Over Foreign Drone Technology.
[42] U.S. Department of Defense (2024). AI Warfare and Autonomous UAV Threats.
[43] U.S. Department of Homeland Security (DHS) (2023). Espionage Risks in AI-Powered UAV Systems.
[44] UK Parliament Science and Technology Committee (2023). Legislative Approaches to AI-Powered UAV Security.
[45] Wezman, P. D., Fluerant, A., Kuimova, A., Tian, N., & Wezeman, S. T. (2019, March). Trends in international arms transfers, 2018. SIPRI. https://www.sipri.org/sites/default/files/2019-03/fs_1903_at_2018.pdf
[46] Wong, Y. H., Yurchak, J. M., Button, R. W., Frank, A., Laird, B., Osoba, O. A., & Bae, S. J. (2020). Deterrence in the age of thinking machines. RAND Corporation.
[47] Wu, X. (2020). Technology, power, and uncontrolled great power strategic competition between China and the United States. China International Strategy Review, 2(1), 99–119.
[48] Zenko, M. (2013). Reforming US drone strike policies (No. 65, pp. 56–58). Council on Foreign Relations.
[49] Zenko, M. (2017a). The (not-so) peaceful transition of power: Trump's drone strikes outpace Obama. Council on Foreign Relations.
[50] Zenko, M. (2017b, February 2). Trump could take Obama's drone war further into the shadows. Foreign Policy. Retrieved May 29, 2023, from https://foreignpolicy.com/2017/02/02/the-buck-doesnt-stop-with-trump-on-counterterrorism/
[51] Zoli, C. (2017). The changing role of law in security governance: Post-9/11 gray zones and strategic impacts. Syracuse Law Review, 67(613).
[52] Hassan Rasheed Siddiqui, Maria Muniza. (2025). ANALYZING THE SHORTFALLS OF THE U.S. COUNTERING CCP DRONES ACTH.R.2864IN LIGHT OF CHINA'S NATIONAL INTELLIGENCE LAW AND THE ZHENHUA DATA 2020. Social Sciences & Humanity Research Review, 3(1), 567–584. Retrieved from https://jssr.online/index.php/4/article/view/94
[53] 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. https://doi.org/10.35484/ahss.2025(6-I)36
[54] 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. https://doi.org/10.35484/pssr.2025(9-I)41
[55] Hassan Rasheed Siddiqui, and Ms. Maria Muniza. 2024. "The Drone's Gaze, Religious Perspective on Privacy and Human Dignity in the Age of Surveillance Mentioning Security Threats & Regulatory Gaps". Al-Qamar, December, 1-12. https://doi.org/10.53762/alqamar.07.04.e0
[56] https://crlsj.com/index.php/journal/article/view/448 DOI: https://doi.org/10.52783/crlsj.448
[57] 16th-https://crlsj.com/index.php/journal/article/view/449
[58] Siddiqui, H. R. ., & Leghari, A. . (2007). FAITH, FREEDOM, AND THE FUTURE: RECLAIMING INCLUSIVE DEMOCRATIC VALUES IN SOUTH ASIA. The Journal of Contemporary Issues in Business and Government, 13(1), 107–116. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2868 2.
[59] Siddiqui, H. R. ., & Leghari, A. . (2008). LIBERALISM IN SOUTH ASIA, A CASE STUDY OF CIVIC LEADERSHIP AND INTERFAITH HARMONY. The Journal of Contemporary Issues in Business and Government, 14(2), 90–97. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2870 3.
[60] Siddiqui, H. R. ., & Muniza, M. . (2009). SOWING ILLUSIONS, REAPING DISARRAY: MEDIA INFLUENCE, URBAN MIGRATION, AND THE DISMANTLING OF SOCIETAL NORMS IN SOUTH ASIA. The Journal of Contemporary Issues in Business and Government, 15(2), 126–139. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2871 4.
[61] Siddiqui, H. R. . (2011). IN THE COURT OF KNOWLEDGE, JUDGING THE JUDGES OF LEARNING. The Journal of Contemporary Issues in Business and Government, 17(1), 83 91. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2872 5.
[62] Siddiqui, H. R. . (2013). THE PERSONAL LENS IN ACADEMIC EVALUATION: A CRITIQUE OF EDUCATOR BIAS. The Journal of Contemporary Issues in Business and Government, 19(1), 93–101. Retrieved from https://cibgp.com/au/index.php/1323 6903/article/view/2873 6.
[63] Siddiqui, H. R. (2016). ESTABLISHING AIR AMBULANCE SERVICES IN PAKISTAN: A REGULATORY AND INVESTMENT FRAMEWORK FOR EMERGENCY MEDICAL AVIATION. Journal of Advanced Research in Medical and Health Science (ISSN 2208-2425), 2(5), 17 30. https://doi.org/10.61841/z1tjva12 7.
[64] Siddiqui, H. R. . (2019). WHO JUDGES THE JUDGES? ADDRESSING INTEGRITY AND SECURITY GAPS IN THE SINDH JUDICIAL RECRUITMENT SYSTEM. International Journal of Advance Research in Education & Literature (ISSN 2208-2441), 5(8), 5-15. https://doi.org/10.61841/txq2w096 8. Siddiqui, H. R. (2022). PUBLIC FUNDS, PRIVATE GAINS: INVESTIGATING CORRUPTION IN NADRA'S MEGA CENTER LEASE DEALS. Journal of Advance Research in Social Science and Humanities (ISSN 2208-2387), 8(12), 17-28. https://doi.org/10.61841/2s3kmv78 9.

[65] Siddiqui, H. R. (2023). STRUCTURAL INJUSTICES IN THE RECOGNITION OF FOREIGN MEDICAL DEGREES BY THE PAKISTAN MEDICAL COUNCIL: A CALL FOR POLICY REFORM. Journal of Advanced Research in Medical and Health Science (ISSN 2208-2425), 9(1), 58 67. https://doi.org/10.61841/vmqgts53
[66] H. R. . (2010). DELAYED JUSTICE AND DUAL STANDARDS: THE ENFORCEMENT OF ARBITRAL AWARDS IN PAKISTAN. The Journal of Contemporary Issues in Business and Government, 16(2), 88–99. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2877
[67] Siddiqui, H. R. ., & Leghari, A. . (2007). FAITH, FREEDOM, AND THE FUTURE: RECLAIMING INCLUSIVE DEMOCRATIC VALUES IN SOUTH ASIA. The Journal of Contemporary Issues in Business and Government, 13(1), 107–116. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2868
[68] Siddiqui, H. R. ., & Leghari, A. . (2008). LIBERALISM IN SOUTH ASIA, A CASE STUDY OF CIVIC LEADERSHIP AND INTERFAITH HARMONY. The Journal of Contemporary Issues in Business and Government, 14(2), 90–97. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2870
[69] Siddiqui, H. R. ., & Muniza, M. . (2009). SOWING ILLUSIONS, REAPING DISARRAY: MEDIA INFLUENCE, URBAN MIGRATION, AND THE DISMANTLING OF SOCIETAL NORMS IN SOUTH ASIA. The Journal of Contemporary Issues in Business and Government, 15(2), 126–139. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2871
[70] Siddiqui, H. R. . (2011). IN THE COURT OF KNOWLEDGE, JUDGING THE JUDGES OF LEARNING. The Journal of Contemporary Issues in Business and Government, 17(1), 83– 91. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2872
[71] Siddiqui, H. R. . (2013). THE PERSONAL LENS IN ACADEMIC EVALUATION: A CRITIQUE OF EDUCATOR BIAS. The Journal of Contemporary Issues in Business and Government, 19(1), 93–101. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2873
[72] Siddiqui, H. R. (2016). ESTABLISHING AIR AMBULANCE SERVICES IN PAKISTAN: A REGULATORY AND INVESTMENT FRAMEWORK FOR EMERGENCY MEDICAL AVIATION. Journal of Advanced Research in Medical and Health Science (ISSN 2208-2425), 2(5), 17-30. https://doi.org/10.61841/z1tjva12
[73] Siddiqui, H. R. . (2019). WHO JUDGES THE JUDGES? ADDRESSING INTEGRITY AND SECURITY GAPS IN THE SINDH JUDICIAL RECRUITMENT SYSTEM. International Journal of Advance Research in Education & Literature (ISSN 2208-2441), 5(8), 5-15.https://doi.org/10.61841/txq2w096
[74] Siddiqui, H. R. (2022). PUBLIC FUNDS, PRIVATE GAINS: INVESTIGATING CORRUPTION IN NADRA'S MEGA CENTER LEASE DEALS. Journal of Advance Research in Social Science and Humanities (ISSN 2208-2387), 8(12), 17-28. https://doi.org/10.61841/2s3kmv78
[75] Siddiqui, H. R. (2023). STRUCTURAL INJUSTICES IN THE RECOGNITION OF FOREIGN MEDICAL DEGREES BY THE PAKISTAN MEDICAL COUNCIL: A CALL FOR POLICY REFORM. Journal of Advanced Research in Medical and Health Science (ISSN 2208-2425), 9(1), 58-67. https://doi.org/10.61841/vmqgts53
[76] https://crlsj.com/index.php/journal/article/view/448 DOI: https://doi.org/10.52783/crlsj.448
[77] https://crlsj.com/index.php/journal/article/view/449
[78] Publication URL: https://cibgp.com/au/index.php/1323-6903/article/view/2881 Hussain, N. . (2025) EVALUATING THE NATIONAL SECURITY AND ECONOMIC CONSEQUENCES OF U.S. RESTRICTIONS ON FOREIGN DRONES. The Journal of Contemporary Issues in Business and Government, 31(2), 1–13. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2881
[79] Hassan Rasheed Siddiqui, Maria Muniza. (2025). ANALYZING THE SHORTFALLS OF THE U.S. COUNTERING CCP DRONES ACTH.R.2864IN LIGHT OF CHINA'S NATIONAL INTELLIGENCE LAW AND THE ZHENHUA DATA 2020. Social Sciences & Humanity Research Review, 3(1), 567–584. Retrieved from https://jssr.online/index.php/4/article/view/94
[80] 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.https://doi.org/10.35484/ahss.2025(6-I)36
[81] 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. https://doi.org/10.35484/pssr.2025(9-I)41

[82] Hassan Rasheed Siddiqui, and Ms. Maria Muniza. 2024. “The Drone’s Gaze, Religious Perspective on Privacy and Human Dignity in the Age of Surveillance Mentioning Security Threats & Regulatory Gaps”. Al-Qamar, December, 1-12. https://doi.org/10.53762/alqamar.07.04.e01.

[83] MS Shahzadi Sarwat Noreen, Talat Ara. (2025). THE ROLE OF INTERNATIONAL LAW IN AI DRONE REGULATIONS. Social Sciences & Humanity Research Review, 3(1), 626–645. Retrieved from https://jssr.online/index.php/4/article/view/98