Malaysian Journal of Syariah and Law
مجلة الشريعة والقانون بماليزيا
USIM

Vol. 13, No. 2, pp. 325-338 | AUGUST 2025
DOI: https://doi.org/10.33102/mjsl.vol13no2.1102

MALAYSIAN COMMUNICATION AND MULTIMEDIA COMMISSION'S (MCMC) LAW ENFORCEMENT SPECTRUM: EXPLORING ARREST AUTHORITY

[i,*]Mimi Sofiah Ahmad Mustafa, [i]Yuhanza Othman, [i]Nasihah Naimat, [i]Ida Rahayu Mahat, [i]Marziana Abd Malib, [i]Mohd Ab Malek Md Shah & [ii]Muhammad Arif Haron

[i]Department of Law, Universiti Teknologi MARA Cawangan Melaka Kampus, KM 26, Jalan Lendu, 78000 Alor Gajah, Malacca, Malaysia
[ii]Melaka Malaysian Communication and Multimedia Commission, No. 24-4, Aras 4, Bangunan Kota Cemerlang, Hang Tuah Jaya, 75450, Lebuh Ayer Keroh, Melaka, Malaysia

*(Corresponding author) e-mail: mimi@uitm.edu.my

Article history:
Submission date: 21 November 2024
Received in revised form: 22 May 2025
Acceptance date: 20 June 2025
Available online: 31 August 2025

Keywords:
MCMC, issues, scam, power of arrest, jurisdiction

Funding:
This research was funded by the Research and Industrial Linkages Department of Universiti Teknologi MARA Melaka under the Skim Geran Dalaman TEJA (GDT2024/1-14).

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
Ahmad Mustafa, M. S., Othman, Y., Naimat, N., Mahat, I. R., Abd Malib, M., Md Shah, M. A. M., & Haron, M. A. (2025). Malaysian Communication and Multimedia Commission's (MCMC) law enforcement spectrum: Exploring arrest authority. *Malaysian Journal of Syariah and Law*, *13*(2), 325-338.
https://doi.org/10.33102/mjsl.vol13no2.1102

ABSTRACT

The Malaysian Communications and Multimedia Commission (MCMC) regulates multimedia and communication activities and plays a role in protecting consumers from harms such as online scams and digital fraud. However, it is rather ironic that the unit mandated to receive public complaints about scams does not have the power to make an arrest upon the presentation of sufficient proof, a task that often rests with the Royal Malaysian Police Department (RMPD). Therefore, this study examines a key enforcement gap in the Malaysian Communications and Multimedia Commission's (MCMC) role, specifically its lack of arrest powers when handling scam-related complaints. It highlights the challenges this limitation poses and proposes the inclusion of arrest authority to strengthen MCMC's enforcement effectiveness. In doing so, this study employed a qualitative research method in which data were collected through semi-structured interviews conducted with officers from the MCMC, the RMPD, and the Ministry of Communications and Multimedia. Secondary data were gathered from internet sources, relevant legislations, and journals to illustrate the law in this area. Upon analysing the primary and secondary data, the researchers found that it is imperative to grant arrest power to the MCMC due to the challenges encountered in carrying out its tasks. The outcomes of this study can facilitate the Parliament in passing a law to confer the power of arrest to the MCMC through the current legislation, thus reducing the burden of the RMPD in making arrests related to media and communication cases. The public directly benefits from this study as it raises their confidence to lodge complaints with the MCMC, knowing fully well that the commission possesses the power to make an immediate arrest.

Introduction

The Malaysian Communications and Multimedia Commission (MCMC) is a statutory body established under the Malaysian Communications and Multimedia Commission Act 1998 (Act 588) to regulate and oversee the nation's communications and multimedia sectors. As the primary regulator, the MCMC plays an important role in telecommunications, broadcasting, and online services, with responsibilities encompassing consumer protection, licensing, content monitoring, innovation promotion, and cybersecurity (Shariff & Kosmin, 2015; MCMC, 2013). The law enforcement power of the MCMC is governed by various acts, including the Communications and Multimedia Act 1988, the Communications and Multimedia Commission Act 1998, the Digital Signature Act 1997, and the Postal Service Act 2012.

In today's digital landscape, the rising number of cyber threats, ranging from online fraud to content-related offences, has placed increasing pressure on the MCMC to respond more swiftly and effectively. According to MyCERT (2025), over 3,000 cybersecurity incidents were reported in the first half of 2024 alone, including data breaches, intrusion attempts, and fraud (CyberSecurity Malaysia, 2024). Despite receiving public complaints and evidence of online scams, the MCMC lacks the legal authority to make arrests, a role currently limited to the Royal Malaysian Police Department (RMPD). This gap often delays enforcement and may hinder the preservation of digital evidence.

This study examines whether granting arrest powers to the MCMC is a necessary and viable measure in addressing modern cybercrime challenges. It critically analyses the legal, ethical, and practical implications of such a reform, contributing to ongoing discussions on regulatory governance and digital enforcement in Malaysia.

The Malaysian Communications and Multimedia Commission: Mandate and Enforcement Powers

The MCMC serves as the primary regulatory authority overseeing Malaysia's communications and multimedia industry, including telecommunications, broadcasting, and internet services (Shariff & Kosmin, 2015). Established in 1998 as part of Malaysia's convergence-driven regulatory reform, the MCMC replaced the outdated Telecommunications Act 1950 and Broadcasting Act 1988. Its creation marked a significant shift toward unified regulation in response to the rapid evolution of digital communications.

The MCMC's mandate extends beyond telecommunications. It acts as a regulatory authority, consumer watchdog, licensing body, compliance enforcer, and innovation promoter (Kee et al., 2015). It also oversees cybersecurity, content regulation, and digital safety, and manages the spectrum and postal services under the Postal Services Act 2012. The Commission's functions include promoting competition, enforcing licensing conditions, monitoring technical compliance (e.g., frequency spectrum use). and curbing offensive or illegal online content in alignment with cultural norms.

Over time, the MCMC has expanded its influence. It regulates postal and courier services, licenses Certification Authorities under the Digital Signature Act 1997, and plays a central role in initiatives like Jalinan Digital Negara (JENDELA) for broadband development and National Digital ID for secure online identity verification. It has also spearheaded campaigns such as Sebenarnya.my to combat misinformation, particularly during the COVID-19 pandemic. In addition, the MCMC has intensified efforts in public education and digital literacy to bridge the digital divide and foster responsible internet usage.

Despite this expansive regulatory reach, the MCMC's enforcement powers are currently limited in scope. It is authorised to impose fines and financial penalties on individuals or organisations that violate the Communications and Multimedia Act 1998 and related legislation (Kee et al., 2015). These fines can range from thousands to millions of Ringgit Malaysia, depending on the breach. The Commission may also compound offences, offering settlement through monetary payment in lieu of prosecution.

Beyond financial penalties, the MCMC may issue warnings and formal notices for non-compliance (Bada & Nurse, 2020). It can revoke or suspend the licences of service providers who repeatedly or seriously violate regulatory requirements (Ahmad & Nordin, 2018). In such cases, the suspension may be temporary while investigations proceed or permanent in extreme instances of non-compliance.

Further, the MCMC holds authority to revoke or reallocate spectrum assignments and to impose technical or operational restrictions on service providers that fail to meet prescribed quality standards (Kitsiou et al., 2024). These powers serve as indirect means of compelling compliance while protecting consumer interests.

The MCMC is also empowered to investigate regulatory breaches, collect evidence, and conduct interviews. It may initiate legal proceedings against violators and seek judicial enforcement of its decisions (Fisher et al., 2017). However, despite these enforcement mechanisms, the absence of direct arrest powers continues to restrict the MCMC's effectiveness in swiftly addressing time-sensitive cyber offences and online fraud.

Limitations of MCMC Powers to Effectively Combat Digital Crimes and Violations

Existing limitations that hinder the MCMC from effectively carrying out its functions must be outlined and explained to justify the call for arrest powers.

Regarding jurisdiction, the MCMC faces apparent challenges, especially as digital crimes often transcend national borders, making it difficult for the commission to exercise its enforcement powers against perpetrators located outside Malaysia (Shukurov & Jafarov, 2023). Cross-border crimes such as hacking, phishing, and online fraud are perpetrated by individuals or groups operating from other countries. The MCMC's jurisdiction is limited to Malaysia, making international cooperation essential but often challenging.

Additionally, as the methods employed by cybercriminals become increasingly sophisticated, the use of equally sophisticated technologies can outpace regulatory measures (Alnifie & Kim, 2023). The use of advanced encryption, anonymisation tools, and other technologies by cybercriminals can make it difficult for the MCMC to track and identify the offenders. The rapid pace of technological advancements often means that regulatory frameworks struggle to keep up, leaving gaps that cybercriminals can exploit.

The MCMC may also face limitations in terms of financial, human, and technical resources necessary to effectively combat digital crimes (Rahim & Pawanteh, 2019). Limited resources often hinder effective monitoring, investigation, and enforcement, thus impacting the commission's ability to respond swiftly and comprehensively to digital crimes. There is also a constant need for highly skilled cybersecurity professionals who can keep up with the latest threats and technologies. Realistically, recruiting and retaining such talent can be quite challenging.

Furthermore, existing laws and regulations may not fully cover the scope of new and emerging digital threats (Familoni, 2024). Outdated legislation may lag behind technological advancements, leaving certain digital crimes inadequately addressed by the existing legal framework (Anwary, 2022). New forms of digital crimes, such as those involving cryptocurrencies or emerging technologies, may fall outside the scope of current regulations.

With regard to coordination and collaboration issues, effectively combating digital crimes requires the involvement of multiple agencies and stakeholders, which can be challenging to achieve (Chetry & Sharma, 2023). Crucial inter-agency collaboration can be hampered by bureaucratic hurdles and jurisdictional issues, causing ineffective enforcement collaboration with other national and international law enforcement agencies (Uzougbo et al., 2024; Cohen, 2017). Engaging with private sector entities, such as internet service providers and technology companies, is paramount for effective enforcement but can be difficult due to varying priorities and interests.

Methodology

This study adopts a qualitative research design, combining doctrinal legal analysis with empirical inquiry through semi-structured interviews. The choice of this hybrid approach is justified by the dual objectives of the study: (1) to examine the legal and constitutional framework governing the power of arrest in Malaysia, and (2) to understand the practical implications, perceptions, and challenges faced by enforcement agencies regarding the possible extension of such powers to the Malaysian Communications and Multimedia Commission (MCMC).

The informants in this study also included 10 staff members from the Ministry of Communication, to whom the researchers distributed questions via Google Forms to gather their opinions regarding the arrest authority granted to the MCMC. The following table summarises the information gathered from them.

Table 1. Background of the Informants

Informants	Gender	Division	Duration of service at the Ministry of Communications
R1	Male	Social Media and New Social Division	Less than 5 years
R2	Male	Cyber Media Division	Above 10 years
R3	Male	Crisis Management Division	Above 10 years
R4	Female	Social Media and New Social Division	Less than 5 years
R5	Male	Social Media and New Social Division	Above 10 years
R6	Male	Content Development Division	Less than 5 years
R7	Female	Social Media and New Social Division	Less than 5 years
R8	Male	Visual Communication and Design Arts Division	Above 10 years
R9	Male	Communication Committee Division	Less than 5 years
R10	Male	Information Division	Above 10 years

The doctrinal component involved an in-depth analysis of primary and secondary legal sources, including statutory provisions, subsidiary legislation, case law, scholarly journal articles, and authoritative texts. This method is suitable for critically evaluating the legal positioning of the MCMC within Malaysia's constitutional structure, particularly regarding the separation of powers, human rights protections, and administrative law doctrines. Sources were selected based on their relevance, authority, and publication credibility, with an emphasis on materials published within the last ten years to ensure contemporary relevance.

In parallel, the empirical component employed semi-structured interviews to gather insights from key stakeholders. Interviews were conducted with officers from the MCMC, the Royal Malaysia Police Department (RMPD), and officials from the Ministry of Communications and Multimedia. This method was chosen for its flexibility and effectiveness in eliciting detailed, experience-based responses while allowing for probing follow-up questions. Interviews were conducted via online platforms (Cisco Webex), telephone calls, and supplemented by correspondence through WhatsApp and personal messaging, which proved necessary due to scheduling constraints and pandemic-era communication norms.

The integration of doctrinal and empirical methods enables a comprehensive understanding of the issue from both normative and practical perspectives. While doctrinal research provides the legal foundation and critical constitutional analysis, qualitative interviews add experiential depth and context, capturing nuances that are often absent in purely textual legal analysis. This triangulation of data sources also enhances the validity and credibility of the findings by incorporating multiple viewpoints from regulators, law enforcement, and policymakers.

This study employed purposive sampling to identify individuals with direct expertise in cyber enforcement, regulatory compliance, and digital policy. Key informants were selected based on their institutional roles and relevance to the research topic. Participants included officers from the Malaysian Communications and Multimedia Commission (MCMC), ten senior officials from the Ministry of Communications and Multimedia Malaysia, and a representative from the Royal Malaysia Police (PDRM). Semi-structured interviews were conducted via online meetings, telephone calls, and secure messaging platforms such as WhatsApp, allowing for flexible and candid participation. Data collected from the interviews were transcribed and analysed using thematic analysis. Responses were coded manually and then grouped into emerging themes to identify recurring concerns and divergent viewpoints, particularly regarding enforcement limitations, legal frameworks, and views on expanding the MCMC's powers.

Case Studies and Examples

The enforcement of digital legislation in the rapidly changing digital ecosystem presents several issues for the Malaysian Communications and Multimedia Commission (MCMC). The following case studies and real-world examples highlight these difficulties.

The first example entails the spread of false information and fake news during the COVID-19 pandemic. Like many other nations, Malaysia experienced a spike in the dissemination of false information and fake news during this time (Islam et al., 2020). The MCMC had to deal with a significant volume of false information being disseminated on social media about the virus, available treatments, and governmental regulations. One of the main difficulties was separating damaging disinformation from free speech. To maintain public safety without violating the right to free speech, the MCMC must exercise caution. Additionally, it was challenging for the commission to identify the source of such content, particularly when it was distributed using encrypted messaging services like WhatsApp (Henrina et al., 2021). Thus, the MCMC adopted a more proactive stance by launching public awareness programmes and working with tech companies to remove dangerous content. However, the sheer amount of false information was hard to control, underscoring the difficulty of real-time digital content regulation.

The global reach of websites like YouTube, which allow the inflow of content from all over the world, is another major challenge for the MCMC. Since the commission has little authority over content hosted outside Malaysia, it is challenging to enforce local laws (Zubaidi, 2021). In this regard, the MCMC frequently experiences delays in eliminating or controlling content that is judged improper or unlawful by Malaysian law. This is because the procedure necessitates collaboration with the platform owners, who may be subject to distinct regulatory requirements. The MCMC has endeavoured to establish connections with international tech firms to accelerate the removal of information. However, jurisdictional issues remain a major obstacle to the successful implementation of digital legislation.

Additionally, data privacy and personal data protection are major concerns. A significant data breach in 2017 exposed the private information of 46.2 million Malaysian mobile phone users (Straits Times, 2017). The hacking seriously called into question the security of personal information and the efficacy of current laws (Mohamad et al., 2024). Finding the source of the leak and bringing the offenders to justice was a challenge for the MCMC. Issues were also raised over the effectiveness of the current Personal Data Protection Act 2010 (PDPA) in preventing such occurrences, leading to calls for improved enforcement procedures and stricter data protection regulations. To prevent such violations in the future, weaknesses in the regulatory framework must be effectively addressed by the MCMC and other agencies.

Freedom of speech and internet censorship are also important issues. The MCMC has been active in banning access to websites that violate Malaysian law, including those that promote unlawful gambling, terrorism, or hate speech. Restricting dangerous content while upholding the right to free expression is a difficult task. Some content producers have managed to work around the restrictions, such as by using VPNs or mirror sites. Although the MCMC has been successful in blocking several unlawful websites, the effectiveness of these measures is frequently short-lived due to the adaptability of content creators. This has sparked ongoing discussions about Malaysia's optimal strategy for internet censorship.

These instances highlight the various difficulties faced by the MCMC in implementing digital laws, including concerns about jurisdiction, technological development, and striking a balance between freedom of speech and regulation.

Literature Review

Many studies have examined the effectiveness of the MCMC's enforcement powers, but very few have addressed the need to confer arrest power to the commission. The issue of granting arrest authority to non-police regulatory entities is an increasingly relevant topic, especially as these bodies tackle complex challenges in the digital and economic spheres. Scholars argue that as regulatory agencies, such as telecommunications and financial commissions, assume greater responsibility for enforcing sector-specific laws, arrest authority could serve as a critical tool for deterring violations and ensuring compliance (Sihabudin, 2023; Héritier & Karremans, 2021; Dudley & Wegrich, 2015). For instance, regulatory agencies equipped with limited arrest powers, as seen in cases within the US Securities and Exchange Commission, demonstrate enhanced enforcement potential against digital and financial crimes (Davis, 2012). However, literature on administrative law warns of significant risks associated with empowering non-police bodies, especially given their limited training in law enforcement and the absence of established oversight mechanisms typical of traditional police forces (De Hert, 2016). Comparative studies in regulatory governance suggest that jurisdictions granting arrest powers to non-police entities, such as customs and immigration authorities in the EU, often apply strict accountability frameworks to

prevent potential abuses and protect civil liberties (Dudley & Wegrich, 2015). Ethical concerns, including risks of regulatory capture and erosion of public trust, highlight the need for a balanced approach, where any expansion of arrest powers is accompanied by rigorous safeguards and transparency measures (Marzouki, 2021). These studies suggest that while arrest authority could strengthen regulatory impact, its implementation must be carefully managed to uphold democratic values and public accountability.

In addition, comparative studies on non-police enforcement powers provide insight into how various jurisdictions manage and limit these authorities. For instance, in the US, agencies like the Securities and Exchange Commission (SEC) have enforcement capabilities but rely on partnerships with law enforcement for arrests (Stechschulte, 2022). The European Union practices a similarly cautious approach, granting limited detainment rights to customs and border agencies under strict oversight (European Parliament & Council of the European Union, 2018). These case studies reveal a trend towards specialised, narrowly defined powers for non-police agencies, aimed at addressing regulatory gaps without infringing on civil liberties. Practical challenges accompany the implementation of arrest powers for non-police entities. Studies highlight that these bodies often lack the training, experience, and procedural protocols of law enforcement agencies, which can lead to legal and ethical issues (Kee et al., 2015). Additionally, scholars warn that empowering non-police agencies with such authority can blur the line between regulation and criminal enforcement, potentially leading to conflicts with existing police agencies and ambiguity in citizens' rights during regulatory detentions (Koziarski & Lee, 2020).

The Legal Framework Governing Law Enforcement Powers in Malaysia

The legal framework for law enforcement powers in Malaysia is a multi-layered and complex system that aims to balance the enforcement of laws with the preservation of individual rights. A combination of statutory law, constitutional provisions, and judicial interpretations shape this framework, reflecting Malaysia's commitment to upholding the rule of law while ensuring public safety and order. The Federal Constitution of Malaysia, as the supreme law, establishes key provisions related to enforcement law and delineates that the enforcer's power should uphold the fundamental rights of citizens at the core of this legal framework.

The Federal Constitution contains several key provisions that directly impact law enforcement activities. For instance, Article 5 protects an individual's liberty and guarantees the right to a fair trial. According to Hashim (2013), the term 'right to life' in Article 5 includes the right to have a livelihood, a healthy environment, and modern healthcare. In addition, Article 9 of the Federal Constitution grants citizens the right to move freely throughout the Federation. Despite the constitutional protection of freedom of movement, it remains subject to several restrictions, including laws relating to security, public order, public health, or the punishment of offenders, and such laws cannot be challenged on the grounds that they do not relate to any of these matters (Ahmad Masum et al., 2021). Article 10 of the Constitution guarantees the right to freedom of expression, assembly, and association, subject to specific legal limitations based on national security, public order, and morality. These constitutional articles establish a fundamental legal framework that governs the conduct of all law enforcement powers.

The main enforcement agency in Malaysia is the Royal Malaysian Police (RMP). The Police Act 1967 governs the role and duties of the RMPD. The Act outlines the police's general duties, which include maintaining law and order, preventing and detecting crime, and enforcing the law. It also sets out the conditions under which police officers can arrest individuals without a warrant and details their powers to conduct searches and seize property linked to criminal activity.

The Criminal Procedure Code (CPC) complements the Police Act 1967 by addressing the implementation of law enforcement activities. It specifically outlines the procedural elements of criminal investigations, arrests, detentions, and trials. The CPC provides clear guidelines on appropriate arrest procedures and the legal rights of detained individuals. It grants law enforcement bodies the authority to carry out investigations, gather evidence, and question individuals, guaranteeing a lawful and methodical execution of these procedures. The CPC also outlines the conditions under which individuals can receive bail or remain in custody, offering comprehensive details about the procedural safeguards that guarantee the protection of the accused's rights.

In addition, the Dangerous Drugs Act of 1952 grants significant powers to law enforcement agencies, specifically addressing offences related to drug trafficking and abuse. Section 39B of the Act imposes severe penalties for drug trafficking, including the death penalty, and gives the police wide powers to combat drug offences (Dangerous Drugs Act 1952). Section 31 allows for the arrest and detention of persons suspected of drug trafficking without a warrant (Dangerous Drugs Act 1952).

Besides the aforementioned statutes, Parliament has also introduced tstatutes that contain enforcement powers to control specific agencies' operations. and powers. For example, the Customs Act 1967 establishes the authority of the Royal Malaysian Customs Department to enforce customs laws, while the Immigration Act 1959/63 sets out the powers of the Immigration Department concerning individuals' entry, residence, and release. The Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) also provides enforcement powers to freeze, seize, and forfeit properties involved in money laundering and terrorism financing.

The legal framework governing law enforcement powers in Malaysia is comprehensive, combining constitutional protections, statutory provisions, specific agency laws, and oversight mechanisms. Law enforcement should operate under a precisely defined legal framework, tailored to its specific tasks and responsibilities, to safeguard both national security and individual rights.

International Perspectives on Best Practices of Enforcement Power in Other Countries

Enforcement power is the process of ensuring that the law is upheld through monitoring, the imposition of penalties, and even arrest authority. People regard the law as toothless when no action is taken against wrongdoers. In term of arrest authority, countries worldwide have similar practices in enforcing such measures.

Arrest authority pertaining to internet and social media offences involves the legal power granted to law enforcement agencies to detain individuals suspected of committing crimes online (Clifford, 2011). These offences include cyberbullying, hacking, identity theft, online fraud, dissemination of illegal or sensitive content, harassment, body shaming, and more. The process typically involves investigation, warrants, arrest, and prosecution. However, laws governing these processes vary by jurisdiction.

Examples from American experiences can be seen in several recorded cases. In 2013, the Federal Bureau of Investigation (FBI) shut down Silk Road, an online black market operating on the dark web. The site's founder, Ross Ulbricht, was arrested and later sentenced to life in prison (Hawdon, 2021). The site facilitated the sale of illegal drugs, weapons, and other illicit goods and services. In the same year, the police apprehended cybercriminals who stole credit and debit card information from over 40 million Target customers during the holiday shopping season. The breach involved malware installed on Target's point-of-sale systems.

The arrest of online criminals in the UK follows a structured process that integrates traditional law enforcement procedures with specialised digital investigation techniques. The procedures involve reporting and initial assessment, investigation and evidence gathering, legal authorisation, arrest operation, Miranda rights and processing, evidence seizure and documentation, prosecution and legal proceedings, penalties and sentencing, and international cooperation (if applicable). Enforcement actions require specialised knowledge of digital technologies, cyber laws, and procedural compliance. They involve collaborations between law enforcement agencies, digital forensic experts, cybersecurity professionals, and legal authorities to ensure effective investigation, prosecution, and prevention of cybercrimes.

Chetry and Sharma (2023) state that Australia takes a comprehensive approach to arresting cybercriminals, involving multiple agencies and coordinated efforts. The process includes detection and reporting, investigation, operations and arrest, and legal proceedings. Australia's approach to combating cybercrime is robust and involves continuous efforts to stay ahead of evolving threats. The collaboration between federal and state agencies, along with international partners, is crucial in tackling this global issue (Persadha et al., 2015). For instance, as a result of the Australian arm of the investigation led by the Australian Federal Police (AFP) and Joint Policing Cybercrime Coordination Centre (JCP3), more than 200 officers from the AFP and state and territory police were involved in executing 22 search warrants

across five states on 17 April 2024. This included fourteen in Victoria, two in Queensland, three in New South Wales, one in South Australia, and two in Western Australia (AFP, 2024).

Discussions

This section examines the legal, constitutional, and ethical implications of extending arrest powers to the Malaysian Communications and Multimedia Commission (MCMC). Building on the doctrinal and empirical findings presented earlier, the discussion explores whether such an expansion of authority is justifiable within Malaysia's legal framework and aligns with broader human rights standards. It considers both the practical enforcement challenges faced by the MCMC, and the potential risks associated with granting arrest powers to a regulatory body. By weighing operational efficiency against constitutional principles and public accountability, this section seeks to present a balanced analysis of the proposed reform.

i. The Legal and Conceptual Framework of Arrest in Malaysia

This section introduces the traditional legal understanding of arrest within Malaysian law and how arrest powers are conventionally associated with the police. Harmon (2016) asserts that arrests are quintessential police functions, unchallenged even by reformists. Similarly, Dube & Bedi (2021) emphasise that arrest is a fundamental element of policing that inherently restricts liberty until reviewed by the courts. These conceptual foundations reinforce the deeply institutionalised link between arrest and police authority in Malaysia.

ii. Regulatory Limitations of the MCMC in Combating Online Fraud

This subsection highlights the operational limitations faced by the MCMC in addressing the rise of cybercrimes, especially online fraud, and justifies the motivation behind the proposed extension of arrest powers. Despite increasing public complaints and clear evidence, the MCMC cannot detain suspects due to the absence of arrest authority. Naturally, this could significantly impede timely intervention in fast-moving cybercrime cases such as banking scams and phishing schemes (MCMC, n.d.).

iii. Constitutional and Doctrinal Concerns: Separation of Powers

This subsection explores how the separation of powers doctrine under the Malaysian Federal Constitution potentially limits the expansion of enforcement powers to non-police bodies like the MCMC. Montesquieu's doctrine of separation of powers argues for clear boundaries between legislative, executive, and judicial authority (Akhtar, 2022; Barberis & Sardo, 2024). Extending arrest powers to the MCMC, a body under the executive branch, risks encroaching on traditional functions of law enforcement and potentially judicial review mechanisms (Police Act, 1967).

iv. Human Rights and Constitutional Safeguards

This subsection elaborates on how any arrest authority must conform to the rights enshrined in the Federal Constitution and international human rights norms. Articles 5 and 8 of the Federal Constitution provide for the right to personal liberty, due process, and equality before the law. Malaysia's commitment to international human rights instruments, including the Universal Declaration of Human Rights (UDHR), necessitates careful legal design of enforcement powers (Sreedharam & Ramayah, 2020; Bidin & Khan, 2022).

v. Ethical Implications of Expanding Enforcement Authority

This section introduces ethical concerns such as potential power abuse, biased enforcement, and mission creep if the MCMC is given police-like authority. Brady (2019) warns that extended enforcement mandates often lead to civil rights violations if not well regulated. The MCMC's involvement in sensitive content moderation tasks heightens the risk of infringing freedom of expression and disproportionately targeting particular groups.

vi. Accountability and Transparency in Enforcement

This final analytical section provides solutions and risk mitigation strategies through accountability, transparency, and oversight mechanisms. Strong internal governance mechanisms such as audits, public complaints channels, and independent oversight must accompany any new enforcement mandate (Mulgan, 2000; Bolívar et al., 2015). Saripan et al., (2022) and Tregidga et al., (2019) emphasise that legitimacy and ethical compliance rest on accountability, while Fox (2007) and Stasavage (2020) argue that transparency fosters public trust.

Analysis from Interviews

Interviews conducted with officers from the Malaysian Communications and Multimedia Commission (MCMC) highlighted a recurrent concern. The lack of arrest power is a significant hindrance to effective enforcement, particularly in time-sensitive cybercrime cases. A central theme that emerged was the dependence on external agencies, especially the Royal Malaysia Police (RMP), which often causes delays and operational inefficiencies. For instance, Mr. Sithick Ali Abd Salam, the Johor Deputy Director of MCMC, explained during an online interview on 11 September 2024 that opening an investigation paper requires police involvement. Specifically, it must be signed by an Assistant Superintendent of Police (ASP). In rural areas, where stations may be led by lower-ranking officers, MCMC officers must travel to District Police Headquarters to secure the necessary authorisation, which risks evidence tampering or loss due to delays.

Another commonly raised issue was the difficulty in handling high-profile cases, namely, those involving race, religion, or royalty, which must be investigated within strict timelines (typically 30 days). Respondents noted that suspects in such cases are often mobile and alerted in advance, potentially through leaked information. As a result, MCMC officers may arrive at locations where suspects have already fled or have had time to delete, alter, or hide incriminating digital content. These themes point to a shared frustration among MCMC officers regarding limited autonomy in enforcement and a strong consensus that arrest powers could enhance response time and evidence integrity.

Despite this consensus among MCMC officers (R1–R10), it is critical to interrogate the assumption that granting arrest powers would be an unequivocal improvement. Assistant Superintendent of Police Tuan Jasnie bin Misran of Bukit Aman, for example, expressed caution. He emphasised that conferring arrest powers to the MCMC might blur jurisdictional boundaries, resulting in overlapping authority, potential inter-agency conflicts, and duplication of efforts. His concerns highlight a valid risk: too many entities with similar enforcement powers can lead to procedural confusion, hinder effective coordination, and ultimately diminish accountability.

Beyond institutional friction, legal and human rights concerns must be addressed. Granting arrest powers to a regulatory body like the MCMC, which traditionally focuses on oversight and technical matters rather than direct law enforcement, may raise questions about due process, proportionality of power, and oversight mechanisms. Without adequate checks and balances, MCMC officers could exercise arrest powers in a manner that infringes upon freedom of expression and privacy rights, particularly in politically sensitive or high-profile cases. There is also the risk of mission creep, where regulatory objectives become entangled with punitive enforcement, potentially undermining public trust.

Based on Table 2 below, these responses are organised into themes to help contextualise the qualitative findings and set the stage for deeper discussion, particularly around how to reconcile calls for operational efficiency with concerns about constitutional authority, regulatory boundaries, and the necessity for legislative reform.

i. Enforcement Deficiencies as the Dominant Concern: All respondents (R1–R10) identified enforcement challenges as the central obstacle to combating cybercrime. This was frequently linked to gaps in capabilities or procedural acceleration, such as delays in obtaining police assistance or limitations imposed by incomplete legislation.

ii. Supporting Arrest Power as a Means to Strengthen Enforcement: A majority of respondents (R1–R6) favoured granting MCMC arrest powers. R1, R2, R3, R4, R5, and R6 highlighted that such authority would enable faster, more direct action, prevent evidence tampering, and help ensure impartial justice. Responses emphasised that the MCMC should not just regulate but also act when wrongdoing is detected, particularly given its digital oversight role.

iii. Concerns Over Institutional Role and Jurisdiction: In contrast, R7–R10 opposed MCMC having arrest powers, cautioning that MCMC is fundamentally a regulatory body and that traditional arrests should remain the remit of law enforcement. They noted that existing specialised agencies already bear arrest authority, and that expanding MCMC's mandate may cause overlaps, confusion, or legal overreach.

iv. Legislative and Jurisdictional Gaps: Across responses, gaps in legislation and unclear jurisdiction hinder enforcement effectiveness. Some respondents mentioned incomplete legal frameworks or lack of enabling statutes (R2-R10), suggesting that before power expansion, enabling legislation must be developed and jurisdictional boundaries clarified.

Table 2. Responses in relation to the power of arrest for MCMC

Informant	Main Issues in Solutions to Cybercrime and Offences	Answer for Previous Question (if any, otherwise 'None')	Agreement on Granting MCMC Power of Arrest	Reason for Agreement or Disagreement
R1	Facilities or technical resources, enforcement, others	Enforcement by the Authority	Yes	Because MCMC can monitor and take immediate action for an offence
R2	Enforcement, incomplete legislation	None	Yes	As a commission, it should play this role to strengthen enforcement
R3	Enforcement, incomplete legislation	None	Yes	Strengthening enforcement
R4	Enforcement, incomplete legislation	None	Yes	So that justice is not biased
R5	Facilities or technical resources, enforcement, jurisdiction	Enforcement needed	Yes	Must have legislation and enforcement
R6	Facilities or technical resources, enforcement, jurisdiction	None	Yes	Because it facilitates the search for all detected data
R7	Enforcement, incomplete legislation	None	No	MCMC is not an enforcement body that has the power of arrest
R8	Enforcement, incomplete legislation	None	No	MCMC can prosecute offenders, while arrests can only be made by enforcement authorities
R9	Facilities or technical resources, enforcement, jurisdiction	None	No	There are other special agencies responsible for this issue
R10	Enforcement, incomplete legislation	None	No	Arrests by the authorities: the police can arrest, while MCMC can only prosecute

Table 3. Thematic Summary of Informants' Views on MCMC's Arrest Powers

Theme	Details
Enforcement Weaknesses	Frequent delays, limited authority, and an incomplete legal framework undermining cybercrime response
Support for MCMC Arrest Powers	Cited need for timely intervention, evidence preservation, and fair justice
Institutional Role Concerns	Opposition based on MCMC's non-enforcement mandate and the risk of overlapping jurisdiction
Legislative and Jurisdictional Gaps	Need for clear laws and defined mandates before expanding arrest authority

Therefore, while the interviews reveal a compelling narrative of operational bottlenecks caused by reliance on external enforcement, any move to expand MCMC's authority must be carefully calibrated. It must include clear legal frameworks, training protocols, and oversight mechanisms to prevent abuse, protect civil liberties, and maintain institutional clarity between MCMC and the police. The researchers believe this could prompt further studies to explore a feasible and practical framework for establishing an arrest unit within the MCMC.

Suggestions

Based on all the above, there are two arguments regarding whether or not the MCMC should be conferred the power of arrest. Arguments for granting arrest authority to the MCMC include improved efficiency due to the streamlining of processes for combating cybercrimes, by reducing bureaucratic hurdles and centralising enforcement capabilities within a specialised agency. The MCMC's expertise in communications and multimedia could result in more effective enforcement. Lastly, proactivity could crystallise, allowing the MCMC to act swiftly in stopping cybercrimes before they escalate.

Arguments against conferring arrest authority to the MCMC include the inadequacy of checks and balances to prevent abuse of power, leading to oversight concerns. Some argue that it could result in infringements of freedom of speech and privacy. There are also doubts about whether the MCMC has the necessary resources and training for such powers. Balancing these arguments is crucial in deciding whether to grant such authority to the MCMC, highlighting the need to balance effective law enforcement with the protection of civil liberties.

Oversight mechanisms for bodies like the MCMC typically involve, firstly, a legislative review where it is necessary to regularly report to and be scrutinised by legislative bodies. Parliament or any other legislative bodies can make rules to prevent unwanted glitches in the day-to-day activities of the MCMC. The second oversight mechanism entails a judicial review by the courts, whereby the decisions and actions made by the MCMC are reviewed for legality and constitutionality. Thirdly, the existence of internal audits results in self-assessment procedures to ensure compliance with laws and regulations. Next, public transparency in releasing information to the public can foster accountability, supporting the legal concept of the right to information. Lastly, independent commissions can be of utmost importance, whereby external bodies are appointed to conduct investigations and evaluations of the MCMC's performance. These mechanisms are designed to ensure that the MCMC operates within its mandate and respects civil liberties while performing its duties.

Citizens can actively participate in MCMC oversight by making Public Consultations to engage in forums and discussions hosted by the MCMC, where all queries are answered transparently. Such a drive is similar to the ombudsman concept held in many countries to counter maladministration. In addition, there should be Feedback Mechanisms for the public to submit complaints or suggestions through official channels. These should be welcomed warmly because it is the public who go through the procedures set up by the MCMC, and hence they would know what is lacking in practice. Next, the formation of Advocacy Groups is significant because the public can join or support organisations that monitor the MCMC's activities. Meanwhile, through Media Engagement, journalism and social media can be used to raise awareness and hold the MCMC accountable for its actions. Last but not least, the pursuit of legal remedies is important in instances of overreach or rights infringement. This should be the last resort after all the other mentioned approaches have been exhausted. These actions can help ensure that the MCMC remains transparent and accountable to the public it serves.

Limitations of the Study

Despite its contributions, this study is subject to several limitations. First, the sample size was relatively small and purposive, comprising selected officers from the MCMC, RMPD, and the Ministry of Communications and Multimedia. While their perspectives are valuable, the findings may not comprehensively reflect the views of other stakeholders such as legal practitioners, civil society organisations, or members of the judiciary who may have different insights on the implications of arrest powers.

Second, interviews were conducted using online platforms and messaging tools such as Webex, WhatsApp, and phone calls. Although these methods were practical and ensured flexibility, they may have limited the depth of engagement and follow-up questioning due to time constraints, technical interruptions, or the lack of non-verbal cues in remote communication.

Third, the study relied primarily on self-reported data from government officials, which may be influenced by institutional loyalty or perceived expectations. This could lead to response bias, particularly when discussing the advantages or disadvantages of expanding enforcement powers within their own agencies.

Fourth, the thematic analysis conducted was based on a manual interpretation of interview transcripts, which may be influenced by the researchers' own perspectives or preconceptions. Although efforts were made to ensure objectivity through coding and verification, the potential for interpretive bias cannot be entirely ruled out.

Finally, the legal analysis was constrained by the limited availability of up-to-date case law or statutory amendments directly addressing the enforcement powers of non-police agencies in Malaysia. As cybercrime laws continue to evolve, the relevance of the findings may diminish over time without continual updates.

Conclusion

Having stated all the above points, the researchers are of the opinion that granting the power of arrest to the MCMC is essential for ensuring prompt action in tackling the challenges it encounters. Undeniably, it will involve considerable expenditure and time to set up the appropriate non-police team under the MCMC, but the conferment of such power to the commission is desirable and well-intentioned. It is high time that the MCMC be given the power of arrest so that it can reduce the burden on the police force in handling communication and multimedia-related cases, in addition to alleviating its status as one of the main agencies contributing to the well-being of Malaysia.

References

Ahmad Masum, M. H. A., & S. M. M. N. (2021). Covid-19 and freedom of movement: A case study of the Malaysian Federal Constitution. *Legal Network Series*, *1*, 1–17.

Ahmad, R., & Ismail, A. (2018). Personal data protection in Malaysia: The 2017 mobile phone data breach. *Malaysian Journal of Law and Society*, *12*(2), 76–89.

Ahmad, R., & Nordin, S. (2018). Administrative powers of MCMC: Examining licensing and sanctioning abilities under Malaysian law. *International Journal of Regulation and Governance*, *18*(1), 67–83.

Akhtar, Z. (2022). Montesquieu's theory of the separation of powers, legislative flexibility and judicial restraint in an unwritten constitution. *Amicus Curiae*, *4*(3), 552–577.

Alnifie, K. M., & Kim, C. (2023). Appraising the manifestation of optimism bias and its impact on human perception of cyber security: A meta-analysis. *Journal of Information Security*, *14*(2), 93–110.

Anwary, I. (2022). The role of public administration in combating cybercrime: An analysis of the legal framework in Indonesia. *International Journal of Cyber Criminology*, *16*(2), 216–227.

Australian Federal Police. (2024). *"Global sting sees Australian offenders arrested for cybercrime and phishing attacks"*. https://www.afp.gov.au/news-centre/media-release/global-sting-sees-australian-offenders-arrested-cybercrime-and-phishing

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Academic Press.

Barberis, M., & Sardo, A. (2024). The separation of powers: Old, new, and newest. In *Research handbook on legal evolution* (pp. 263–275). Edward Elgar Publishing.

Bidin, A., & Khan, S. (2022). *Compatibility analysis of Malaysian civil and Syariah laws to the International Covenant on Civil and Political Rights (ICCPR)*. Suhakam.

Bolívar, M. P. R., Galera, A. N., & Muñoz, L. A. (2015). Governance, transparency and accountability: An international comparison. *Journal of Policy Modeling*, *37*(1), 136–174.

Brady, H. E. (2019). The challenge of big data and data science. *Annual Review of Political Science*, *22*(1), 297–323.

Chetry, A., & Sharma, U. (2023). Anonymity in decentralized apps: Study of implications for cybercrime investigations. *International Journal of Experimental Research and Review*, *32*, 195–205.

Clifford, R. D. (2011). *Cybercrime: The investigation, prosecution and defense of a computer-related crime* (3rd ed.). Carolina Academic Press.

Cohen, G. (2018). Cultural fragmentation as a barrier to interagency collaboration: A qualitative examination of Texas law enforcement officers' perceptions. *The American Review of Public Administration*, *48*(8), 886–901.

Davis, J. T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies & Management*, *35*(2), 272–284.

De Hert, P. (2016). Accountability mechanisms for regulatory agencies with law enforcement powers: A legal analysis. *European Journal of Public Law*, *22*(1), 101–119.

Dube, D., & Bedi, S. (Eds.). (2021). *Arrest and detention in India: Law, procedure and practice*. SAGE Publishing India.

Dudley, S. E., & Wegrich, K. (2015). The role of transparency in regulatory governance: Comparing US and EU regulatory systems. *Journal of Risk Research*, *19*(9), 1141–1157.

European Parliament & Council of the European Union. (2018). *Regulation (EU) 2018/1240 of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624, and (EU) 2017/2226*. *Official Journal of the European Union*, *L 236*, 1–71.

Familoni, B. T. (2024). Cybersecurity challenges in the age of AI: Theoretical approaches and practical solutions. *Computer Science & IT Research Journal*, *5*(3), 703–724.

Fisher, R. P., Ross, S. J., & Cahill, B. S. (2017). Interviewing witnesses and victims. In *Forensic psychology in context* (pp. 56–74). Willan.

Fox, J. (2007). The uncertain relationship between transparency and accountability. *Development in Practice*, *17*(4–5), 663–671.

Fuad, K. T. (2020, May 9). *"Overview: On arrests (rights and restrictions)"*. LinkedIn. https://www.linkedin.com/pulse/overview-arrests-rights-restrictions-tiara-katrina-fuad/

Harmon, R. A. (2016). Why arrest. *Michigan Law Review*, *115*(30), 307–359.

Hashim, N. (2013). The need for a dynamic jurisprudence of right to "life" under Article 5(1) of the Federal Constitution. *Procedia - Social and Behavioral Sciences*, *101*, 299–306.

Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. *American Journal of Criminal Justice*, *46*(6), 837–842.

Henrina, J., Lim, M. A., & Pranata, R. (2021). COVID-19 and misinformation: How an infodemic fuelled the prominence of vitamin D. *British Journal of Nutrition*, *125*(3), 359–360.

Héritier, A., & Karremans, J. (2021). Introduction: Regulating finance in Europe: Policy effects and political accountability. In *Regulating finance in Europe* (pp. 1–15). Edward Elgar Publishing.

Islam, A. K. M. N., Laato, S., Talukder, M. S., & Sutinen, E. (2020). Misinformation sharing and social media fatigue during COVID-19: An affordance and cognitive load perspective. *Technological Forecasting and Social Change*, *159*, 1–14.

Kee, C. P., Nie, K. S., Korff, R., & Helbardt, S. (2015). Malaysia's contemporary broadcast media regulation through the eyes of regulators. *Journal of Asian Pacific Communication*, *25*(2), 231–242.

Kitsiou, A., Sideri, M., Pantelelis, M., Simou, S., Mavroeidi, A. G., Vgena, K., & Kalloniatis, C. (2024). Specification of self-adaptive privacy-related requirements within cloud computing environments (CCE). *Sensors*, *24*(10), 1–23.

Koziarski, J., & Lee, J. R. (2020). Connecting evidence-based policing and cybercrime. *Policing: An International Journal*, *43*(1), 198–211.

Mabillard, V. (2022). Trust in government: Assessing the impact of exposure to information in a local context. *International Journal of Public Administration*, *45*(9), 687–696.

MCMC. (2013). *"Annual report 2013"*. Malaysian Government Document Archives. https://govdocs.sinarproject.org/documents/ministry-of-science-technology-and-innovation/malaysia-communications-and-multimedia-commission-mcmc/mcmc-annual-repor2013_bm.pdf/view

Mohamad, A. R. B., Yaakop, M. R., & Razif, M. A. B. M. (2024). The efficacy of the Malaysian government's response towards cybercrime. *Open Journal of Political Science*, *14*(1), 166–176.

Mulgan, R. (2000). 'Accountability': An ever-expanding concept?. *Public Administration*, *78*(3), 555–573.

MyCERT. (2025, February 22). *"MyCERT advisory - SR-029.022025"*. Malaysian Computer Emergency Response Team. https://www.mycert.org.my/portal/advisory?id=SR-029.022025

Persadha, P. D., Waskita, A. A., & Yazid, S. (2015, October). Comparative study of cyber security policies among Malaysia, Australia, Indonesia: A responsibility perspective. In *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)* (pp. 146–150). IEEE.

Rahim, S. H. A., & Pawanteh, L. (2019). The role and challenges of the Malaysian Communications and Multimedia Commission in digital regulation. *Malaysian Journal of Communication*, *35*(4), 91–108.

Saripan, H., Hassan, R. A., Hashim, N., Salleh, A. S. M., Putera, N. S. F. M. S., & Nasrun, M. (2022). Unveiling the risks of corruption in the Malaysian telecommunication sector. *NeuroQuantology*, *20*(12), 1889–1902.

Shariff, S. Z. M., & Kosmin, R. (2015). Regulating content in broadcasting, media and the internet: A case study on public understanding of their role on self-regulation in Malaysia. *International Journal of Education and Social Science*, *2*(4), 58–69.

Shukurov, E., & Jafarov, U. U. (2023). Legal professionals' perspectives on the challenges of cybercrime legislation enforcement. *Interdisciplinary Studies in Society, Law, and Politics*, *2*(4), 25–31.

Sihabudin, S. (2023). Expanding the limitations of the protection and processing of children's personal data: An overview of current regulations, challenges, and recommendations. *Brawijaya Law Journal*, *10*(1), 59–71. https://doi.org/10.21776/ub.blj.2023.010.01.04

Sreedharam, R. K., & Ramayah, B. (2020). Sedition law and the bloggers' freedom of expression in Malaysia. *Malaysian Journal of Law & Society*, *26*, 85–96.

Stasavage, D. (2020). *The decline and rise of democracy: A global history from antiquity to today*. Princeton University Press.

Stechschulte, N. (2022, June 21). *"Can the SEC file criminal charges?"*. Stechschulte Nell Law. https://www.tpatrialattorneys.com/sec-criminal-charges/

Straits Times. (2017, October 31). *"Malaysia data breach puts personal details of 46.2 million mobile subscribers at stake"*. The Straits Times. https://www.straitstimes.com/asia/se-asia/malaysia-data-breach-puts-personal-details-of-462-million-mobile-subscribers-at-stake

Tregidga, H., Kearins, K., & Collins, E. (2019). Towards transparency? Analysing the sustainability governance practices of ethical certification. *Social and Environmental Accountability Journal*, *39*(1), 44–69.

Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). International enforcement of cryptocurrency laws: Jurisdictional challenges and collaborative solutions. *Magna Scientia Advanced Research and Reviews*, *11*(1), 68–83.

Zubaidi, N. H. A. (2021). Monitoring internet child pornography (ICP) in Malaysia. *Pertanika Journal of Social Sciences and Humanities*, *29*(2), 185–203.