INSTITUTIONAL ACTORS AND LEGISLATIVE DECISION-MAKING IN THE SECURITISATION OF CYBER THREATS IN MALAYSIA

Hanis Shaheera Ahmad Hisham, Sheila Devi Michael, Azah Anir Norman[*]

ABSTRACT

This study investigates the role of key actors in Malaysia in the securitisation of cyber threats at the national level, addressing a significant gap in existing research that often overlooks the human element in cybersecurity. Correspondingly, the research employs a qualitative approach, triangulating evidence from parliamentary debates, cybersecurity policy, and legislative documents. As such, the findings highlight the contested nature of Malaysia's legislative process, where the articulation of an issue by a credible actor can transform it into a matter of national concern, prompting governmental action. At the parliamentary level, the advancement of cybersecurity-related legislation is shaped by the authority, influence, and strategic intent of the actors involved, reflecting their capacity to influence the nation's policy trajectory. In essence, cyber threats pose substantial risks to national security, often serving as instruments of hybrid warfare and thereby challenging conventional notions of state sovereignty.

Keywords: Actors, Cyber Threats, Securitising, Policymaking, Malaysia

INTRODUCTION

Decision-making is an essential practice of a state's government. It extends beyond a mere debate between policymakers. Instead, it refers to an action aimed at deciding on various matters, maintaining sovereignty and security, and allocating public resources to achieve national interests (Peters & Pierre, 2016). In general, the process is complex. It depends on the decision-makers, or actors, to declare an object an existential threat requiring the state's attention. However, it takes an effective government to practice safe and secure governance.

This study examines the role of actors in decision-making by emphasising the significance of speech acts in shaping security issues. Within securitisation theory, an effective speech act integrates linguistic elements with societal context, reflecting both the intrinsic characteristics of language and the community that validates and acknowledges its expressions. Consequently, when an actor invokes the term "national security," it should not be romanticised, as such rhetoric often suppresses dissent and provides those in power with opportunities to exploit perceived "threats" for domestic agendas. Furthermore, this exploitation frequently justifies claims that address reduced democratic oversight and its limitations (Bourdieu, 1991; Buzan et al., 1998). In addition, the perlocutionary and illocutionary effects play pivotal roles in persuading audiences of the urgency of a threat, prompting decision-makers to prioritise the issue on their agenda and propose corresponding measures (Vuori, 2008). In the Malaysian context, these securitising dynamics are particularly evident during parliamentary sessions. In

[*] Hanis Shaheera Ahmad Hisham (hanis2924@yahoo.com) is the corresponding author. She is a PhD Candidate in the Department of International and Strategic Studies at the Faculty of Arts and Social Sciences, Universiti Malaya. Sheila Devi Michael (sheilamike@um.edu.my) is a Senior Lecturer in the Department of International and Strategic Studies at the Faculty of Arts and Social Sciences, Universiti Malaya. Azah Anir Norman (azahnorman@um.edu.my) is an associate professor in the Department of Information Systems, Faculty of Computer Science and Information Technology, Universiti Malaya.

particular, Malaysian political actors articulate cyber threats as security narratives through debate, justification, and persuasion to convince audiences of the need for policy interventions.

Cyber threats in Malaysia have become increasingly significant. For instance, Malaysia was ranked the eighth-most breached country in the third quarter of 2023 by the cybersecurity company Surfshark. Compared with the previous quarter, the breach rate has increased to 144%, placing Malaysia fifth in breach density. Following this, Kaspersky stated that Malaysia ranks second in Southeast Asia for mobile malware attacks in 2022 (PIKOM, 2024). Nonetheless, there is an urgent need to explore the role of actors in securing against cyber threats at the parliamentary level. Correspondingly, this study aims to explore the roles of Malaysian state actors in securitising cyber threats and the need to treat them as national security threats. Subsequently, two research questions arise: first, what are the prominent roles of Malaysian state actors in securitising cyber threats? Moreover, why does the Malaysian government need to treat cyber threats as a national security issue? Overall, this study seeks to investigate cybersecurity from a Malaysian perspective, which is crucial, given that cyberattacks frequently target the state and pose a serious threat due to cyberspace's borderless nature.

LITERATURE REVIEW

The Actors' Role in Political Activity

According to securitisation theory, an actor is defined as an individual who frames an issue as a threat to national security, thereby seeking validation to securitise it. The referent object is then invoked to justify extraordinary measures in response to the perceived threat. Despite this, the conceptualisation of actors remains theoretically underdeveloped, as it has been primarily understood as authoritative entities capable of performing speech acts, implicitly privileging political elites and state institutions (Buzan et al., 1998; Floyd, 2021; Lenz-Raymann, 2014). On a similar note, Floyd (2021) sought to address this limitation by introducing the concept of functional actors. She argued that none of the actors identified by Critical Studies (CS) fulfils roles that are not already addressed by other actors in the securitisation process. The entities identified by CS include:

a) Securitisation requesters
b) Securitising actors or executors of securitisation
c) Threateners

Floyd (2021) asserted that the actors with sector-specific roles shape the security environment. Notably, securitising acts are not always intended to initiate the securitisation process. Instead, they are often intended to enhance persuasion among influential actors. Accordingly, agencies of force may propose securitising acts to sell their products and address perceived threats arising from globalisation. In the cybersecurity sector, functional actors include cybersecurity professionals and organisations whose activities are directly linked to and significantly influence the quality of the environment (Buzan et al., 1998; Floyd, 2021). Compared with the national security concept, which privileges state sovereignty and is associated with military defence, securitisation theory expands the range of actors involved in cybersecurity governance beyond the state to include public- and private-sector stakeholders (Wolfers, 1952). This shift is evident in the way private-sector expertise shapes threat perception and policy responses. Constructivism, on the other hand, emphasises how identities and norms shape international relations. In line with this, securitisation theory directly explains cybersecurity governance by focusing on how cyber threats are politically framed and legitimised as national security issues that demand an urgent policy response (Wendt, 1999).

Researchers have long been drawn to political speech as a prominent area of language use. The study of political speech is critical due to its intricate nature as a human activity, which is significant to the structure and administration of society. As such, political language involves manipulating power to shape and control individuals' thoughts and beliefs, serving as a tool for governing society as a whole. Concurrently, political speech creates and upholds social connections, conveys emotions, and promotes concepts, policies, and political initiatives within a cultural framework. Speech Act Theory, a central topic in pragmatics, provides valuable insights into this phenomenon. In essence, speech acts are expressions or statements that depend heavily on the speaker's intention and the surrounding environment. Still, the effectiveness of political speech does not depend solely on the accuracy of its content. Rather, it lies in the skilful presentation of arguments. Additionally, a political speech functions as a written or spoken text, as an output, and as a process. Nonetheless, many politicians remain unaware of the correlation between speech, intention, and the resulting behaviours. Generally, the Speech Act Theory has proven to be a highly effective and suitable approach for analysing political speeches (Dylgjeri, 2017).

The decision-making process is crucial for distributing national resources, utilising them to meet demands, and enforcing them. Pettigrew (2014) stated that communication at the administrative level, where the interests of each party are voiced, eventually leads to decision-making. Elling (2012), on the other hand, characterised the decision-making process in terms of three factors: the objective (physical), the social (roles and norms), and the subjective (inner experience/internal factor). Combining these elements is referred to as the theory of modernity for national development. In Malaysia, the government operates within a constitutional monarchy and a democratic system, in which the parliament is the highest legislative body responsible for creating, amending, and approving laws, policies, and government spending. Historically, Malaysia's political system was viewed as practising a closed-door approach, in which high-level activities were conducted in secrecy and involved only select individuals. This lack of transparency led to breaches of parliamentary codes of conduct by members of parliament, exacerbated by the absence of appropriate guidelines. Such misconduct has often overshadowed the responsibilities of elected representatives. Nevertheless, in the 15th parliament, this approach shifted to a people-centric model, designed to foster a closer relationship between legislative bodies and the people they represent (Abdul Hai et al., 2024; Aslan, 2022).

Therefore, the securitisation of cyber threats is largely executive-centric. This is due to Malaysia's political system applying a more bureaucratically embedded form of securitisation. The primary securitising actors are located in the executive branches, particularly involving the Prime Minister, Members of Parliament, and the National Security Council (NSC). Operationally, the National Cyber Security Agency (NACSA), under the NSC and Cyber Security Malaysia, contributes to the securitisation of processes through threat assessment. The system demonstrates the epistemic authority necessary to frame cyber threats as risks to Malaysia's security. Conversely, the audience is primarily intra-executive rather than societal. The parliament and broader public function as secondary audiences, often receiving securitised narratives through legislative ratification or public communication rather than acting as decisive arbiters (Malaysian National Security Council, 2019, 2020; NACSA, 2024; Talib et al., 2023). Consequently, Malaysian cyber securitisation reflects routine, institutionalised governance practices rather than exceptional emergency politics, raising crucial questions about transparency and democratic oversight.

Despite the growing literature on cybersecurity governance, scholarly attention has focused primarily on how Malaysian parliamentary speech acts shape these processes. The existing studies focus on Malaysian cyber policy narratives and cybersecurity frameworks. At the same time, it overlooks the legislative arenas in Malaysian parliamentary deliberations

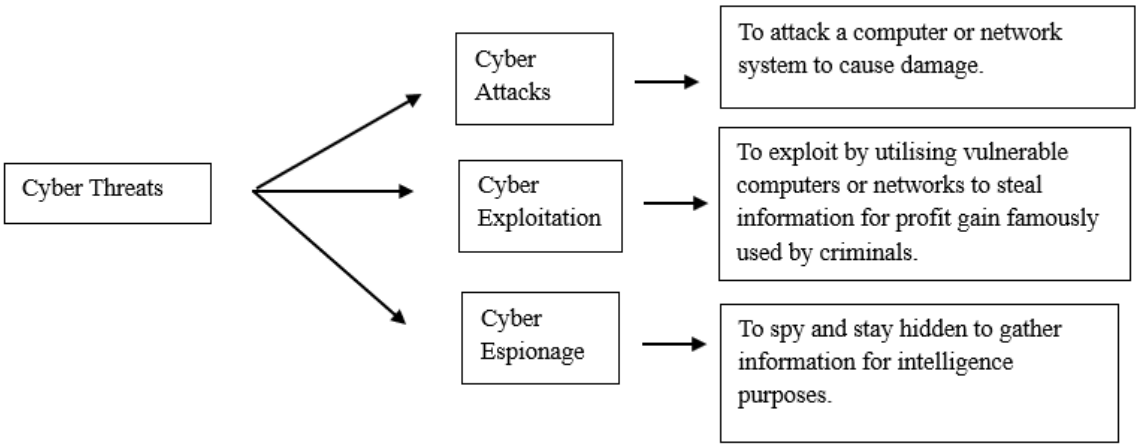
where security discourses are debated and legitimised. In a democratic system, parliaments serve as a critical platform for articulating, contesting, and institutionalising securitising moves through political speech acts (Floyd, 2021). Still, limited attention was paid to parliamentary speech acts in the securitisation of cyber threats within Malaysia's democratic framework, and to how such discourse contributes to the broader securitisation of cyberspace. Thus, existing studies rely on the parliamentary Hansard, which provides a valuable yet underutilised dataset for examining securitising speech acts. Consistent with this, applying discourse-oriented methods to these documents enables a better understanding of how Malaysian actors frame cyber threats.

The Emergence of Cyber Threats in Malaysia

The primary purpose of the internet is to provide connections across borders. Correspondingly, cyberspace has emerged as a significant concern in international relations, with the question of sovereign rights being a highly contested issue in international law. Several challenges arise in securing cyberspace: (1) Cyberspace is artificial; it does not have traditional borders, thus creating a blurred line between international and domestic borders; (2) The public and private sectors are vaguely divided, and it is impossible to separate them as both sectors are highly connected and dependent on cyberspace; (3) Distance and time are meaningless in cyberspace. Launching an attack is a conducive platform as it requires no time or distance; (4) There are no rules to control cyberspace. As Pande (2017) mentioned, cyberspace does not belong to anyone. Therefore, each state's laws and regulations may differ, and international law provides few regulations for cyberwar (Katin-Borland, 2016).

There are various types of cyber threats. However, this study focuses on three: cyberattacks, cyber exploits, and cyber espionage. Notably, Malaysia is experiencing these three cyber threats, raising policymakers' concerns. The three types of cyber threats are as follows:

Figure 1: Types of Cyber Threats



Source: *Author's compilation*

Figure 2 illustrates that cyber threats generally involve activities that inflict harm on the adversary, either by creating a significant effect or by remaining hidden to gather intelligence, and that they use cyberspace as a platform. These types of cyber threats may lead to various attacks, including cybercrime, cyberterrorism, and cyber warfare. Notably, all these threats are interlinked, meaning that cyber threats can simultaneously conduct a range of activities, including attacks, exploitation, and spying. Cyberattacks are mostly well coordinated. For example, Advanced Persistent Threats (APT) enable hackers to attack other computer

systems or networks using a variety of hybrid attack techniques. This event also has multiple attack vectors (Leszczyna, 2019).

Conversely, cyber exploitation is recognised as the manipulation of a specific weakness in a computer or network system to change the behaviour of the isolated system (Meena et al., 2021). The difference between cyberattacks and cyber exploitation is that cyberattacks aim to damage other computers or network systems. Specifically, cyber exploitation aims to gain unauthorised access to another computer to exert control over it. Meanwhile, snooping in cyberspace is referred to as cyber espionage. It entails gaining unauthorised access to computer systems, networks, and command-and-control systems to gather confidential or proprietary information or to change data. The distinction between cyber espionage and cyber war becomes hazier when a state's security apparatus (the defence ministry, intelligence agencies, and military forces) is targeted by electronic infiltration (Caldwell & Williams Jr, 2016).

Of greater concern is the interconnected nature of cyber threats, in which adversaries can integrate cyberattacks, exploitation, and spying into a single coordinated operation (Singer & Friedman, 2013). Most government agencies and critical infrastructure rely on legacy systems of outdated or unsupported hardware and software, making them vulnerable to cyber threats. Over time, these systems accumulate unpatched vulnerabilities and dormant malware, which pose a cyber threat and can be used as a strategic weapon to disrupt a state's critical infrastructure. Moreover, the growth of Internet of Things (IoT) devices exposes new weaknesses hourly. It can leverage these vulnerabilities to conduct large-scale distributed cyber operations. On a similar note, this expansion increases the strategic value of cyber threats since adversaries can infiltrate interconnected systems across multiple sectors simultaneously (Eggenschwiler & Silomon, 2018; Kolias et al., 2017; Robinson et al., 2015). For example, a North Korean state-sponsored cyber threat actor, the Lazarus Group, is known for conducting invasive cyberattacks, including hacking, financial heists, and espionage, and for executing high-impact campaigns. This, in turn, advances its strategic interests using cyber capabilities whilst exposing critical vulnerabilities in other countries, and is perilous (Perdana et al., 2024).

In 2023, Malaysia ranked eighth globally in terms of the most compromised network systems, with 494,699 compromised accounts. The country also ranked fifth in data breaches, averaging approximately 5,436 compromised accounts per day (Yeoh, 2023). The latest cyber threat data is available from private cybersecurity websites, which are more transparent and not bound by governments (OECD, 2021). Specifically, cyber incident reports are available on the Malaysian government website, providing a general overview without focusing on which public or private sector is affected (Cyber Security Malaysia, 2023). Notably, cyber threats have affected both the public and private sectors, including large firms with robust cybersecurity measures. Malware-as-a-Service (MaaS) and Ransomware-as-a-Service (RaaS) are the two most common types of cyberattacks in Malaysia. Accordingly, these attacks result from advances in cyber tactics, techniques, and procedures over time (Cyber Security Malaysia, 2023).

Above all, although private cybersecurity companies and media outlets increasingly report cyber threats in Malaysia, systematic academic studies examining the evolution and strategic implications of these threats, particularly in Malaysia, remain limited. Existing government reports often provide aggregated statistics with minimal analytical detail, while scholarly literature largely focuses on the operational level. As a result, there is limited understanding of how cyber threats are interpreted, framed, and addressed within Malaysia's institutional and political contexts. As such, this gap highlights the need for further research that analyses cyber threat developments in Malaysia.

RESEARCH METHODS

To achieve the study's results, qualitative methods were employed to answer the research questions. The primary purpose of this study is to explore the credibility of actors involved in the securitising process in Malaysia. Thus, the qualitative approach is appropriate for understanding how cyber threats are constructed, framed, and legitimised within policy discourse, rather than for quantitatively measuring causal relationships. This method utilised primary data comprising Dewan Rakyat Order Papers from 2019 to 2024. Following this, the dataset was compiled by identifying Hansard transcripts from the parliament related to cybersecurity. Simultaneously, secondary data were collected from various sources, including journal articles, books, and relevant websites. In particular, a triangulation strategy was applied to ensure the reliability of the data obtained. In this case, data triangulation was suitable, as it involved a variety of data sources obtained to fulfil the aims of this study (Carter et al., 2014; UNAIDS, 2010). The temporal period between 2019 and 2024 is applicable due to several reasons, including (1) the global shift in online activity due to COVID-19, (2) the Malaysian government introduced its first cybersecurity strategy, and (3) Malaysia is entering the digital transformation.

The identified research questions enable exploration of the literature through a narrative review (Green et al., 2006). The researcher divided two narrative reviews to explain the objectives of two themes: the role of actors and cyber threats. The primary purpose is to identify gaps in the literature and to develop a critical analysis that answers the research questions. Correspondingly, the inclusion criteria for this study are as follows: (1) a focus on Malaysian state actors involved in the decision-making process, (2) the use of parliamentary papers published by the Malaysian government, and (3) the examination of cyber threats, including cyberattacks, cyber exploits, and espionage incidents occurring in Malaysia. Conversely, the exclusion criteria are: (1) studies covering a period of more than six years and (2) studies that do not involve the roles of the private sector in decision-making.

To analyse the collected materials, this study uses qualitative discourse analysis. It aligns with the securitisation theory in exploring the functions of language and narrative through speech acts. Furthermore, it helps construct cyber threats as a security issue and legitimise policy responses through the parliamentary platform. The analytical procedure combines critical discourse analysis and thematic coding to examine the actors' textual data (Aranda et al., 2021; Fairclough, 2013). Subsequently, the coding process was conducted in several stages: (1) the researcher conducted an initial familiarisation with the collected documents based on inclusive and exclusive criteria. (2) The coding process is applied to label segments of text that reflect the research questions and elements of securitisation discourse through keywords such as "cyber threats" and "policymaking." (3) The initial codes were grouped into broader thematic categories to identify relationships between actors and their perspectives in delivering a security narrative in the parliament. Moreover, how actors articulate speech acts is determined by their credibility within the securitisation process, including the use of institutional authority, technical expertise, and strategic narratives. Through iterative comparison across documents, the researchers refined the coding categories to ensure consistency and conceptual clarity.

The coded themes were subsequently synthesised to develop an analytical framework to examine actors' speech acts based on three categories: (1) the actors involved in cybersecurity governance, (2) how actors framed cyber threats as a security concern, and (3) mechanisms of credibility and authority being constructed within policy discourse. The actors were identified based on official statements and parliamentary debate documents related to the Malaysian Member of Parliament. By integrating these components, the framework provides a

structured approach to analysing the legislative process by which actors in Malaysia secure against cyber threats.

FINDINGS

The Role of Malaysian State Actors in Securing Against Cyber Threats

Previous literature has established that the essence of legislative procedures lies in the Bill proposed by the actors. This is how governance works through legislation and influencing the government's decisions. Moreover, organised pressure could impact a state's national strategy. According to the Buchanan Committee, 'personal contact' is the primary approach, as the speaker claimed that *"the way to get bills through is to go up and grab the fellows and talk to them. A speech never changed a vote yet. It is a matter of political strategy. Take the leaders and sell them."* Therefore, "personal contact" is made through interviews, dinner events with legislators, special favours, or any prominent role in demanding that the legislative and administrative action (Dykstra, 1951). In this case, securitisation theory is demonstrated to be a means of successfully performing a speech act in political activity. Meanwhile, communication is used as a structural reform to achieve a broader spectrum of national interests (Stankova, 2019). Therefore, a coding matrix to observe speech act patterns among actors in securitising cyber threats is outlined below:

Table 2: Coding Matrix for Securitising Cybersecurity Discourse based on Dewan Rakyat Order Papers (2019-2024)

Coding theme	Indicator	Analytical description	Example of Parliamentary Order Papers	Securitisation level
Cyber threats	Cyber threats threaten national security	Cyber incidents are framed as threats to sovereignty, national stability, or state security.	Question on cyber threats that could threaten the country's sovereignty without proactive measures.	High
	Cybercrime	Cybercrime is presented as a growing systemic threat requiring government intervention.	Questions on the number of cybercrime cases and financial losses nationwide.	Medium
	Vulnerable in the public sector	Emphasis on cyberattacks targeting government databases or state institutions.	Inquiry into cyberattacks against government agencies and state government systems.	High
	Data breach and personal data exposure	Cybersecurity is framed around the leakage of citizens' personal data.	Concerns over Malaysia's ranking among countries with major data breaches.	Medium–High

Policymaking process	Cyber governance architecture	Discussion of national cyber strategy, agencies, and regulatory bodies.	Parliamentary questions on cyber policy development and governance reforms.	High
	Strategic technology integration	Cybersecurity integration into national digital transformation and 5G expansion.	Questions on cybersecurity planning in the 5G digital economy phase.	Medium–High

Source: *Author's compilation. Retrieved from The Official Portal of Parliament of Malaysia (n.d.)*

Table 2 indicates the coding matrix for securitising cybersecurity discourse, derived from the parliamentary speech acts recorded in the Dewan Rakyat Order Paper from 2019 to 2024. A detailed Dewan Rakyat Order Papers is available in the Appendix. Building on this, the coding matrix is created in line with securitisation theory to identify how actors framed cyber issues through threat narratives and the cyber policymaking process. The table covers six years to observe the pattern of securitisation of cyber threats in parliamentary discourse. 2019 was the year of a major shift in the use of IoT devices, driven by movement restrictions during the COVID-19 pandemic, which forced all physical activities online (Onyeaka et al., 2021). Notably, securitising cyberspace occurs when issues are discursively constructed as existential threats that demand political attention and an exceptional policy response (Buzan et al., 1998). In line with this, the Malaysian parliamentary discourse highlights the process of articulating cyber threats as matters of national security.

The coding category is divided into two: (1) cyber threats threaten national security, and (2) the policymaking process. The first coding category indicates a high level of securitisation, suggesting that cyber threats are consistently framed in terms of their impact on national security, sovereignty, and stability. In addition, it comprehends that the cybersecurity perspective has shifted from a technical concern to a strategic issue of state survival. According to securitisation theory, this change represents a traditional securitising move in which the actors raise an issue beyond routine governance and into the domain of security politics (Buzan et al., 1998). In a parliamentary context, it is expressed in language that emphasises the security of state sovereignty against cyber threats and calls for proactive measures.

The discourse also differentiates between varying levels of threat construction. While threats to national security and vulnerabilities in the public sector are coded as high-level securitisation, cybercrime is primarily coded as medium-level securitisation. The distinction reveals a crucial analytical pattern. That is, cybercrime is often treated as a matter of law enforcement rather than existential security, unless it is explicitly linked to national security or the state's critical infrastructure. By contrast, categories such as data breaches and personal data exposure occupy an intermediate position. Although these issues affect citizens, they are not considered a critical need for securitisation unless cyber threats lead to large-scale disruption. In essence, this variation underscores that parliamentary discourse does not cover all cyber-related issues equally. Rather, it depends on the perceived impact on national security.

The policymaking process, on the other hand, has indicated the institutionalisation of cybersecurity as a strategic policy domain, as evidenced by the cyber governance architecture. Once an issue is successfully framed as a security concern, it often leads to the development of governance structures that consolidate state authority and policy coordination in the domain. Parliamentary attention to governance architecture suggests that securitisation is not limited to constructing rhetorical threats. However, it also extends to the development of institutional mechanisms to contain cyber threats at the national level. Under the strategic technology

integration, the demonstrated cybersecurity discourse intersects with the national digital modernisation planning. Rather than focusing on defensive measures against cyber threats, the actors posit cybersecurity within the broader context of digital infrastructure development and technological competition. This implies that emerging technologies are not limited to their role in national development; they also pose potential sources of systemic vulnerability that require strategic oversight.

From an analytical perspective, the coding framework demonstrates an effective securitisation process, translating it into empirical indicators observable in the parliamentary Hansard. According to Searle (1969), *"speaking a language is performing speech acts,"* even with minimal or basic units of linguistics, is considered part of communication (Searle, 1969). Hence, the Malaysian Ministers' utterances are crucial to ensuring that the objective of securing against cyber threats is achieved. For example, Communications and Digital Minister Fahmi Fadzil delivered a speech on cybersecurity via Radio Televisyen Malaysia (RTM) platforms. His speech is as follows:

> Communications and Digital Minister Fahmi Fadzil said the responsibility for this change lies with the Chief Secretary, chief executive officers, and the highest echelons of ministries while citing cyber threats as a challenge and that the government must safeguard the security of ministries' data in light of evolving cyber risks.
>
> In addition, he said numerous modules within ministries' websites require enhancement or renewal, necessitating the formulation of a specific plan at the ministry level.
>
> "We are witnessing a rise in the ingenuity and sophistication of hackers' techniques and there is a growing concern that they might leverage artificial intelligence (AI) technology to breach, hack, and illicitly obtain our data.

Source: *Retrieved from Bernama (2023)*

The analysis of Dewan Rakyat Order Papers suggests that cybersecurity has increasingly been positioned within Malaysia's strategic policy agenda. Despite this, the success of the securitising move does not depend on actors' articulation of threats. Instead, it requires acceptance by the audience. Table 2, presented previously, summarises how actors framed cyber incidents as technical or regulatory challenges. Thus, parliamentary discussions increasingly adopted security-oriented language, portraying cyber threats as a national security risk. In general, this escalation of threat narratives reflects a discursive shift that legitimised an extraordinary response by the Malaysian government.

The acceptance of the threat narratives is reflected through government initiatives, most notably the implementation of the Malaysia Cyber Security Strategy (MCSS) 2020-2024. However, the limitations in the MCSS have led the government to strengthen it through the latest implementation of the Cyber Security Bill (Act 854) in 2024, aimed at enhancing Malaysian cyber resilience. At the same time, the securitisation process remains ongoing and contested. Similarly, parliamentary debates surrounding Act 854 indicate that several issues remain ambiguous, particularly related to regulatory authority, institutional responsibilities, and oversight mechanisms. Additionally, the Ministers claimed they would discuss the matter further to address it (Medina, 2024).

Overall, this study demonstrates the securitisation process within Malaysia's hybrid political regime. A strong executive authority and limited parliamentary contestation characterise it. Classical securitisation theory emphasises the role of speech acts and audience acceptance. Still, in Malaysia, a dynamic process of securitising highlights bureaucratic and institutional processes rather than overt political discourse. The findings nuance securitisation theory by highlighting how cyber threats are constructed within intra-executive policy networks, whose acceptance is largely due to the state rather than public mobilisation. This is due to Malaysia's political system, which practices semi-democratic institutions. Following this,

the securitisation process may differ across countries depending on their political systems (Balzacq, 2005; Brahim, 2014; Cavelty, 2007).

The Need to Secure Cyber Threats in Malaysia

The primary purpose of the cyberspace platform is to enable information to flow at high speed across a borderless world via a network of satellite links and undersea cables. Any physical form of area contradicts the characteristics of cyberspace. This is where it has posed a challenge to our national security. Note that the government's role is to provide security and maintain harmony among its people and the country. Accordingly, this section explains the need to secure cyberspace at the strategic level from two perspectives: internal and external factors.

The internal factors are identified in three ways: digital maturity, human error, and cyberspace influence. Malaysia is advancing towards digital maturity through government initiatives to introduce MyDigital and the Digital Economy Blueprint, part of a plan to improve and expand connectivity across cities and rural areas. These advantages support economic and social growth in Malaysia and increase trade and investment opportunities. Although previous studies reported that Malaysia experienced slow growth in digital maturity, Chandrakasan et al. (2023) they stated that Malaysian businesses are making positive progress in adapting to it. Nonetheless, the more connectivity is created, the more cyber threats will come in. Since most activities nowadays rely on technology, any disruption will affect the top-down governance in Malaysia (Chandrakasan et al., 2023; FMT, 2022).

Second, insider threats and human error account for most cyber threats. The reason for this is poor cyber hygiene. Scholars generally concur that people are the weakest link in cyberspace. Even with advanced network system technologies, human error is necessary for virus and worm infiltration. According to the Data Breach Investigation Report (DBIR), 83% of cyberattacks, including data breaches, are conducted by external actors. By contrast, human error accounted for was 74% of data breaches (Verizon, 2023). In addition, Kaur (2023) stated that 75% of Malaysian organisations fail to conduct regular risk assessments. This, in turn, impedes timely threat identification, and 48% of Malaysians feel unprepared for and unworthy of threats. The report also highlights that over 50% of businesses experience alert fatigue and oversee an average of 221 events per day (Kaur, 2023). Likewise, public neglect and lack of awareness of cyber threats may expose Malaysia to increased vulnerability.

Third, cyberspace itself serves as a platform for extremists to spread propaganda and ideological groupings. For example, the connectivity in cyberspace allows terrorist activities such as targeting youth for recruitment using social media, using Malaysia as a transit, and criminal activities for terrorist groups (Aslam, 2020; Ismail et al., 2022; US Department of State, n.d.). Therefore, the government is accountable for tackling complex, dynamic security threats, including physical and non-physical threats such as ideological threats to one's mind, which are still considered threats to national security (Malaysian National Security Council, 2019).

Next, the external factors are classified into three categories: evolving technology, the domino effect, and non-state and state-sponsored attacks. In the context of evolving technology, it is understood that technology is becoming increasingly sophisticated. Most critical infrastructure, such as transportation, energy, and health care, relies on networked systems with human interfaces to monitor and control processes. However, once a cyber attacker gains unauthorised access to the network's control systems, they can disrupt physical processes. According to NACSA, cyber threats are alarming and target Malaysia's domain and infrastructure, including government agencies and the private sector (Bashendy et al., 2023; NACSA, n.d.).

In addition, vulnerabilities in networks are widespread and can cause a domino effect. Its effects affect several countries, critical infrastructure, and the private sector within a country (Arief et al., 2020; Cyber Security Malaysia, 2023; Levy & Gafni, 2021). For instance, cyber threats such as Zero-day exploits, sophisticated viruses, and malware have sparked an arms race among criminal organisations and among countries seeking to gain cyber power (Maxwell, 2017; Menendez, 2021). Finally, cyber threats blur the lines between state and non-state actors. This led to greater asymmetry in cyberspace, where concealed system weaknesses were exploited and increasingly sophisticated attacks were developed. As a result, cyber threats serve as a tool for advancing geostrategic objectives in asymmetric warfare (Stafiniak & Wodo, 2022).

CONCLUSION

An object is not a threat unless the actors at the strategic level declare it so. The findings reveal that cyber threats are increasingly portrayed as strategic risks due to their potential to disrupt national security. The actors play crucial roles in enacting speech acts to convince the audience of the severity of cyber threats, thereby demanding extraordinary measures to contain them. Nevertheless, the analysis indicates that the securitisation of cyber threats in Malaysia occurred through institutional and policy mechanisms rather than through dramatic public speech acts. Furthermore, executive institutions such as the Members of Parliament and government cybersecurity agencies, including NACSA and NSC, translate threat narratives into strategic governance practices. This indicates that the cyber securitising process functions as a routine and bureaucratic process embedded within national security governance. Therefore, the Malaysian case of securitisation demonstrated that the construction of cyber threats may occur through technocratic and institutional processes rather than through purely public political discourse. In response, future research should examine the securitisation of cyberspace across Southeast Asia to understand how various political systems shape national responses to cyber threats.

REFERENCES

Abdul Hai, A. H., Tan, M. Z. S., & Jen, A. L. (2024). Conceptualising the People's Parliament Approach in the Parliament of Malaysia. *Journal of the Malaysian Parliament*, *4*, 1–24. https://doi.org/10.54313/journalmp.v4i.137

Aranda, A. M., Sele, K., Etchanchu, H., Guyt, J. Y., & Vaara, E. (2021). From Big Data to Rich Theory: Integrating Critical Discourse Analysis with Structural Topic Modeling. *European Management Review*, *18*(3), 197–214. https://doi.org/10.1111/emre.12452

Arief, R., Khakzad, N., & Pieters, W. (2020). Mitigating cyberattack related domino effects in process plants via ICS segmentation. *Journal of Information Security and Applications*, *51*, 102450. https://doi.org/10.1016/j.jisa.2020.102450

Aslam, M. M. M. (2020). Malaysian terrorist organizations and potential involvement in criminal activities. *Journal of Al-Tamaddun*, *15*(2), 15–28. https://doi.org/10.22452/JAT.vol15no2.2

Aslan, A. A. (2022). Conduct in the House of Representatives (Dewan Rakyat) Parliament

Malaysia. *Journal of the Malaysian Parliament*, *2*, 62–96. https://doi.org/10.54313/journalmp.v2i.56

Balzacq, T. (2005). The three faces of securitization: Political agency, audience and context. *European Journal of International Relations*, *11*(2), 171–201. https://doi.org/10.1177/1354066105052960

Bashendy, M., Tantawy, A., & Erradi, A. (2023). Intrusion response systems for cyber-physical systems: A comprehensive survey. *Computers and Security*, *124*, 102984. https://doi.org/10.1016/j.cose.2022.102984

Bernama. (2023). *Ministries need to appoint chief information security officer to combat data breaches: Fahmi*. New Straits Times.

Bourdieu, P. (1991). *Language and symbolic power*. Harvard University Press.

Brahim, M. (2014). *Peranan dan tanggungjawab wakil rakyat dalam sistem politik Malaysia*. Universiti Utara Malaysia.

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Caldwell, D., & Williams Jr, R. E. (2016). *Seeking security in an insecure world*. Bloomsbury Publishing USA.

Carter, N., Bryant-Lukosius, D., Dicenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, *41*(5), 545–547. https://doi.org/10.1188/14.ONF.545-547

Cavelty, M. D. (2007). *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.

Chandrakasan, C. P., Daud, P., Musa, O., Jidon, A. I. A., & Hanapiah, M. H. M. (2023). The impact of leadership, innovation, and organisation learning on the digital maturity of organisations in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, *13*(5), 1684–1706.

Cyber Security Malaysia. (2023). *Mid-Year Report: Threat Landscape 2023*. Cyber Security Malaysia.

Dykstra, D. J. (1951). The Impact of Pressure Groups on the Legislative Process. *Washington University Law Quarterly*, *1951*(3), 306–328.

Dylgjeri, A. (2017). Analysis of Speech Acts in Political Speeches. *European Journal of Social Sciences*, *2*(2), 19–26.

Eggenschwiler, J., & Silomon, J. (2018). Challenges and opportunities in cyber weapon norm construction. *Computer Fraud and Security*, *2018*(12), 11–18. https://doi.org/10.1016/S1361-3723(18)30120-9

Elling, B. (2012). *Rationality and the environment: Decision-making in environmental politics and assessment*. Routledge.

Fairclough, N. (2013). *Critical discourse analysis: The critical study of language*. Routledge.

Floyd, R. (2021). Securitisation and the function of functional actors. *Critical Studies on Security*, *9*(2), 81–97. https://doi.org/10.1080/21624887.2020.1827590

FMT. (2022). *Malaysia still behind in digital maturity*. FMT. https://www.freemalaysiatoday.com/category/business/local-business/2022/08/04/malaysia-still-behind-in-digital-maturity

Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: secrets of the trade. *Journal of Chiropractic Medicine*, *5*(3), 101–117. https://doi.org/10.1016/S0899-3467(07)60142-6

Ismail, N., Jawhar, J. M., Yusuf, D. M., Ismail, A. I., & Naguib, R. M. K. A. R. M. (2022). Understanding Malaysian Youth's Social Media Practices and Their Attitude towards Violent Extremism. *Intellectual Discourse*, *30*(1), 5–33. https://doi.org/10.31436/id.v30i1.1855

Katin-Borland, N. (2016). Cyberwar: A real and growing threat. In *Cyberspaces and Global Affairs* (pp. 3–22). Routledge.

Kaur, D. (2023). *Malaysia faces cyberthreat surge: phishing dominates, ransomware doubles*. TechWire Asia. https://techwireasia.com/2023/12/what-is-behind-the-worsening-state-of-cybersecurity-in-malaysia/#:~:text=doubling of ransomware incidents across the country

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80–84. https://doi.org/10.1109/MC.2017.201

Lenz-Raymann, K. (2014). *Securitization of Islam: A Vicious Circle; CounterTerrorism and Freedom of Religion in Central Asia*. Transcript Verlag.

Leszczyna, R. (2019). *Cybersecurity in the electricity sector: Managing Critical Infrastructure*. Springer.

Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. *Information and Computer Security*, *29*(5), 724–736. https://doi.org/10.1108/ICS-04-2020-0054

Malaysian National Security Council. (2019). *National Security Policy*. Malaysian National Security Council.

Malaysian National Security Council. (2020). *Malaysia Cyber Security Strategy 2020-2024*. Malaysian National Security Council.

Maxwell, P. (2017). Stockpiling zero-day exploits: The next international weapons taboo. *Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS 2017*, 237–243.

Medina, A. F. (2024). *Malaysia's Cyber Security Act 2024: What Businesses Need to Know*. ASEAN Briefing. https://www.aseanbriefing.com/news/malaysias-cyber-security-act-2024-what-businesses-need-to-know/

Meena, Y., Sankhla, M. S., Sonone, S. S., Parashar, A., Parihar, K., & Saini, K. (2021). Cyber Exploitation through Cybercrimes & Challenges. *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 1467–1472. https://doi.org/10.1109/ICAC3N53548.2021.9725493

Menendez, H. (2021). Malware: The never-ending arms race. *Open Journal of Cybersecurity*, *1*(1), 1–25.

MyCert. (n.d.). *Incident Statistics*. MyCert. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=a6b391c5-3445-44b8-8266-1d85a272e9af

NACSA. (n.d.). *National cyber coordination and command centre (NC4) alert and advisories*. NACSA. https://www.nacsa.gov.my/alert.php

NACSA. (2024). National Security Council's Directive No. 26. In *National Cyber Security Agency (NACSA)*. https://www.nacsa.gov.my/directive26.php

OECD. (2021). *Competition Issues concerning News Media and Digital Platforms*. OECD.

Onyeaka, H., Anumudu, C. K., Al-Sharify, Z. T., Egele-Godswill, E., & Mbaegbu, P. (2021). COVID-19 pandemic: A review of the global lockdown and its far-reaching effects. *Science Progress*, *104*(2), 1–18. https://doi.org/10.1177/00368504211019854

Pande, J. (2017). *Introduction to cyber security*. Uttarakhand Open University.

Perdana, A., Aminanto, M. E., & Anggorojati, B. (2024). Hack, heist, and havoc: The Lazarus Group's triple threat to global cybersecurity. *Journal of Information Technology Teaching Cases*, 1–12. https://doi.org/10.1177/20438869241303941

Peters, B. G., & Pierre, J. (2016). *Comparative governance: Rediscovering the functional dimension of governing*. Cambridge University Press.

Pettigrew, A. M. (2014). *The politics of organizational decision-making*. Routledge.

PIKOM. (2024). *Growing Threat Cybersecurity Landscape in Malaysia 2024*. PIKOM.

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, *49*, 70–94.

Searle, J. R. (1969). *Speech acts: An essay in the philosophy of language*. Cambridge University Press.

Singer, P. W., & Friedman, A. (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press.

Stafiniak, M., & Wodo, W. (2022). State-sponsored Cybersecurity Attacks. *2022 63rd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, 1–6. https://doi.org/10.1109/ITMS56974.2022.9937131

Stankova, M. O. I. (2019). *Frontiers of economic policy communications*. International Monetary Fund.

Talib, S., Abdul Munir, R., Abdul Molok, N. N., & Ahmad, M. R. (2023). Information Security Governance Issues in Malaysian Government Sector. *Journal of Information Systems and Digital Technologies*, *5*(2), 1–18. https://doi.org/10.31436/jisdt.v5i2.404

The Official Portal of Parliament of Malaysia. (n.d.). *Dewan Rakyat Order Paper*. The Official Portal of Parliament of Malaysia.

UNAIDS. (2010). *An Introduction to Triangulation*. UNAIDS. http://www.unaids.org/en/media/unaids/contentassets/documents/document/2010/10_4-Intro-to-triangulation-MEF.pdf

US Department of State. (n.d.). *Country Reports on Terrorism 2019: Malaysia*. US Department of State.

Verizon. (2023). *2023 Data Breach Investigations Report*. Verizon. https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

Vuori, J. A. (2008). Illocutionary logic and strands of securitization: Applying the theory of securitization to the study of non-democratic political orders. *European Journal of International Relations*, *14*(1), 65–99. https://doi.org/10.1177/1354066107087767

Wendt, A. (1999). *Social theory of international politics*. Cambridge University Press.

Wolfers, A. (1952). " National security" as an ambiguous symbol. *Political Science Quarterly*, *67*(4), 481–502.

Yeoh, A. (2023). *Cybersecurity report ranks Malaysia as eighth most breached country in Q3 2023*. The Star. https://www.thestar.com.my/tech/tech-news/2023/12/06/cybersecurity-report-ranks-malaysia-as-eighth-most-breached-country-in-q3-2023

APPENDIX

Table 2: Dewan Rakyat Order Papers (2019-2024)

No	Year	Speech Acts (Cyber Threats Threatening National Security)	Representative Speaker (Actor)
1.	3/4/2019	To ask the PRIME MINISTER to state the Ministry's efforts to curb cyber threats that can threaten the country's sovereignty if no proactive measures are taken.	Kelantan

No	Year	Speech Acts (Cyber Threats Threatening National Security)	Representative Speaker (Actor)
2.	20/11/2019	To ask the MINISTER OF COMMUNICATIONS AND MULTIMEDIA to state the number of cybercrime cases and the amount of losses recorded from January 1, 2018, until now in Sarawak, and the measures taken by the Ministry to address cybercrimes.	Sarawak
3.	13/7/2020	To ask the PRIME MINISTER to state the preparation and action taken by the Ministry in addressing and strengthening the country's cybersecurity at the individual level, following the recent increase in hacking cases to 80.5% during the MCO, as reported by Cyber Security Malaysia in the Berita Harian dated May 26 2020.	Kuala Lumpur
4.	27/7/2020	To ask the MINISTER OF COMMUNICATIONS AND MULTIMEDIA to state the data and statistics on cyber fraud cases during the enforcement period of the Movement Control Order (MCO).	Johor
		To ask the MINISTER OF COMMUNICATIONS AND MULTIMEDIA to state the government's cyber plans, especially in dealing with fake News that affects the relationship of multiracial and multi-religious communities in our country, and the steps taken to overcome it.	Johor
5.	4/11/2020	To ask the PRIME MINISTER to state the strategies adopted by the Ministry to strengthen international cooperation to protect the country's cyberspace, as there have been reports of attempted cyberattacks on several Government agencies.	Pahang
		To ask the PRIME MINISTER to state the Ministry's plan in ensuring protection from cyberattacks from inside and outside, and to ensure that it will not threaten the security of our country's digital infrastructure at this time.	Terengganu
6.	8/12/2021	To ask the PRIME MINISTER to state: (a) The Ministry's long-term plan in facing the threat of cyberattacks; and (b) the way for the Ministry to ensure that the people are always prepared to face the cyber threats and attacks that are becoming more prevalent despite the rapid pace of technology.	Perak
7.	1/3/2022	To ask the PRIME MINISTER to state : (a) The different types and number of cybercrimes reported and total losses for the past 2 years; and (b) Steps by the National Cyber Security Agency to address the rise in cybercrimes.	Selangor

No	Year	Speech Acts (Cyber Threats Threatening National Security)	Representative Speaker (Actor)
8.	7/3/2022	To ask the MINISTER OF COMMUNICATIONS AND MULTIMEDIA to state the Ministry's efforts in preventing cyber threats and attacks on the digital economy platform, as well as the long-term action planned upon entering the 5G phase, as the cyber threats are becoming increasingly complex.	Sabah
9.	18/7/2022	To ask the MINISTER OF COMMUNICATIONS AND DIGITAL to state that Internet outages in rural areas occur due to vandalism activity that damages the fibre optic cables or steals the generator sets. The Ministry can overcome the problem by focusing on developing a comprehensive communication infrastructure, including providing Internet coverage for fixed and mobile lines.	Kedah
10.	26/7/2022	To ask the MINISTER OF COMMUNICATIONS AND DIGITAL to state the Ministry's plan to improve the broadband network in the rural areas of the Sabah Region. Several problems have been identified, including very slow broadband access, difficulty obtaining broadband signals in non-hotspot areas, and loss of broadband signals when the electricity supply is cut off.	Sabah
11.	20/2/2023	To ask the PRIME MINISTER to state the cybersecurity issues in Malaysia, such as internet fraud, phishing, and ransomware, and the measures that can be taken to increase the talent pool at the National Cyber Security Agency Malaysia.	Sarawak
12.	5/3/2024	To ask the MINISTER OF ECONOMY to state the latest statistics of registration of the Main Database System (PADU) by state and the specific measures that have been taken regarding the security aspects of the system (PADU), including the proposed implementation of security audits periodically, taking into account the risk of cyber threats and the emergence of new technologies.	Kedah
13.	7/3/2024	To ask the MINISTER OF DIGITAL to state the Ministry's control measures to contain and control the leakage of personal data on the internet, considering that Malaysia is ranked 11th in the country with the most user data breached according to a cybersecurity company, Surfshark, and the leakage of personal data in open-source done by the public themselves.	Johor
14.	13/3/2024	To ask the MINISTER OF DIGITAL to state the Ministry's new approach to dealing with cyber	Kelantan

No	Year	Speech Acts (Cyber Threats Threatening National Security)	Representative Speaker (Actor)
		threats that are becoming more complex every day, including identifying the cyber inequality gap, as well as the emergence of rapid technology such as AI, being one of the main cybersecurity risks next year, according to the World Economic Forum (WEF).	
15.	19/3/2024	To ask the MINISTER MINISTRY OF COMMUNICATIONS to state the specific measures that can be taken to address the issue of theft and vandalism to telecommunications towers in rural areas that affect the mobile network and internet access coverage in the areas involved.	Sarawak
16.		To ask the MINISTER OF DIGITAL to state the extent of the Ministry's action in creating a safe, reliable, and resilient cyber environment, as well as in curbing intrusion into Government databases and leakage of public information by irresponsible parties.	Johor
17.	24/6/2024	To ask the PRIME MINISTER to state comprehensively the cyberattacks that have occurred to Government agencies, including the Perlis State Government. The measures taken to prevent such attacks from recurring.	Perlis
18.	16/7/2024	To ask the PRIME MINISTER to state: (a) The number of cyberattacks on government databases from 2014 to 2024; and (b) the annual cost and readiness of the government's cybersecurity infrastructure (including agencies and departments) in tackling cyberattacks such as the one that happened in Indonesia recently.	Selangor
19.	28/10/2021	To ask the PRIME MINISTER to state when the Cyber Security Act or Bill will be tabled in parliament so that the country can defend, preserve, and launch a counterattack (Defence, Protect, and Attack) against elements that threaten the security of the country, institutions, and society.	Selangor
20.	23/2/2023	To ask the PRIME MINISTER to state the development of the proposal to establish the Cyber Security Commission.	Selangor
		To ask the MINISTER OF COMMUNICATIONS AND DIGITAL to state the development of negotiations with the telecommunication service provider, Telegram, to curb cybersecurity crimes, pornography, and the sale of prohibited goods.	Melaka
21.	27/2/2024	To ask the MINISTER MINISTRY OF COMMUNICATIONS to state the efforts to curb	Sarawak

No	Year	Speech Acts (Cyber Threats Threatening National Security)	Representative Speaker (Actor)
		the spread of false information and disinformation on social media that is on the rise.	
		To ask the MINISTER OF DIGITAL to state the Ministry's plan for enhancing the digital economy and absorbing the 5G technology, including cybersecurity, into the government sector, private sector, and society in general as quickly as possible. What are the costs involved? Whether MCMC is placed under the Ministry of Digital to facilitate all digital implementations.	Penang
22.	29/2/2024	To ask the MINISTER OF HOME AFFAIRS to state whether the Ministry has any intention to offer citizenship to foreign nationals with high expertise in strategic fields to help speed up the national transformation process and to be more orderly, such as in drone technology and cybersecurity.	Selangor
23.	25/3/2024	To ask the MINISTER OF DIGITAL to state the effectiveness of the steps taken to deal with cybersecurity threats such as ransomware attacks, cyber espionage attempts, data leaks, and cyber scams.	Kuala Lumpur
24.	27/6/2024	To ask the PRIME MINISTER to state when the Cyber Security Bill 2024, which was presented and passed in parliament at the last meeting, will be fully enforced, to assure the people that the cyber environment in this country is completely safe from any form of cyberattack.	Kelantan

Source: *Author's compilation. Retrieved from* The Official Portal of Parliament of Malaysia (n.d.)