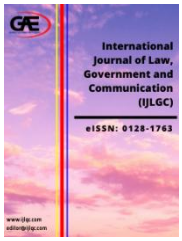
International Journal of Law, Government and Communication
IJLGC
EISSN : 0128-1763
Volume: 11 Issue: 44 (June 2026) PP. 88-106



INTERNATIONAL JOURNAL OF LAW, GOVERNMENT AND COMMUNICATION (IJLGC)
www.gaexcellence.com/ijlgc

GLOBAL ACADEMIC EXCELLENCE

UAVs SECURITY THREATS IN MALAYSIAN AIRSPACE: ISSUES AND CHALLENGES

Khairul Nizam Taib[1]*, Salma Yusof[2], Mazura Md Saman[3], Noor Azmi Mohd Zainol[4], Azrul Azlan Abd Rahman[5], Mohd Haniff Sofian[6], Zulkarnain Haron[7]. Ariffin Ismail[8],

[1]Centre for Military and International Humanitarian Law, National University of Malaysia
khairulnizamtaib3596@gmail.com https://orcid.org/0009-0008-9319-855X
[2] Faculty of Defence Studies and Management, National Defence University of Malaysia
salma@upnm.edu.my https://orcid.org/0000-0001-9973-9873
[3] Centre for Military and International Humanitarian Law, National University of Malaysia
mazura.mdsaman@upnm.edu.my https://orcid.org/0009-0001-0679-3692
[4] Faculty of Defence Studies and Management, National Defence University of Malaysia
noorazmi@upnm.edu.my https://orcid.org/0000-0002-9512-7332
[5] Faculty of Defence Studies and Management, National Defence University of Malaysia
azrulazlan@upnm.edu.my https://orcid.org/0000-0002-0053-3064
[6] Faculty of Defence Studies and Management, National Defence University of Malaysia
haniff@upnm.edu.my https://orcid.org/0009-0009-3012-9482
[7] Centre for Military and International Humanitarian Law, National University of Malaysia
zukarnain.haron@upnm.edu.my https://orcid.org/0000-0001-6824-179X
[8] Faculty of Defence Studies and Management, National Defence University of Malaysia
ariffinismail@upnm.edu.my https://orcid.org/0000-0001-6591-2367
*Corresponding Author

Article Info:

Article history:
Received date: 30.12.2026
Revised date: 15.01.2026
Accepted date: 31.05.2026
Published date: 11.06.2026

Abstract:

The UAV's development in Malaysia has progressed due to its prominent features, especially in security and defence industries, agriculture, logistics, surveillance and disaster management. The versatility, deployability and cost efficiency influenced modern technology innovation in fulfilling the needs of the society. However, the benefits of UAVs now bestowed on the society have left a negative impact on the society, especially on the Malaysian airspace. The security threats posed by UAVs include disruptions to the civil and military airspace, violations of personal rights and illegal activities

International Journal of Law, Government and Communication
IJLGC
EISSN : 0128-1763
Volume: 11 Issue: 44 (June 2026) PP. 88-106

To cite this document:

Taib, K. N., Yusof, S., Saman, M. M., Zainol, N. A. M., Abd Rahman, A. A., Sofian, M. H., Haron, Z., & Ismail, A. (2026). Developing A Citizen-Centric Performance Evaluation for State Legislative Representatives in Malaysia. *International Journal of Law, Government and Communication, 11*(44), 88-106.

DOI: 10.35631/IJLGC.1144006

within borders. Despite its prominent benefits to society, this article emphasises the utmost significant need to address the risks in light of security and defence matters. In lieu, the lacuna left in our law regarding the use of UAVs will be highlighted as well. Furthermore, balancing innovation and security measures through a robust framework, investment in counter-UAV technology and public awareness, and collaboration for border security with neighbouring countries must be established. Through a qualitative methodology, this article will propose guidelines for government stakeholders, policymakers and enforcement agencies to mitigate UAV-related risks and, at the same time, maximise UAVs' potential benefits bestowed on society.

Keyword:

Border Security, Security Threats, Surveillance UAVs, Weaponisation,

Introduction

The technology of UAVs for the purpose of strategic and defence objectives had been introduced long ago, in the 2000s, inter alia to secure national security through enhancing surveillance capability, covering technology and supporting the economy and environment. In the defence sector alone, UAVs were used for intelligence, surveillance, and reconnaissance to secure maritime and land border security, especially within the Straits of Malacca, from illegal activities, piracy, smuggling, and others (Marhalim Abas, 2020). In conjunction with global threats within the Southeast Asia region, the prominent features of UAVs expanded not only for surveillance and border security purposes but also mapping and data collection as well (Marhalim Abas, 2021). Aligning with the geographical factors and emerging threats within the region, which demand a robust yet enhanced capability of UAVs in monitoring West and East Malaysia, the MQ-9 Reaper and Wing Long II were purchased to complete the task (Linda Kay, 2019). The need to balance and leverage technology demands the purchase and use of UAVs for civilian purposes: agricultural monitoring, recreational mapping and environmental conservation. The government also saw the need to enhance capability for civilian security, such as for search and rescue, urban fire and disaster management (Wong YB, et al., 2023). Whilst the prominent features of UAVs attract the government's intent to secure the security and defence sector and, at the same time, give advantages bestowed to the society, the emerging threats aligned with the technological development of UAVs are inevitable. A series of incidents relating to the use of UAVs shows the significant danger, not only to the strategic and defence, but personal rights as well. Increasing use of UAVs, or drones, for recreational purposes by civilians while the COVID-19 pandemic was near airports posed a hazard to aviation safety. Similarly, a drone was detected being used to smuggle contraband across

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 44 (June 2026) PP. 88-106

Malaysia's border along the Malaysia-Thailand border (Marion Garans & Melania Andakova, 2022). These are examples of where the government has to seek resolutions in enhancing the use of UAVs' prominent features. Taking into consideration this article's objectives, it is to examine and analyse the threats posed by UAVs to the Malaysian airspace and at the same time to recommend the best solutions to mitigate such threats in a layman context.

Problem Statement

Despite the UAV's technology expansion, which brought significant benefits to the military and civilian sector, the growing prevalence of this technology also includes critical risk and imminent danger to national security, especially to airspace security. Hundreds of incidents involving the UAV's misuse, including illegal smuggling, unauthorised flights near airports and technical areas, and potential espionage, highlight the vulnerabilities posed by this technology. Although Malaysia has taken proactive steps in investing in UAV's capabilities, the enforcement mechanisms and existing policies to control UAV's misusage and threats remain status quo. It started with the insufficient legal framework, ineffective integration of anti-drone technologies, and weaknesses in government agencies' coordination that had left weak links and vulnerabilities to airspace security. Hence, this gap demands the urgent need for further research to examine and analyse UAV's potential related threats in order to recommend strategies which can strengthen the national airspace security and sovereignty.

Significant of Research

The prominent nature of UAVs and their benefits to the national interest, especially in defence security and civilian applications, include the potential threats that demand a specific effective mechanism to address the issues. Based on specific cases of misuse of UAVs as mentioned above, the research urges the government stakeholder by highlighting critical lacunae in policies, enforcement and technological standards. The findings will recommend all government stakeholders draft an additional formulation of comprehensive strategies which can mitigate UAV-related risks and at the same time enhance and empower Malaysia's national security and regional stability.

Objectives of the Research

The research focuses its objectives on three (3) prongs. Firstly, to identify and examine the benefits bestowed on Malaysia, especially in national security and civilian applications. Secondly, to analyse the danger or threats that emerge from UAV misusage. Finally, this research intends to propose practical recommendations and strategies to balance the UAVs' technologies with effective security measures.

Scope and Limitation of the Study

This study examines the role of UAVs in Malaysia, particularly their contributions to national security, border surveillance and civilian applications, including agriculture, disaster response and environmental monitoring. It also considers the potential risks of UAV misuse, such as smuggling, aviation hazards and unauthorized activities, and assesses possible policy and regulatory measures that could be considered to mitigate such threats. This study is limited in a number of ways. It does not delve into technical or engineering issues of UAV design and instead focuses on policy, security and governance perspectives. It is limited in its scope to

Malaysia and the regional security environment and does not make extensive comparisons with the global situation. Furthermore, the study uses open sources, which may not include classified or sensitive defence data. These scope and limitations are designed to keep the research relevant, practical and consistent with Malaysia's current security and governance priorities.

Research Methods

This research adopts a qualitative approach based on document analysis of academic literature, government reports, defence white papers and credible news sources. The method focuses on content analysis to identify key themes relating to the use, risks and governance of UAVs in Malaysia. Regional experiences provide comparative insights and wider implications. This approach is chosen to provide an in-depth understanding of UAV-related threats and policies without requiring access to classified defence data.

The Security Threats Posed by UAV's in Malaysian Airspace

The threats posed by UAVs during the COVID-19 pandemic were evidentiary proof that the prominent features of UAVs do offer an imminent threat instead of giving their benefit to society alone (Mohit Aurora et al., 2021). The threats by UAVs include:

Espionage and Surveillance Threats.

It is the practice of gathering information and the act of transmitting secret information without authorisation. Espionage may include the practice of gathering information against national security, military confidentiality or corporate secrecy (SentinelOne, 2024). Advanced technology of UAVs permits espionage practice to be conducted with a variety of methods, such as stealth activities and high-tech surveillance, rather than in the old days, which included high-risk overt and covert activities (Jose Carlos Palmer, 2024). The capability to conduct unauthorised data collection with advanced imaging and surveillance technology poses high risks and threats to the national interest, especially to government installations (Wardatus Hayat Adnan & Mohd Fadly Khamis, 2022). UAVs, or drones, have the capability to fly over government buildings, military installations and restricted zones to capture high-resolution images, record activities or intercept wireless communication, thus jeopardising government and military operations. Data collection by UAVs in lieu may be converted through either Signal Intelligence (SIGINT) or Imagery Intelligence (IMAGINT) to Human Intelligence (HUMINT), which may expose the vulnerability of either government operation or military operations (Deveraux A, 2024).

In 2015, Japan saw the emerging UAV technology as a threat and imminent danger. A drone with radioactive sand was sent to the roof of the Japanese Prime Minister's office in Tokyo. Equipped with a camera with particular markings, it indicates that the drone was sent as a signal of protest. Even though no casualties were involved, the incident signalled a significant potential for using UAVs as espionage tools (Yamaguchi M, 2016). The incident proves that a simple yet advanced tool in technology with its prominent features may mock the most highly sensitive place monitoring system. The capability in a different context saw that a camera and radioactive sand may be substituted with a weapon system, a high-resolution camera and surveillance technology. The incident was considered a wake-up call to the Government of Japan, demanding the installation of drone detection systems and frameworks to prevent UAV flights near government buildings. Apart from that, the incident had triggered global awareness

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 44 (June 2026) PP. 88-106

about the potential use of UAVs as a tool of espionage, whereby the legal framework upon airspace intrusion was reviewed.

The private sector is also exposed to the UAV's threats. It may be used as a tool of espionage and surveillance, as it can be equipped with advanced technology to enable it to operate from afar. The remote-control capability with specific attributes raised serious concern among corporate giants about intellectual property theft by capturing blueprints, prototypes or sensitive documents by using a high-definition camera or wireless information hacking (Conventus Law, 2022). Competitors, either domestic or international, may use UAVs to monitor Malaysian companies such as Petronas to sabotage oil and gas refineries, palm oil industries and others through their infiltrating production processes, logistic chains and supply systems and even trade routes (Moonyati Yatid, 2022). Some UAVs are equipped with a WiFi system which enables them to operate cyberattack espionage through intercepting WiFi signals and hacking devices distributing malware and computer viruses. In 2020, a corporate network was hacked by a drone equipped with 2 hacking tools, including Raspberry Pi and WiFi Pineapple. The drone used their payloads to perform a man-in-the-middle (MITM) attack through intercepting WiFi communication to secure unauthorised access to the company's system (Ottila W & Rameez Asif, 2024). After the incident, all corporate giants had taken imminent measures to restrict free WiFi with specific guidance to mitigate the threat posed by UAVs (K. Ley Best et al., 2020).

Weaponization of UAV's

UAVs are known as tools that can be modified due to their accessibility, stealth and versatility to carry imminent threat devices such as explosives, firearms, or biological agents (Jean Paul Yaacoub et al., 2020). These are perfect features searched by terrorists, criminals or lone attackers. Weaponisation of UAVs includes:

> ***Explosives.*** The accessibility of UAVs, or drones, due to the low cost and public offering enables any person with malicious intention to buy and modify them. In addition, with remote control capability to operate from afar, hard-to-detect and utmost efficient modes of transportation turn the UAVs into perfect tools to drop explosives at any time, in any place and at the operators' will (Calcara, A & Zaccognini, I, 2022). The 2019 drone attack on Saudi Aramco facilities saw the damages caused by modified drones equipped with explosives to the infrastructure, high casualties and psychological impact.
>
> ***Firearm, Biological and Chemical Agent***. Drones were used widely, especially in the large agricultural industry, for surveillance and distribution or dispersing pesticides and fertiliser. However, the same tools were used by malicious persons to disperse biological or chemical agents to create terror in overpopulated areas. In a very recent incident, "Family Boat" a lead vessel of the Gaza-bound humanitarian Global Sumud Flotilla (GSF) in Tunisia was attacked by drones installed and equipped by a type of incendiary weapon intended to intimidate and undermine the peaceful mission aimed at breaking Israel's blockade of Gaza (Bernama, 2025). Even though there are no such cases involving biochemical agent yet, Kallenborn and Ackermann strongly opined that biological agents or chemical agents such as anthrax can be dispersed to harm humans and the environment.

International Journal of Law, Government and Communication
IJLGC
EISSN : 0128-1763
Volume: 11 Issue: 44 (June 2026) PP. 88-106

Combined Capabilities. UAV's advanced technology normally can create collateral damage on a huge scale through the combination of explosives, biochemical agents and firearms. This means that UAVs or drones can be treated as weapons of mass destruction if there is no preventive measure to control the outburst. The US Air Force had shown their 'predators' capabilities in operating covert missions and, at the same time, offensive missions in Syria and Iraq while combatting ISIS. Applying the same principles, ISIS was observed using modified drones to drop grenades and small explosives targeting military and civilians in Mosul and Raqqa. (Rassler D, 2018). Kunertova in 2023, on the other hand, saw the same repercussion upon military and civilian objects when both Russia and Ukraine used drones for reconnaissance purposes. Both belligerents equipped their drone with a payload combination including a firearm and explosives.

Smuggling and Illicit Activities.

Jean-Paul Yaacoub and Hassan Nova Olla Salwan in 2020 opined that UAVs, or drones, unique capabilities, which include mobility, stealth and accessibility, posed a significant threat through smuggling and illicit activities. Smuggling and illicit activities may include:

Drug Smuggling. In the old days smugglers faced the high risk of apprehension due to the high security measures prepared between the borders of two neighbouring countries. Nowadays, these obstacles can be easily overcome by using drones. Drones can be the most effective means of transportation to smuggle drugs in a better, smarter and cost-effective way, as the human efforts have been taken over. Fences, enforcement agency personnel, high walls, checkpoints or even large rivers can be bypassed easily (Koslowski R & Schulke M, 2018). With a slight minimum modification, a drone can make multiple small, undetected load deliveries. Even if the drone is captured, a minimal cost incurred makes it the best and most popular method of drug smuggling nowadays (Blazakis J, 2006). Javier Sutil Toledano in 2024 proves his argument by sharing the use of drones to deliver small quantities of drugs across the US-Mexico border.

Contraband Delivery to Prisons. Delivery of contraband to prison by using UAVs has the same modus operandi as drug smuggling across borders (Joe Russo et al., 2024). The contraband includes cell phones, drugs, cigarettes, and even weapons. However, the delivery operation is usually conducted at night to prevent being apprehended by prison guards. Comparing the delivery in the old days, the use of UAVs was smarter and more efficient. Nevertheless, there were numbers of cases where drones were being intercepted. In the UK, for example, attempts to deliver drugs, phones and other illegal contraband were intercepted, demanding a drastic change for anti-drone development measures to mitigate the problem (Ministry of Justice @ Rt Hon Damian Hinds MP, 2023).

Human Trafficking and Border Violations. Drones in this context were used to aid smugglers in human trafficking through surveillance of border patrol movements or operations. It is also used to identify and examine the best routes and terrain for illegal crossing. Terrains and routes then will be analysed by smugglers in line with the border patrol movement, pattern and strategies. In short, drones were used to scout the border security loopholes and weaknesses to transport or traffic humans individually or in groups (Navid Ahmadin et al., 2022).

International Journal of Law, Government and Communication
IJLGC
EISSN : 0128-1763
Volume: 11 Issue: 44 (June 2026) PP. 88-106

Smuggling High Value Goods. The old days saw smuggling high-value goods to be a rare occasion due to the high risk of being apprehended. High-value goods include gold, cash, cigarettes, and bootlegging of cars and alcohol. Mostly, the old days of smuggling were conducted by human effort. The prominent features of UAVs superseded those obstructions because they are cost-effective and on-shelf characters. For most serious high goods smuggling operations, the smugglers do not hesitate to invest in drones to be modified with surveillance systems and data collection features. If ever being apprehended, the smuggler did not hesitate to start over in a very short time. (Laine JP, 2021).

Arm Trafficking. UAVs, or drones, were very popular amongst the arm traffickers using the same modus operandi and variations of methods. The high capability in transporting firearms, explosives or weapons into conflict areas or supplying their proxy across borders is at their utmost will. The same methods were intercepted by Israeli authorities in the West Bank in 2018 (Robin Kellemann, Tobias Biehle, Lilian Fischer, 2020).

Risk of Airspace Interference

The safety of the airports and restricted airspaces can be prejudiced whenever any person conducts drones or UAVs with malicious or even bona fide intentions. Any incident, whether intentional or accidental, may disrupt commercial or civil aviation and may lead to potential catastrophic collisions.

Potential for Mid-air Collisions. Hu Liu, Mohd Hasrizam and Huot Low in 2021 argued that mid-air collisions may be caused by the possibility of UAVs or drones colliding with commercial aircraft during either take-off or landing phases. The disparity of material between UAVs and an aircraft may cause significant damage to the aircraft. Drones or UAVs made from carbon fibre could damage the aircraft fuselage or wings. In the event whereby the collision strikes a jet engine, an engine failure could lead to catastrophic internal damage. Damage to vital engine systems such as sensors or landing gear could occur as well (Marina Milos & Cokorilo et al., 2024).

Pilot Distraction and Loss Control. A sudden appearance and interference of UAVs or drones may cause a pilot distraction, which leads to delay and technical errors. Drone or UAV appearance: According to the Civil Aviation Agency Malaysia (CAAM), the threat posed by drone or UAV appearance causes a cockpit distraction mostly in phases of taxiing, taking off, landing and any operations below 10,000 feet. Causing a diversion of pilot intention. (AAM Safety Information 13/2024, 2024). There is a research study that shows pilot distractions by drones such as visual distractions are safety flight risks in 11% of situations (Alyssa Ryan, Cole Fitzpatrick, Eleni Christofa, et al., 2020).

Flight Delay and Airport Closure. In 2018, Gatwick Airport was forced to halt operations entirely, causing hundreds of flight schedules to be cancelled and disrupted. The incident happened because a drone was sighted within the airport area. For safety reasons, airports are places which demand a maximum degree of safety and special attention. Flights may be delayed, rerouted or even cancelled to ensure the safety of the passenger and to reduce financial losses due to drone sightings (Pyrgies John, 2019).

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 44 (June 2026) PP. 88-106

Restricted Airspace Violations. Drones, or UAVs, operating near restricted airspace often violate and pose a significant threat to national security, especially the restricted airspace which includes dual-use airports for commercial and military purposes (Anghuwo JS, Immanuel D & Nangolo SS, 2024). The purpose of having a dual-use airport is to enhance both military and commercial capabilities and operations, especially for military exercises, and to secure sensitive military equipment. Commercial purposes, on the other hand, are to increase passenger capacity and cargo and to reduce pressure on other civil airports (Shue H & Whipman D, 2002). Hence, any disruption caused by drones/UAVs can pose a significant threat to the dual-use airport as to the operation of both commercial and military capabilities.

Military Airspace Violations. Yaacoub, Noura and Salma in 2020 believed that UAVs, or drones, that have the capabilities to run overt and covert operations potentially may disrupt military operations and compromise training exercises. A military operation is a coordinated activitydesigned to resolve a situation in favour of a state or non-state actor. Most of the coordinated activities include planning of movements and manoeuvres, intelligence, firing sustainment, command and control and others. The planning is coordinated either during conflict, peacetime or for training purposes. According to Sei Daliyeva and Ilipbayeva (2024), prominent features of drones, even if not weaponised, can disrupt military operations by interfering with routine operations and pose direct threats to personnel and military assets. During a live-firing exercise or crucial operation in a military compound or area of operation, a drone may lead to postponement of the exercise or operation to give priority to safety, wasted resources that had been allocated and delays. Watkin, Simon and Burry in 2019 echo the same effect when it comes to military exercises. Military exercises such as air-to-ground offensive training, Command Post Exercise (CPX) and Search and Rescue (SAR) were conducted to coordinate a familiarisation process into a real incident. Even though it does not involve real-world geography or players, they still resemble realistic situations. Any interference by UAVs or drones with specific attributes may jeopardise the exercise significantly through data gathering, observation, images, troop movements, military strategies and weapon technologies. Such information shall give vital advantages to the adversaries (Hu, Dingkun & Minner, Jenni, 2023).

Surveillance or Reconnaissance Interference. Surveillance and reconnaissance missions or operations share the same modus operandi, which includes visual observation or electronic observation. What differentiates the two operations is the time and specificity of the activity. Whilst surveillance needs a prolonged length of time for the purpose of gathering information, reconnaissance is conducted rapidly and is targeted to retrieve specific information (Chizek, Judy, 2003). The operation of surveillance or reconnaissance depends on or is subject to UAV or drone interference. Drones, or UAVs, often block the collection of information or intelligence or open disruption to force the military conducting surveillance or reconnaissance to lose focus or shift focus to neutralising the unauthorised drone. Signal waves and frequencies may also cause electromagnetic interference and communication system issues as well (Abich IV, Julian & Reinermann et al., 2016).

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 44 (June 2026) PP. 88-106

Public Privacy Concerns

In 2023, research by Gargi Sarkar and Sandeep K. Shukla reveals that almost all UAVs, or drones, are capable of being equipped with advanced technologies. With these attributes, UAVs, or drones, are capable of conducting illegal surveillance. With imaging and recording technologies, they can operate discreetly, accessing hard-to-reach areas, which raised serious public concern and privacy rights. A night surveillance with a high-quality presentation with other multitasking operations can be conducted in a safe, faraway location without fear of being apprehended. Des Butler in 2019 furthers that illegal surveillance raised additional concerns by arguing that drones hover outside windows, in backyards or near balconies. On the other hand, UAVs can be used to gather business information, recording employees' activities and spying on industrial processes.

Challenges in Addressing UAV's Security Threats in Malaysia

The fact that our authorities were left behind with the development of UAV technologies and means and methods to mitigate the threats posed by them cannot be negated. As far as it is now, CAAM as the authorised government agency to overcome security threats posed by UAVs through enforcement, policing strong regulations and increasing stronger counter-drone technology alone cannot be accepted. There is a need to create stronger collaboration with other agencies to mitigate such serious concerns. However, before further steps are taken, it is utmost rational for us to identify and be clear of the most dominant challenges in addressing UAV security threats in Malaysia. The challenges identified are as follows:

Regulatory Gaps in Malaysia UAV's Legal Frameworks.

It is sufficient to say that the draughting of UAV regulations is not commensurate with the prominent features and its development in technology due to its ongoing nature. The lack of comprehensive regulations compared to the grey area that left a lacuna is the main challenge (Stocker et al., 2017). This is what Civil Aviation Regulation 2016 (MCAR 2016) had: limited scope and enforcement capabilities. MCAR 2016 was draughted focusing on airspace safety alone and none addressing privacy invasion, cyber threats or drone weaponisation (Syed Zomael Hussain & Muhammad Azly Haziq, 2019). The lacuna involves the enforcement of regulatory provisions and the registration of UAVs for smaller drones, which gives an advantage to illegal operators to evade accountability (The Malaysian Lawyer, 2019). The award of punishments provided in the same MCAR 2016 are also not commensurate to the deterrence effect compared to the greater danger and cost to be borne in the future (Zaf Seraj, 2024).

Unclear Boundaries to No-Fly Zone.

Henry Yeo in 2020 echoes the lacuna in MCAR 2016 from a different angle. Henry argued that the provision addressing boundaries for no-fly zones was unclear. An unclear legal framework will leave behind inter-chain risks in the future should the question about boundaries be addressed. This creates ambiguity which prolongs amongst jurists regarding restricted areas such as airports and military zones being given priority. Areas such as cultural landmarks, government buildings, technical areas, and urban populations, however, remain unclear. Keith Davis in 2022 further commented that although MCAR 2016 offers preventive measures to mitigate the danger or threats due to UAV usage, such as geo-fencing technology installation,

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 44 (June 2026) PP. 88-106

it only covers the area of the no-fly zone and no other technical area, which leaves no option for the enforcement to rely on manual monitoring, which is not commensurate with malicious drones operated with undetected high-technology features (Yunus et al., 2020).

Enforcement Issues

Challenges in mitigating UAV's threats are also borne due to a limited law enforcement presence compared to the vast terrain area (Hua Siong W, 2022). In a restricted area, priority is given to airports whereby the airports are equipped with PSRS and SSRS radar systems which can detect larger aircraft. In military bases or airspace, CCTV was used to monitor unwanted activities (Marhalim Abas, 2021). However, UAV detection often relies on and is conducted by human effort through observation rather than advanced surveillance. This will create a delay in detecting a rogue drone (Asif Ali Laghari et al., 2023). De Benedetto in 2018 explained that the enforcement issue in related UAV usage is caused by the inefficiency and reluctance of government agencies to invest in UAV technology and conduct training programmes, especially skills regarding counter-UAV-related threats. (Rao, Bharat & Gopi et al., 2016).

Technological Limitations

Several root causes have been spotted under technological limitation. The first area to be questioned is the difficulty in identifying rogue UAVs involved in illegal activities. The identification of rogue UAVs is so hard to be conducted because of the registration process under MCAR 2016 itself (Edwin Lee, 2019). The MCAR 2016 provision focuses only on larger aircraft to register for a permit, while smaller UAVs may operate unregistered. Secondly, challenges of distinguishing between a bona fide operator and a malicious operator due to overlapping airspace usage. The enforcement personnel find it very difficult since the usage of drones varies between rogue UAVs and those who operate for commercial purposes such as agriculture, recreation, industry and others (Tan Kheng Soon et al., 2024). In addition, the current detection systems, such as RF scanners and visual spotting, are still struggling to level with those advanced UAV systems. Even though the government may always turn to counter-UAV technologies such as drone-jamming devices, catching nets, and GPS spoofing equipment, these technologies are expensive and not widely deployed in Malaysia (Aouladhadj D, et al., 2023). Zifar, Raed & Aal Betar conquered with the additional argument that UAV technology is not only expensive, but counter-UAVs are usually installed and used within critical areas such as airports and military bases. For rural and border regions, the problems and challenges still remain.

Proposed Strategy to Mitigate UAV's Security Threats in Malaysia

The UAV's technologies rapidly grow at a fast velocity, as do the dangers and threats posed by it. In order to address these issues, robust strategies are paramount by combining stricter laws, advanced technologies and assertive regional cooperation. These strategies must be draughted and implemented promptly to ensure UAVs continuously give benefits bestowed to the society while national interest is kept protected.

Enhance UAV's Regulations.

There is a prompt need for the Malaysian government to enhance UAV regulations. The current legal provisions had many lacunas that must be reviewed and amended. Legal provisions

provided by MCAR in regulating registration of licences and permits, for example, only focus on UAVs or drones weighing more than twenty (20) kilograms and give leniency to those weighing less (The Malaysian Lawyer. 2019). A new set of mandatory drone registration schemes must be introduced. It must include stricter regulations requiring all UAV operators to register their drones with the Civil Aviation Authority of Malaysia (CAAM) and obtain operating licences, particularly for commercial or high-capability drones. Drones with a recreational purpose must not be excluded. Any business proprietor must also register under the Kementerian Dalam Negeri for the sale of UAVs or drones, even if it is for recreational purposes, so that tracking operations of rogue UAVs or drones can be executed. The definition of No-Fly Zones under the new regulation must also be included (Edwin Lee, 2019). The definition must include clearer and more enforceable no-fly zones around airports, military bases, government buildings, and critical infrastructure. This would include mandatory installation of geo-fencing measures on each piece of technical infrastructure to prevent UAVs from entering restricted airspace (Edwin Lee, 2019). For deterrence purposes, the new proposed legal provision should also establish heavier penalties for unauthorised drone usage (Zaf Seraj, 2024).

Development of Counter-UAV's Technologies

In terms of counter-UAV technologies, the government has no other option other than opting to enhance in line with its evolving prominent features. Counter-UAV technologies can be improved by deploying radar systems, radio frequency detectors, and optical sensors to monitor drone activity in sensitive areas (Tinshu Sasi, Arash Habibi Lashka, et al., 2024). The corroborations with information fed by the mandatory registration scheme system proposed earlier would allow authorities to track and identify rogue UAVs in real time.

Anti-Drones Solutions

The aim of an anti-drone system is to detect, identify and track, and neutralise rogue UAVs or drones. This system can be tailored to the needs of the security team, which include a mobile detection unit, drone mitigation technology, and a software platform to tie everything together (NQ Defence Blog, 2024). Among anti-drone solutions that can be adopted are the following:

> ***Jamming Technologies***. The aim of is to detect, intercept, and neutralize rogue drones in restricted areas. It has the capability to disrupt radio frequency (RF) signals or GPS communications between a drone and its operator, effectively neutralizing the UAV (Pietro, 2019). RF jammer's function is to block the drone's control signals, causing it to lose communication and either return to its base or hover until its battery depletes while GPS jammers have the capability to disrupt the UAV's navigation by interfering with its ability to lock onto satellite signals, making it unable to maintain its route. Both jammers are effective against a wide range of consumer and commercial drones. It can be deployed in both portable (handheld) and fixed systems for flexible use.
>
> ***GPS Spoofing***. This is the only anti-drone solution capable of redirecting new instructions to a rogue UAV or drone to a new location or locations. It is most effective to be applied for autonomous drones that rely heavily on GPS for navigation. However, the use of GPS spoofing includes requiring a complex implementation whereby precise calibration is utmost needed to ensure the spoofing signal overrides the drone's existing GPS data (Joeaneke, Princess & Val, et al., 2024).

International Journal of Law, Government and Communication
IJLGC
EISSN : 0128-1763
Volume: 11 Issue: 44 (June 2026) PP. 88-106

Drone Capture Systems. It is a specialised drone equipped with nets that can intercept rogue UAVs by ensnaring them mid-air or from the ground. There are two (2) types of drone capture systems, net equipped UAVs and ground based systems (NQ Defence Blog, 2024) . Net-equipped UAVs capture rogue drones mid-air by launching a net at the target, capturing it and bringing it to the ground safely or carrying it away. Ground-based systems on the other hand are launchers that fire projectiles or deploy nets to capture drones at close range. Both systems employ net guns or automated net cannons that are positioned around restricted areas. Both capture methods are non-lethal, reducing the risk of collateral damage in populated areas, and can hold the drone for analysis or evidence collection. However, both systems can only be effective within a defined radius and are unsuitable for high-altitude or long-distance interceptions (Nooralishahi, P., Ibarra-Castanedo, C. et al., 2021).

Other Advance Systems. Zachary and Marcel in 2024 saw Laser and Kinetic Interceptor as the finest other advanced systems a government can opt for. Laser systems offer precision and scalability with minimal risk of affecting surrounding infrastructure, even though they are expensive to deploy and maintain, with high power requirements. A kinetic interceptor, on the other hand, is a specialised weapon focusing on neutralising rogue UAVs or drones by using anti-drone missiles or high-speed projectiles which can destroy rogue UAVs.

Establishment of Counter UAV's Task Force. Mohsan, S.A.H., Othman et al. (2023) highlighted the importance of Malaysia having a specialised UAV Task Force to prevent drone threats to sensitive areas such as airports, military bases and border areas. Lykou, Georgia and Moustakas (2020) also proposed that the task force should be responsible not only for surveillance but also for detection and neutralisation of rogue drones, enforcement of compliance with UAV regulations, licensing and incident response. The task force must have specialised training in drone operations, anti-drone technologies and UAV forensics to be effective. Training should be done through joint exercises with the military and border security and collaborations with aviation and cyber security agencies such as CAAM and Cyber Security Malaysia. Continued funding from federal and state governments is essential, along with incentives for private industries to assist in covering the costs of urban monitoring systems. Ultimately, the response to UAV threats must be a collective effort, requiring active participation from both government and the public (Gomez, 2020). Strengthening Malaysia's airspace security and counter-drone efforts should not be limited to national initiatives alone but also extended through international cooperation and knowledge sharing. Malaysia is confronted with similar challenges to its neighbors, Singapore, Thailand, and Indonesia, with regard to UAVs, especially in border control and maritime security. This proximity calls for cooperation to tackle issues such as smuggling, piracy, espionage, or unauthorized drone surveillance (Muhmad Kamarulzaman, A. M., Wan Mohd Jaafar, et al. 2023). Cross-border cooperation may take the form of sharing information on illicit UAV activities and joint operations to monitor sensitive areas such as the Strait of Malacca, a hot spot for smuggling and piracy. Such efforts may build upon existing frameworks such as the Indonesia-Malaysia-Thailand Cooperation to encompass coordinated UAV surveillance and response strategies (Arifin, Bustanul & Damanik, Nur. (2020). The adoption of globally recognized standards and protocols for UAV regulation, counter-drone technologies, and threat mitigation would also help to reduce the risks of airspace interference and enable smoother coordination across borders. Malaysia's leadership in

regional UAV governance could serve as a model for Southeast Asia in managing drone-related security threats while strengthening regional cooperation.

Findings

The research finds that there are several major gaps in handling UAV issues. Firstly, the current legal framework under the Malaysia Civil Aviation Regulations (MCAR 2019) left a great lacuna by giving leniency to smaller or recreational purpose UAVs. Thus, a stronger and stricter registration system that covers all types of drones regardless of their size and purposes must be promptly draughted. A clearer no-fly zone and a heavier punishment for deterrence purposes are needed as well (The Malaysian Lawyer, 2019). Secondly, threats and dangers posed by UAV technology must also be addressed by technology as well. Assets such as radar, radio frequency detectors, and optical sensors, which enable the authorities to track suspicious or rogue UAVs' movement, must also be secured. Rogue UAVs can be easily detected, especially if they are linked to a national database registration system (Sasi, Lashka, et al., 2024). Such tools or assets would improve the security in technical areas such as airports, military bases, and other critical areas. It must be noted that there is no single solution that can override all UAV threats. Thus, a mix of preventive measures or tools, for example, jamming signal apparatus, GPS spoofing, drone catching systems and advanced tools like lasers or interceptors, will create a stronger and more reliable defence (Pietro, 2019). Mohsan and Othman in 2023 opined, in addition, that a dedicated Counter-UAV Task Force is also needed. A combination of skills and expertise from the military, aviation experts and cybersecurity agencies ensures a quick response to incidents with stronger, reliable and efficient enforcement. Last but not least, an assertive cooperation between Malaysia and fellow ASEAN countries is important to tackle cross-border crime such as smuggling contraband and illegal surveillance. Sharing intelligence is so significant with common standard practices among the ASEAN countries. Malaysia at the same time could take a strong stand with assertive policy in setting a stronger, reliable and effective regional security (Kamarulzaman, Jaafar, et al., 2023).

Conclusion

UAVs are like a coin for Malaysia’s future, having both exciting opportunities and serious risks. It supports industries such as agriculture, logistics, and surveillance, boosting economic growth and modernisation. On the other hands, their misuse for smuggling, illegal spying or violating restricted airspace poses growing threats to national security and public safety. Weak enforcement, regulatory gaps and limited counter-drone technology have compounded the risks. Malaysia must strike the right balance between innovation and security in addressing these challenges. Stronger regulations, better enforcement and wider public awareness are the key starting points. Meanwhile, investments in counter-UAV technologies such as detection systems, jamming tools and capture mechanisms are essential for protecting sensitive areas and cannot be negated. These tools, once integrated into current air traffic management systems, will raise the effectiveness of such systems in both rural and urban areas. Just as importantly, a dedicated UAV Task Force with specialized training and advanced equipment needs to be established to respond promptly to threats. Regional cooperation with neighbours such as Singapore, Indonesia and Thailand is also key for intelligence sharing and to build a stronger collective defence. Malaysia has no other option but to secure a future with the use of UAVs. It depends on finding the right balance between encouraging innovation and protecting its airspace. By combining smart policies, advanced technology, and international cooperation, Malaysia can lead the way in building a safe and responsible drone ecosystem.

Acknowledgements: The authors would like to express their sincere gratitude to National Defence University of Malaysia, University Malaysia of Sabah and University Science Islam of Malaysia for providing the necessary resources and support throughout the course of this research. Special appreciation is extended to colleagues and peers who contributed valuable insights and constructive feedback, which greatly enhanced the quality of this paper.

Funding Statement: This research received financial support from the Collaborative Research Grant (CRG/2020/SSK/5) and GPJP Short Grant reference J0419 – UPNM/GPJP2025/SSI/8. The funding body had no role in the design of the study, data collection, analysis, interpretation of results, or the decision to publish this manuscript.

Conflict of Interest Statement: The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the International Journal of Law, Government and Communication (IJLGC).

Ethics Statement: This study did not involve any human participants, animals, or sensitive data requiring ethical approval. The authors confirm that the research was conducted in accordance with accepted academic integrity and ethical publishing standards.

Author Contribution Statement: All authors contributed significantly to the development of this manuscript. Author 1 was responsible for the conceptualization, methodology, and overall supervision of the study. Author 4,5,6,7 and 8 handled data collection, analysis, and interpretation of results. Author 2 and 3 contributed to the literature review, drafting, and critical revision of the manuscript. All authors read and approved the final version of the manuscript prior to submission.

References

Abich IV, Julian & Reinerman-Jones, Lauren & Matthews, Gerald. (2016). Impact of three task demand factors on simulated unmanned system intelligence, surveillance, and reconnaissance operations. Ergonomics. 60. 10.1080/00140139.2016.1216171.

Alyssa Ryan, Cole Fitzpatrick, Eleni Christofa, Michael Knodler, (2020). Driver performance due to small unmanned aerial system applications in the vicinity of roadways, Transportation Research Part F: Traffic Psychology and Behaviour,Volume 68,2020, Pages 118-131, ISSN 1369-8478, https://www.sciencedirect.com/science/article/pii/S1369847819304516

Arifin, Bustanul & Damanik, Nur. (2020). The Implementation of Indonesia's Counter Piracy Strategies through Multilateral Cooperation in the Malacca Strait (2004-2009). Verity: Jurnal Ilmiah Hubungan Internasional (International Relations Journal). 12. 5. 10.19166/verity.v12i23.2482.

Anghuwo, J.S., Imanuel, P. & Nangolo, S.S. (2024). Anti-unmanned aerial vehicle detection system for airports: aviation and national security perspective. J Transp Secur 17, 12 https://doi.org/10.1007/s12198-024-00280-w

Aouladhadj, D., Kpre, E., Deniau, V., Kharchouf, A., Gransart, C., & Gaquière, C. (2023). Drone Detection and Tracking Using RF Identification Signals. Sensors, 23(17), 7650. https://doi.org/10.3390/s23177650

Asif Ali Laghari, Awais Khan Jumani, Rashid Ali Laghari, Haque Nawaz, (2023). Unmanned aerial vehicles: A review,Cognitive Robotics,Volume 3, Pages 8-22, ISSN 2667-2413,https://doi.org/10.1016/j.cogr.2022.12.004.(https://www.sciencedirect.com/science/article/pii/S2667241322000258)

Bernama (2025). Malaysia Condemn Drone Attack on Gaza-Bound Flotilla, Called in Cowardly and Inhumane. Published 10 September 2015.

Blazakis, J. (2006). Border Security and Unmanned Aerial Vehicles. Connections, 5(2), 154–159. http://www.jstor.org/stable/26323244

Calcara, A., Gilli, A., Gilli, M., & Zaccagnini, I. (2022). Will the Drone Always Get Through? Offensive Myths and Defensive Realities. Security Studies, 31(5), 791–825. https://doi.org/10.1080/09636412.2022.2153734

Chizek, Judy. (2003). Military Transformation: Intelligence, Surveillance and Reconnaissance. 34. https://www.researchgate.net/publication/235075622Military_Transformation_IntelligenceSurveillance_and_Reconnaissance/citation/download

Conventus Law (2022). Malaysia – Civil Remedies for Economic Espionage. Retrieved August 5, 2022 https://conventuslaw.com/report/malaysia-71-01-civil-remedies-for-economic-espionage/

De Benedetto, M. (2018). Effective Law from a Regulatory and Administrative Law Perspective. European Journal of Risk Regulation, 9(3), 391–415. doi:10.1017/err.2018.52

Des Butler (2019) Drones and Invasions of Privacy: An International Comparison of Legal Responses. UNSW Law Journal https://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2019/09/Issue-423-Butler-12.pdf

Devereaux A. (2024). Thermal Imaging and Drones in Military Tactics, The Havok Journal https://havokjournal.com/nation/science-technology/thermal-imaging-and-drones-in-military-tactics

Edwin Lee (2019).Flying Drone Legally in Malaysia. Lee & Poh Partnership accessible at https://lpplaw.my/insights/e-articles/flying-drones-legally/

Eric Gabriel Gomez (2020). Game of Drones. Skrine Advocate & Solicitor. Accessible at https://www.skrine.com/insights/newsletter/july-2020/games-of-drones

Gargi Sarkar, Sandeep K. Shukla, (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies, Journal of Economic Criminology, Volume 2, 100034,ISSN 2949-7914,https://doi.org/10.1016/j.jeconc.2023.100034.(https://www.sciencedirect.com/science/article/pii/S2949791423000349)

Henry Yeo (2020). Flying a commercial drone in Malaysia: Part 1 – Rules & Regulations. https://www.poladrone.com/blog/flying-drone-in-malaysia-rules-regulations-pt-1.html

Hua Siong, Wong. (2022). Usage of the Drones by Law Enforcement in Daily Duties: Legal Issues in Malaysia. International Journal of Law, Government and Communication. 7. 504-512. 10.35631/IJLGC.729036.

Hu, Dingkun & Minner, Jenni. (2023). UAVs and 3D modeling to Aid Urban Planning and Preservation: ASystematicReview.10.20944/preprints202310. 1015.v1. https://www.researchgate.net/publication/374785561_UAVs_and_3D_modeling_to_Aid_Urban_Planning_and_PreservationA_Systematic_Review/citation/download

Hu Liu, Mohd Hasrizam Che Man, Kin Huat Low, (2021) UAV airborne collision to manned aircraft engine: Damage of fan blades and resultant thrust loss. Aerospace Science and Technology, Volume113,2021,106645, ISSN1270-9638,https://doi.org/10.1016/j.ast.2021.106645. https://www.sciencedirect.com/science/article/pii/S1270963821001553

Javier Sutil Toledano (2024). Narco-Drones: The Use of Drones by Drug Cartels. Retrieved October 26, https://greydynamics.com/narco-drones-the-use-of-drones-by-drug-cartels/

Jean-Paul Yaacoub, Hassan Noura, Ola Salman, Ali Chehab, (2020). Security analysis of drones systems: Attacks, limitations, and recommendations,Volume 11, 2020,100218, ISSN 2542-6605,https://doi.org/10.1016/j.iot.2020.100218. (https://www.sciencedirect.com/science/article/pii/S2542660519302112)

Joe Russo, Dulani Woods, Michael J. D. Vermeer, Brian A. Jackson (2024). Countering the Emerging Drone Threat to Correctional Security. Research published Mar 13, 2024. https://www.rand.org/pubs/research_reports/RRA108-21.html

José Carlos Palma (2024). Unveiling the Tools and Techniques of Modern Espionage, https://smartencyclopedia.org/2024/05/12/unveiling-the-tools-and-techniques-of-modern- espionage

Joeaneke, Princess & Val, Onyinye & Olaniyi, Oluwaseun & Ogungbemi, Olumide Samuel & Olisa, Anthony & Akinola, Oluwaseun. (2024). Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques. Journal of Engineering Research and Reports. 26. 71-92. 10.9734/jerr/2024/v26i101291.

Kallenborn, Z., Ackerman, G., & Bleek, P. C. (2022). A Plague of Locusts? A Preliminary Assessment of the Threat of Multi-Drone Terrorism. Terrorism and Political Violence, 35(7), 1556–1585. https://doi.org/10.1080/09546553.2022.2061960

Katharina Ley Best, Jon Schmid, Shane Tierney, Jalal Awan, Nahom M. Beyene, Maynard A. Holliday, Raza Khan, Karen Lee (2020). How to Analyze the Cyber Threat from Drones Background, Analysis Frameworks, and Analysis Tools. Research Published Mar 5, 2020 https://www.rand.org/pubs/research_reports/RR2972.html

Keith Davis (2022). Geofencing on Drones (All You Need to Know). Accessible at https://www.droneblog.com/geofencing-on-drones/

Koslowski, R., & Schulzke, M. (2018). Drones along Borders: Border Security UAVs in the United States and the European Union. International Studies Perspectives, 19(4), 305–324. https://www.jstor.org/stable/27011733

Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. Contemporary Security Policy, 44(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

Laine, J. P. (2021). Beyond Borders: Towards the Ethics of Unbounded Inclusiveness. Journal of Borderlands Studies, 36(5), 745–763. https://doi.org/10.1080/08865655.2021.1924073

Linda Kay (2019). Chinese Wing Loong, United States' Predator in Battle to Sell Drones to Malaysia onApr7th,https://www.defenseworld.net/2019/04/07/chinese-wing-loong-united-states- predator-in-battle-to-sell-drones-to-malaysia.html

Lykou, Georgia & Moustakas, Dimitrios & Gritzalis, Dimitris. (2020). Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. Sensors. 20. 3537. 10.3390/s20123537.

Marhalim bin Abas (2020). Malaysia receives first batch of donated ScanEagle UAVs from US 27 March https://www.janes.com/osint-insights/defence-news/malaysia-receives-first-batch-of-donated-scaneagle-uavs-from-us

Marhalim Abas (2021) Lockheed Martin Radar for Malaysia. Accessible at https://www.malaysiandefence.com/lockheed-martin-radar-for-malaysia/

Marhalim bin Abas (2021). From Aludra To Matrice https://www.malaysiandefence.com/from-aludra-to-matrice

Marina, Miloš & Cokorilo, Olja & Mirosavljevic, Petar & Vasov, Ljubiša & Stojiljkovic, Branimir & Milovanović, Milica. (2024). Analysis of the impact of UAV collision on a commercial aircraft. https://www.researchgate.net/publication/385880332_Analysis_of_the_impact_of_UAV_collision_on_a_commercial_aircraft/

Marion Garaus, Melánia Hudáková (2022). The impact of the COVID-19 pandemic on tourists' air travel intentions: The role of perceived health risk and trust in the airline, Journal of Air Transport Management Volume 103, 102249, ISSN 0969-6997, https://doi.org/10.1016/j.jairtraman.2022.102249. (https://www.sciencedirect.com/science/article/pii/S0969699722000692)

Ministry of Justice@Rt Hon Damian Hinds MP (2023).New prison 'no-fly zones' for drug-delivering drones press release. Published 23 October 2023 https://www.gov.uk/government/news/new-prison-no-fly-zones-for-drug-delivering-drones

Mohit Arora, Stefan Tuchen, Mohsen Nazemi, Lucienne Blessing (2021). Airport pandemic response: An assessment of impacts and strategies after one year with COVID-19, Transportation Research Interdisciplinary Perspectives Volume 11, 100449, ISSN 2590-1982, https://doi.org/10.1016/j.trip.2021.100449.

Mohsan, S.A.H., Othman, N.Q.H., and Li, Y. et al. (2023) .Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. Intel Serv Robotics 16, 109–137 https://doi.org/10.1007/s11370-022-00452-4

Moonyati Yatid (2022). Cyber Risks in Malaysia's oil and gas industry. Malaysia Petroleum Resources Corporation https://mprc.gov.my/

Muhmad Kamarulzaman, A. M., Wan Mohd Jaafar, W. S., Mohd Said, M. N., Saad, S. N. M., & Mohan, M. (2023). UAV Implementations in Urban Planning and Related Sectors of Rapidly Developing Nations: A Review and Future Perspectives for Malaysia. Remote Sensing, 15(11), 2845. https://doi.org/10.3390/rs15112845

Navid Ahmadian, Gino J. Lim, Maryam Torabbeigi, Seon Jin Kim, (2022). Smart border patrol using drones and wireless charging system under budget limitation, Computers & Industrial Engineering, Volume 164, 2022, 107891, ISSN 0360-8352, https://doi.org/10.1016/j.cie.2021.107891. (https://www.sciencedirect.com/science/article/pii/S0360835221007956)

Nooralishahi, P., Ibarra-Castanedo, C., Deane, S., López, F., Pant, S., Genest, M., Avdelidis, N. P., & Maldague, X. P. V. (2021). Drone-Based Non-Destructive Inspection of Industrial Sites: A Review and Case Studies. Drones, 5(4), 106. https://doi.org/10.3390/drones5040106

NQ Defence Blog, (2024). What is Anti-Drone Technology? Accessible at https://www.nqdefense.com/what-is-anti-drone-technology/

Ottilia W. & Rameez Asif (2021). Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things, https://ueaeprints.uea.ac.uk/id/eprint/83147/1/Accepted_manuscript.pdf

Pietro, Roberto & Oligeri, Gabriele & Tedeschi, Pietro. (2019). JAM-ME: Exploiting Jamming to Accomplish Drone Mission. 10.1109/CNS.2019.8802717.

Pyrgies, John. (2019). The UAVs threat to airport security: risk analysis and mitigation. Journal of Airline and Airport Management. 9. 63. 10.3926/jairm.127. https://www.researchgate.net/publication/336336752_The_UAVs_threat_to_airport_security_risk_analysis_and_mitigation/citation/download

Rao, Bharat & Gopi, Ashwin Goutham & Maione, Romana. (2016). The societal impact of commercial drones. Technology in Society. 45. 83-90. 10.1016/j.techsoc.2016.02.009.

Rassler, D. (2018). Keep It Simple, Stupid! The Islamic State's Tactical and Operational Drone Innovations. In The Islamic State and Drones: Supply, Scale, and Future Threats (pp. 2–4). Combatting Terrorism Center at West Point. http://www.jstor.org/stable/resrep21486.5

Robin Kellermann, Tobias Biehle, Liliann Fischer, (2020). Drones for parcel and passenger transportation: A literature review. Transportation Research Interdisciplinary Perspectives, Volume 4, 2020, 100088, ISSN 2590-1982, https://doi.org/10.1016/j.trip.2019.100088. (https://www.sciencedirect.com/science/article/pii/S2590198219300879)

Seidaliyeva, U., Ilipbayeva, L., Taissariyeva, K., Smailov, N., & Matson, E. T. (2024). Advances and Challenges in Drone Detection and Classification Techniques: A State-of-the-Art Review. Sensors, 24(1), 125. https://doi.org/10.3390/s24010125

SentinelOne (2024). What is Cyber Espionage? Types & Examples https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-espionage

Shue, Henry and Wippman, David (2002) "Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions,"Cornell International Law Journal: Vol. 35: Iss. 3, Article 7. Pp 569-573. Available at: http://scholarship.law.cornell.edu/cilj/vol35/iss3/7

Stöcker, C., Bennett, R., Nex, F., Gerke, M., & Zevenbergen, J. (2017). Review of the Current State of UAV Regulations. Remote Sensing, 9(5), 459. https://doi.org/10.3390/rs9050459

Syed Zomael Hussain & Muhammad Azly Haziq (2019). Air Mobility in Malaysia: Laws and Regulations. Azmi & Assc. Accessible at https://www.azmilaw.com/insights/air-mobility- in-malaysia-laws-and-regulations/

Tan Kheng Soon, Ng Chiew Teng, et al (2024). Challenges and Barriers for Unmanned Aerial Vehicle (UAV) Implementation in Malaysian Infrastructure Projects. ASEAN Engineering Journal, 14(1), 237-243. https://doi.org/10.11113/aej.v14.2058

The Malaysian Lawyer (2019). A Bird's-eye View of Drone Regulation in Malaysia. Accessible at https://themalaysianlawyer.com/2017/03/02/a-birds-eye-view-of-drone-regulation-in-malaysia/#google_vignette

Tinshu Sasi, Arash Habibi Lashkari, Rongxing Lu, Pulei Xiong, Shahrear Iqbal, (2024).A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges, Journal of Information and Intelligence, Volume 2, Issue 6, Pages 455-513, ISSN 2949- 7159, https://doi.org/10.1016/j.jiixd.2023.12.001. (https://www.sciencedirect.com/science/article/pii/S2949715923000793)

Wardatul Hayat Adnan, Mohd Fadly Khamis (2022).Drone Use in Military and Civilian Application: Risk to National Security. Journal of Media and Information Warfare Vol. 15(1), 60-70, January 2022 https://jmiw.uitm.edu.my/images/Journal/Vol15No1/5-Drone-Use-in-Military-and-Civilian-Application-Risk-to-National-Security.pdf

Wong, Y. B., Gibbins, C., Azhar, B., Phan, S. S., Scholefield, P., Azmi, R., & Lechner, A. M. (2023). Smallholder oil palm plantation sustainability assessment using multi-criteria analysis and unmanned aerial vehicles. Environmental monitoring and assessment, 195(5), 577. https://doi.org/10.1007/s10661-023-11113-z

Yamaguchi Mari, (2016). Drone found on roof of Japanese prime minister's office April 22, 2015. Miami Herald, Archived March 10, 2016 https://www.miamiherald.com/news/nation-world/world/article19207314.html

Yunus, Asniza & Hamzah, Abd & Azmi, Fatin Afiqah Md. (2020). Drone Technology as A Modern Tool in Monitoring the Rural-Urban Development. IOP Conference Series: Earth and Environmental Science. 540. 012076. 10.1088/1755-1315/540/1/012076.

Zachary K (2023). Why cheap drones pose a significant chemical terrorism threat. Retrieved on November 21, 2023. Bulletin of Atomic Scientist https://thebulletin.org/2023/11/why-cheap-drones-pose-a-significant-chemical-terrorism-threat/

Zaf Seraj (2024). Report: Stricter enforcement of drone registration, permission to fly by Q3 2025, says civil aviation chief. Malay Mail. Accessible at https://www.malaymail.com/news/malaysia/2024/06/03/report-stricter-enforcement-of- drone-registration-permission-to-fly-by-q3-2025-says-civil-aviation-chief/137829

Zitar, Raed & Al-Betar, Mohammed & Ryalat, Mohammad & Kassaymeh, Sofian. (2023). A review of UAV Visual Detection and Tracking Methods.