Project GAIA

Open-Source

Global Conflict Analysis Report

February 2024

In focus this issue:

Malaysia's Cyber Threat Assessment

Project GAIA is a student-led project facilitated through the Cyber Analytics and Security Research group (CASR).

The open-source analysis in this publication is produced by our student analysts. The research is nonpartisan and non-proprietary. CASR, Carleton University and our guest speakers do not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in Project GAIA's publications should be understood to be solely those of the author(s).

This document is publicly available at ccasr.ca. Not intended for commercial use.

Cover page image: City Lights Skyline royalty-free stock illustration by Brigitte Werner. Free for use under the Pixabay Content License.

Project GAIA

Open-Source
Global Conflict Analysis Report
(February 2024):

Malaysia's Cyber Threat Assessment

This page is intentionally left blank.

Table of Contents

Case Studies

Case 1: Malaysian Government Surveillance

Case 2: DragonForce Malaysia

Assessments

Project GAIA Update in February 2024

This report is constructed to serve as a foundational template for subsequent student-led projects, illustrating a rigorous approach to cyber offensive capability assessments. Drawing upon influential models such as the National Cyber Security Index, Belfor Center Cyber Power Index, and insights from the Council on Foreign Relations, we have identified 12 critical capability categories for a comprehensive assessment framework.

We chose Malaysia for this report because it was ranked as one of the most targeted countries by cyber attacks in 2023. Given its strategic geopolitical position, we believe that studying Malaysia could provide valuable insights for Canada's Indo-Pacific strategy. We aim to use Malaysia as a baseline for our threat assessment template, reasoning that while it may not be as complex as some of the major cyber powers, as an evolving cyber power, Malaysia presents intriguing emerging capabilities and regional impacts.

We apply the MITRE ATT&CK framework as an exercise to dissect two contrasting case studies: the cyber surveillance initiatives of the Malaysian government and the activities of a prominent Malaysian hacker group, DragonForce Malaysia. The selection of these case studies aims to encapsulate a spectrum of threat dynamics, from state-level cyber capabilities to the impact of asymmetric cyber actors. And we produce strategic recommendations for Canadian cybersecurity posture enhancement, aligned with CISA’s Guide to Conducting Cybersecurity Risk Assessments.

On other note, as we continue with GAIA:ISDA task unit, focusing on Insider Threat Assessment in Critical Infrastructure, we anticipate to present our findings on the OSINT conference on March 27th. This will be a major milestone for our student group to showcase the findings of our open-source education, methodology, and production initiatives. Thank you for the support for our first academic year, and I invite you to stay tuned for our presentation.

ori navoiy

Project Manager, Team GAIA

(GAIA:EXCC\C01)

This page is intentionally left blank.

Key Event Highlights

November 17, 2023 | Source: Business Today

Malaysia Partners with BlackBerry to Bolster National Cybersecurity, Establishing Center of Excellence in Kuala Lumpur

At the APEC Summit, Malaysia and BlackBerry Limited announced a significant long-term cybersecurity agreement aimed at enhancing Malaysia's cybersecurity framework. This deal grants the Malaysian Government access to BlackBerry's comprehensive cybersecurity solutions, including AI-powered attack prediction and prevention, secure communication tools, data protection for roaming workforces, and incident response capabilities. Additionally, a Cybersecurity Center of Excellence will be established in Kuala Lumpur by 2024, focusing on training to address Malaysia's need for cybersecurity professionals. This collaboration is part of Canada's Indo-Pacific Strategy, emphasizing international cooperation in cybersecurity to strengthen regional security and resilience against cyber threats.

December 6, 2023 | Source: The Star

Malaysia Ranked 8th Most Breached Country in Q3 2023 Cybersecurity Report

In Q3 2023, a cybersecurity report by Surfshark identified Malaysia as the eighth most breached country globally, with 494,699 leaked accounts. The report, covering data breaches between July and September across over 200 countries, noted a 144% increase in breach rates for Malaysia compared to Q2 2023. With an average of approximately 5,436 Malaysian accounts compromised daily, the country also ranked fifth in breach density, a measure of the likelihood of experiencing a data breach relative to population size. The study, drawing from 29,000 public databases, aims to heighten awareness of cybersecurity risks and encourages enhanced security measures, including two-factor authentication, to mitigate potential threats.

Risk Assessment Matrix

The analytical confidence and levels of concern assessments presented in this report are based on a foundational matrix, in line with the pedagogical objectives of Project GAIA. It's important to note that the chosen matrix is designed to be illustrative rather than exhaustive or deeply quantitative. Broadly, our assessment framework draws inspiration from the operational risk model developed by the Economist Intelligence Unit and the Capability Assessment Methodology utilized by Jane's.

Analytical confidence	Levels of concern: LOW — fairly stable	MODERATE — potentially widespread challenges domestically	ELEVATED — poses severe challenges domestically and maybe internationally	HIGH — poses severe challenges internationally
CERTAINLY >90%				
LIKELY 60%-90%				
PROBABLY 40%-60%				
UNLIKELY 10%-40%				
RARE <10%				

Executive Summary

Malaysia's cyber threat profile

The report evaluates Malaysia's cyber capabilities, threat entities, and the implications of its cyber activities. It finds Malaysia to **unlikely** pose as cyber threat to Canada and the global community, highlighting Malaysia's commitment to defensive cyber operations and international cooperation. Despite access to sophisticated tools and a focus on cyber intelligence, Malaysia shows restraint in offensive operations and prioritizes cybersecurity within its digital transformation, especially in cloud security and leveraging AI for defense.

	2020-2021		2023-2024		
Risk	Level of concern	Analytical confidence	Level of concern	Analytical confidence	Trend
Offensive Capability	Moderate	Unlikely	Moderate	Unlikely	⇔
Defensive Capability	Moderate	Probable	Elevated	Probable	↗
Cyber Infrastructure	Moderate	Probable	Elevated	Likely	↗
Asymmetric Threats	Moderate	Unlikely	Moderate	Unlikely	⇔
External Threats	Elevated	Probable	Elevated	Probable	⇔

Malaysia's current cyber capabilities and strategic orientation present a **low to moderate** level of concern, with no significant evidence suggesting intentions to conduct offensive cyber operations against foreign entities, including Canadian interests. The proactive cyber defense measures, commitment to international cooperation, and investments in human capital and technological infrastructure contribute to a relatively stable domestic cybersecurity environment.

It is **probable** that the government's use of surveillance technology, as examined in the Project Magnum case, may pose moderate challenges domestically due to potential privacy and civil liberties implications. However, there's likely a low level of concern that these actions would provoke international disputes or severe challenges.

In the case of DragonForce Malaysia, while the group displays the capability for politically motivated cyber activities, the concern remains moderate domestically, as it's **unlikely** these actions would have significant immediate international repercussions or severe consequences.

The threats of politically motivated attacks from asymmetric powers like hacktivist groups may pose a **low to moderate** level of concern for Canadian interests, where it is **unlikely to rare** to expect such activities to result in high impact disruptions or severe international challenges.

Overall, the report recommends that Canada maintain a likely level of engagement and support to mitigate the moderate risks identified, reinforcing the stability of Malaysia's cybersecurity landscape and protecting against shared threats.

Capability Indicators

Based on latest data as of: March 5, 2024

Capability Overview

It's **very unlikely** that Malaysia poses a significant cyber threat to Canada and the global cybersecurity environment. While there's a notable investment in cyber capability development, the focus primarily leans towards defensive measures and infrastructure protection. Despite possessing tools for cyber intelligence gathering, Malaysia demonstrates restraint in offensive cyber operations conducted toward targets outside of its border. Its strategic partnerships, notably with the US, bolster its position in the digital economy and cybersecurity, suggests a potential that Malaysia's capabilities could be leveraged defensively within alliances. Underpinned by a strong legal and ethical framework and a commitment to international cooperation, Malaysia’s strategy underscores a balanced approach between leveraging digital transformation for economic growth and ensuring cyber resilience, without aggressively pursuing offensive cyber capabilities.

1. Technical Skills and Capabilities

Key Indicators:

The level of sophistication in software development, encryption, intrusion methods, and malware creation. This includes the ability to exploit zero-day vulnerabilities (previously unknown software vulnerabilities).

Malaysia prioritizes cybersecurity integration into its digital transformation, focusing on cloud security and leveraging Generative AI for defense.[1] Challenges persist, including slow security progress, digital upskilling needs, and addressing cloud risks.[2] Despite these, Malaysia cautiously advances its cybersecurity infrastructure and capabilities.

Investments in cybersecurity align with Malaysia's information and communications technology (ICT) market strategy, aiming for a robust digital economy amidst accelerated digitalization due to the pandemic. Cybersecurity is pivotal, with investments in sectors like Aerospace & Defense for advanced skills and threat intelligence.[3] Emphasis lies on enhancing defense capabilities, digital ecosystem visibility, and fostering international partnerships, strategically managing increased cyber threats.

Based on a 2015 leak,[4] the Malaysian government allegedly purchased sophisticated spyware, including tools like the Da Vinci remote control system.[5] While the capabilities include tracking, eavesdropping, and device access,[6] it doesn't necessarily indicate advanced indigenous software development. Questions arise regarding the intent and application of such tools within Malaysia's cyber strategy, suggesting ongoing development of complex indigenous capabilities alongside access to sophisticated tools.

2. Cyber Intelligence Gathering

Key Indicators:

Capabilities for reconnaissance and espionage, including the ability to infiltrate networks, exfiltrate sensitive information, and conduct surveillance operations without detection.

Malaysia's procurement of spyware tools as mentioned previously lays a foundation for its digital surveillance and cyber intelligence gathering capabilities. However, the fast-evolving cyber landscape means these past actions may not fully reflect Malaysia's current cyber capabilities or intentions. The National Cyber Security Strategy (MCSS) 2020-2024[7] underscores Malaysia's dedication to enhancing national cybersecurity, blending defensive measures with potential offensive cyber capabilities. This evolving strategy suggests an ambition for sophisticated cyber operations, emphasizing the development of a robust cyber ecosystem, advanced threat intelligence, and international collaboration to strengthen capabilities.

Malaysia's consistent investment in cybersecurity and strategic emphasis on active defense mechanisms indicate an ongoing effort to equip itself for both protecting against and potentially executing advanced cyber intelligence operations.[8] This includes capabilities for network infiltration, data exfiltration, and undetected surveillance, supported by a legal and policy framework in tune with global standards.[9] Therefore, Malaysia's approach to cyber operations appears to be moving towards a more intricate, well-regulated, and potentially cooperative framework, aiming to fulfill both defensive and offensive roles responsibly on the international stage.

3. Resources and Funding

Key Indicators:

Investment in cyber operations, including the budget allocated to cyber offensive units, cyber research and development, and acquisition of advanced cyber tools and technologies.

Malaysia has launched initiatives like the Global Accredited Cybersecurity Education (ACE) Certification Scheme to standardize professional qualifications, alongside the MCSS 2020-2024 with a RM1.8 billion investment[10] for strengthening the cyber framework through five strategic pillars,[11] including legal enhancements and international cooperation. Supporting the digital shift, the government also offers financial aids like the Smart Automation Grant (SAG) with RM150 million funding under PENJANA to aid SMEs in digitalization.

Malaysia also plans to increase its R&D expenditure to 2.5% of GDP by 2025, aiming for 3.5% by 2030, guided by the NPSTI 2021-2030. This goal relies on fostering collaborations across sectors, with significant R&D funding expected from external sources, demonstrating a commitment to a collaborative funding model. The approval of 99 R&D projects worth RM5.6 billion and the establishment of a Research Management Unit (RMU) underscore efforts to ensure quality and commercial viability in R&D, positioning Malaysia as a formidable player in the global digital economy.[12]

4. Human Capital

Key Indicators:

The number and quality of cybersecurity professionals and hackers employed or sponsored by the government, including training programs to enhance these skills.

In Malaysia, the focus on collaboration, training, and education in cybersecurity reflects a strategic approach to bolstering the nation's cyber resilience. The Malaysian Communications and Multimedia Commission (MCMC)[13] plays a pivotal role in fostering partnerships across various sectors, including academia, industry, and government, to develop a skilled cybersecurity workforce. These collaborative efforts are crucial for advancing cybersecurity knowledge and practices, ensuring Malaysia's digital infrastructure is safeguarded against cyber threats.

The integration of industry-led courses and specialized training programs, facilitated by collaborations between MCMC, universities, and technical institutions, exemplifies Malaysia's commitment to enhancing its human capital in cybersecurity. For instance, initiatives like the Masterclass in Converged Telecommunications Policy and Regulations program, developed in partnership with Multimedia University and the GSMA, highlight the demand for tailored education that meets industry needs. Furthermore, the government's substantial investment in upskilling, with RM750 million allocated for technology-related training, underscores the importance of continuous learning and development in the cybersecurity domain. Such educational and training initiatives are not just about imparting technical skills; they aim to cultivate a holistic understanding of cybersecurity challenges and solutions.

5. Cyber Military and Governmental Units

Key Indicators:

The existence of dedicated military and governmental cyber units or agencies tasked with conducting offensive cyber operations, such as the United States Cyber Command (USCYBERCOM) or Russia's GRU.

The National Cyber Security Agency (NACSA) was officially established in February 2017 with the primary objective of fortifying the nation's resilience against cyber-attacks.[14] NACSA is dedicated to formulating and implementing national-level cybersecurity policies and strategies while safeguarding Critical National Information Infrastructures (CNII).[15]

The Malaysian Armed Forces (MAF) under the Minister of Defence (MINDEF) recently established the Defence Cyber and Electromagnetic Division (BESP) in 2020, marking a significant milestone in bolstering national security capabilities.[16] This division was formed to enhance readiness and resilience against emerging threats in the cyber and electromagnetic domains. The BESP oversees all cyber and electromagnetic activities within the MAF, contributing to the defense against potential cyber-attacks and electromagnetic interference.[17] While the specific roles and mandates of the BESP are not explicitly defined, it is presumed that the division engages in a range of activities, including cyber operations, electronic warfare, and military intelligence, to safeguard Malaysia's interests in these critical domains.

The Royal Malaysian Police is at the forefront of tackling cybercrime and corporate cyber activities. Serving as Malaysia's primary law enforcement agency, it supervises the Cybercrime Investigation Department, which is committed to addressing a wide range of white-collar crimes.[18] From fraud and breach of trust to cyber-related offenses such as ransomware, this department investigates, apprehends, and prosecutes offenders.[19] Within its ranks, the specialized Cyber & Multimedia Crime Investigation unit. Moreover, the RMP includes the special branch the government supreme secretive intelligence branch.[20]

6. Publicly Known Cyber Operations and Attacks

Key Indicators:

Past and present cyber operations attributed to or acknowledged by a country. These can indicate not only capability but also the willingness to use cyber means to pursue national objectives.

Due to its expanding digital infrastructure, growing reliance on technology, and strategic position in Southeast Asia, Malaysia has become a frequent target of cyber-attacks.[21] Malaysia has experienced more cyberattacks than any other country in the Asia-Pacific (APAC), specifically in the private sector. According to a survey conducted among 100 organizations, 76% reported experiencing a cyberattack, nearly double the rate reported by Hong Kong, which recorded the lowest incidence at 43%.[22] These incidents include data loss, ransom payments, theft of intellectual property and more. Additionally, there have been numerous reports of state-sponsored attacks targeting various sectors within Malaysia, including government institutions and user data:

- In 2023, MuddyWater orchestrated a phishing campaign targeting prominent government, aviation, banking, energy, and telecommunications entities across the Middle East and North Africa, believed to have started in July 2021 and allegedly sponsored by Iran.[23]

- In 2022, APT 40 conducted an espionage campaign targeting organizations involved in wind turbine maintenance and production in the South China Sea, as well as Malaysian entities operating in the Kasawari gas field.[24]

- In 2020, APT 40, believed to have ties to the Chinese government, launched highly targeted spear-phishing attacks against Malaysian government officials, aiming to install malware and exfiltrate confidential documents from government networks.[25]

*As of March 2024, Malaysia has not been publicly attributed to an offence cyber operation.

7. International Cooperation and Alliances

Key Indicators:

Participation in international cyber operations, exercises, and partnerships, which can enhance a country's capabilities through shared technologies, strategies, and intelligence.

Malaysia continues to foster bilateral relations in cyber security with other nations and identified international organizations or industry players through the creation of official collaboration instruments either by Memorandum of Understandings, joint statements or legal instruments.[26] The efforts will be followed through with practical collaborations such as knowledge sharing and transfers, joint R&D, technology transfers, information exchange and training, policy dialogues, jointly organized programme, and discussions on harmonization of legislation.[27]

Malaysia actively participate and contribute in regional, subregional and multilateral cyber security collaboration efforts through the United Nations (UN), the Association of South East Asian Nations (ASEAN) and its dialogue partners, the Five Power Defence Arrangements (FPDA) which includes Australia, New Zealand, the United Kingdom, and Singapore, the AsiaPacific Economic Cooperation (APEC), the Commonwealth, the Organization of Islamic Cooperation (OIC), the Global Forum on Cyber Expertise (GFCE), the Asia-Pacific Computer Emergency Response Team (APCERT), the Forum of Incident Response and Security Teams (FIRST), the Council of Europe, and other international entities.[28]

8. Legal and Ethical Frameworks

Key Indicators:

Laws and policies that govern cyber offensive operations, which can indicate the level of operational freedom and the ethical boundaries considered by a country.

The main pieces of legislation related to cybersecurity include:

- the Communications and Multimedia Act 1998;
- the Computer Crimes Act 1997;
- the Copyright Act 1987;
- the Penal Code;
- the Personal Data Protection Act 2010; and
- the Strategic Trade Act 2010.[29]

These laws encompass various criminal offenses related to cyber activities, such as unauthorized access to computer systems, the unauthorized disclosure of secrets, and other illicit activities.

However, the primary legislation governing cyber operations in Malaysia is the National Security Council Act of 2016. This act delineates the powers and functions of the National Security Council, empowering it to address escalating threats to the nation's security.[30] Within cybersecurity, this law grants the National Security Council the authority to coordinate and execute measures to protect national security, including cyber offensive operations in response to cyber threats.[31]

9. Cyber Doctrine and Strategy

Key Indicators:

Publicly available strategy documents and statements that outline a country's approach to cyber warfare, including its offensive and defensive priorities and ethical considerations.

Malaysia's Cyber Doctrine and Strategy has a nuanced approach that marries the nation's economic ambitions with its cyber security imperatives, reflecting a comprehensive strategy aimed at leveraging digital innovation while safeguarding national security.[32]

Malaysia's cyber strategy recognizes the transformative potential of the internet and digital technologies, which has been a catalyst for the country's transition from an agriculture-based to a knowledge-driven economy. [33] This vision is underpinned by a series of strategic policies and frameworks, including the National Cyber Security Policy (NCSP) and the Public Sector Cyber Security Framework, which collectively aim to protect 'Critical National Information Infrastructure' across ten key sectors through governance, innovation, education, and international collaboration.[34] Malaysia's cyber defense posture, as detailed in the 2020 Cyber Security Strategy and defense white paper, marks a shift towards more proactive cyber defense mechanisms in both civil and military domains.[35] This includes the development of offensive capabilities, albeit with a defensive orientation, primarily to be used in retaliation to cyber-attacks against the nation.[36] This strategy is supported by a robust governance and command structure led by the National Security Council (NSC) and the National Cyber Security Agency (NACSA), with dedicated operations centers within the Ministry of Defence (MoD) and the Malaysian Armed Forces (MAF) to protect ICT systems and enhance cyber capabilities.[37]

Malaysia's active engagement in international defense arrangements, such as FPDA, aims to bolster cybersecurity cooperation and resilience. Malaysia’s defence white papers acknowledges the transboundary nature of cyber threats, underscoring the necessity for regional and global cooperation.[38]

10. Technology Infrastructure

Key Indicators:

The overall state of a country's technology infrastructure, which can support or limit cyber offensive capabilities. This includes internet penetration, the availability of high-speed connections, and the presence of technology hubs and research institutions.

Malaysia's technology infrastructure, capable of supporting cyber offensive capabilities, is underscored by comprehensive government initiatives enhancing digital connectivity and cybersecurity. Investments in 5G, hyperscale data centers, and strategic partnerships position Malaysia as a digital hub.[39] The Malaysia Cyber Security Strategy 2020-2024 and the national Cybersecurity Commission fortify defenses against cyber threats.[40] These efforts collectively bolster internet penetration, high-speed connections, and the technological ecosystem, equipping Malaysia for advanced cyber operations while ensuring a resilient and secure digital infrastructure for economic growth and digital transformation.

Malaysia's commitment to advancing its technology infrastructure is evident through substantial government initiatives aimed at enhancing digital connectivity, cybersecurity, and the development of technology hubs. The strategic implementation of the Twelfth Malaysia Plan and the JENDELA action[41] plan showcases the nation's focus on upgrading its broadband services, with a significant shift towards 5G technology, aiming to ensure comprehensive and high-speed internet access across the country. These efforts are supported by considerable investments in hyperscale data centers and partnerships with global technology leaders,[42] positioning Malaysia as a burgeoning digital economy hub in the Southeast Asian region.

Furthermore, the Malaysia Cyber Security Strategy 2020-2024, alongside the establishment of a national Cybersecurity Commission,[43] highlights the proactive measures taken to bolster cybersecurity defenses, addressing the growing threat landscape and ensuring the protection of critical digital infrastructure. These strategic moves not only enhance Malaysia's defensive cyber capabilities but also potentially enable the country to leverage its advanced digital infrastructure for cyber offensive operations.

11. Cyber Defense Capabilities

Key Indicators:

While primarily defensive, a country's ability to protect its own networks can indirectly indicate its understanding of offensive tactics (by knowing how to defend against them).

Malaysia's cyber capabilities are anchored in a robust intelligence framework and strategic defense initiatives, emphasizing technological advancement and international collaboration to ensure comprehensive national security and economic growth.[44]

Malaysia's cyber capabilities are defined by a sophisticated blend of intelligence, technology, and strategic defense. Governed by the National Security Council, the nation's cyber-intelligence infrastructure is robust, focusing on mitigating internal threats and enhancing signals intelligence with specialized units like the Royal Signals Regiment. International collaborations further bolster Malaysia's capacity for counterterrorism and regional security, particularly in sensitive areas like the South China Sea.[45] [46]

Economically, Malaysia's digital sector, contributing significantly to GDP, is spearheaded by initiatives aimed at transforming the nation into a technological hub. This includes substantial investments in artificial intelligence and the development of critical infrastructure, such as extensive fibre-optic networks and the upcoming MEASAT-3d satellite, to enhance communication capabilities.[47]

Strategically, Malaysia emphasizes the importance of Cyber Electromagnetic Activities (CEMA) to protect its CNII from cyber and electronic threats.[48] Plans to establish a Cyber Electromagnetic Command (CEC) highlight a comprehensive defense approach, integrating cyber operations with electronic warfare to ensure national security.[49] These efforts underline Malaysia's holistic approach to safeguarding its digital and physical realms, emphasizing cyber operations' crucial role in national defense and the broader security strategy.

12. International Behavior and Participation:

Key Indicators:

Engagement in international forums on cybersecurity, adherence to norms and agreements, and behavior in global cyber incidents can provide insights into a country's stance and capabilities in cyber operations.

Malaysia demonstrates a robust commitment to international collaboration by actively engaging with various global forums and organizations. Through participation in platforms like the United Nations, the Association of Southeast Asian Nations (ASEAN), the Asia-Pacific Economic Cooperation (APEC), the Commonwealth, and the Organisation of Islamic Cooperation (OIC), Malaysia seeks to contribute to the development of international cybersecurity standards and treaties. This commitment extends to collaborative efforts with entities such as the Global Forum on Cyber Expertise (GFCE), the Asia-Pacific Computer Emergency Response Team (APCERT), and the Forum of Incident Response and Security Teams (FIRST), where Malaysia innovates proposals tailored to the interests of respective forums. Emphasizing the importance of international cooperation, Malaysia's Cyber Security Strategy prioritizes the strengthening of collaboration and cooperation in cybersecurity affairs, aligning domestic efforts with foreign policy objectives and actively participating in key international cyber fora.[50]

Moreover, Malaysia places a strong emphasis on enhancing regional and international cooperation through bilateral and multilateral platforms, seeking to harmonize domestic legislation with international conventions and treaties to effectively combat cyber threats on a global scale. The collaboration between Malaysia and the United States further strengthens cybersecurity efforts, with a focus on initiatives such as Malaysia's Digital Economy Blueprint[51] (MyDIGITAL) and technology transfer plans. This partnership fosters mutual interests in cybersecurity prioritization, introduces Malaysia to innovative technologies like the Open Radio Access Network[52] (O-RAN) system, and underscores the shared goal of enhancing digital economy sectors, promoting technological innovation, and stimulating investment in both nations.

Case Studies

Based on latest data as of: October 27, 2023

Rationale for the Choice of Cases

The selection of the two distinct case studies for this report is aimed at presenting a holistic view of Malaysia's cybersecurity landscape, focusing on both the national cyber threat power and the potential impact of asymmetric cyber actors:

The first case study examines the Malaysian government's engagement in significant cyber intelligence operations, such as the Project Magnum agreement, which highlights the state's capacity to harness advanced technology for surveillance and data analysis.

The second case study delves into DragonForce Malaysia, a group engaging in politically motivated cyber operations without state sponsorship. This case illustrates the threat posed by non-state actors leveraging cyber tools for ideological goals, targeting both domestic and international entities.

Together, the juxtaposition of these cases highlights the broad spectrum of cyber capabilities and intentions. This approach underscores the complexity of managing cyber threats, where the lines between conventional and unconventional cyber operations increasingly blur, requiring nuanced strategies for national and international cybersecurity and policy formulation.

Case Study 1: Malaysian Government Surveillance

Context

Summary

Over the years, Malaysia has been embroiled in numerous controversies, largely attributed to the ten-year tenure of former Prime Minister Najib Razak, who is currently serving a prison sentence for corruption charges.[53] Throughout his tenure, Najib's administration faced criticism for its rollback of human rights, persecution of minority religious groups and LGBTQ+ individuals, suppression of free speech, and restrictions on press freedom. [54]

However, one particularly intriguing development involves the $1.5 million agreement known as Project Magnum, entered into by the Malaysian government, aimed at procuring a system capable of gathering and analyzing civilian activity data.[55] This system was intended for use by Malaysia's intelligence agency, the Special Branch (SB), to monitor political activists associated with the opposition.[56] Due the absence of official diplomatic ties between Israel and Malaysia, the agreement was facilitated through a Cypriot intermediary company named Kohai Corp. Ltd., established by two Senpai shareholders expressly for such transactions.[57] These details were revealed as part of a legal dispute between Senpai's co-founders, which subsequently surfaced in a Tel Aviv court.[58] According to the court documents, the Malaysian government's intentions regarding the Senpai system were transparent, with its application for "political investigations" explicitly outlined.[59]

Senpai's flagship product, RogueEye, is designed to aggregate data from publicly available online sources, including social networks, and then analyze it to generate intelligence reports for various entities, including secret services, law enforcement agencies, militaries, and businesses.[60] While Senpai asserts that its system only accesses publicly available data, correspondence between Shloman and a company salesman, submitted as evidence to the court and reviewed by Calcalist, suggests that RogueEye also scrutinizes data from smartphones infected with spyware "Senpai's system collected the data from the infected phone and is analyzing it."[61] Furthermore, RogueEye's official data collection methods include the utilization of a network of avatars (fake social network profiles) to track targets and extract information through direct interactions with them.[62]

In 2020, Malaysia faced allegations of utilizing Pegasus software developed by the Israeli company NSO. Circles, affiliated with NSO Group, offers a phone surveillance system capable of globally monitoring calls, texts, and phone locations. Circles exclusively sells to nation-states, providing systems that connect to local telecommunications infrastructure or utilize the "Circles Cloud" to access networks worldwide.[63] According to CitizenLab, a Circles system known as Pixcell Mazda Farmer was identified in Malaysia. Pixcell is believed to denote a Circles device, with descriptions from the United States Federal Communication Commission (FCC) and United States Patent and Trademark Office (USPTO) indicating its function as a portable international mobile subscriber identity-catcher (used to intercept mobile phone traffic and location of mobile phone users). [64] According to an "informant withion the Special Branch" spyware has been used on Federal and state ministers and exco members, federal and state MPs and ADUNs, social and political activists, corporate identities of interest, those involved in organized crime, and certain media portals.[65]

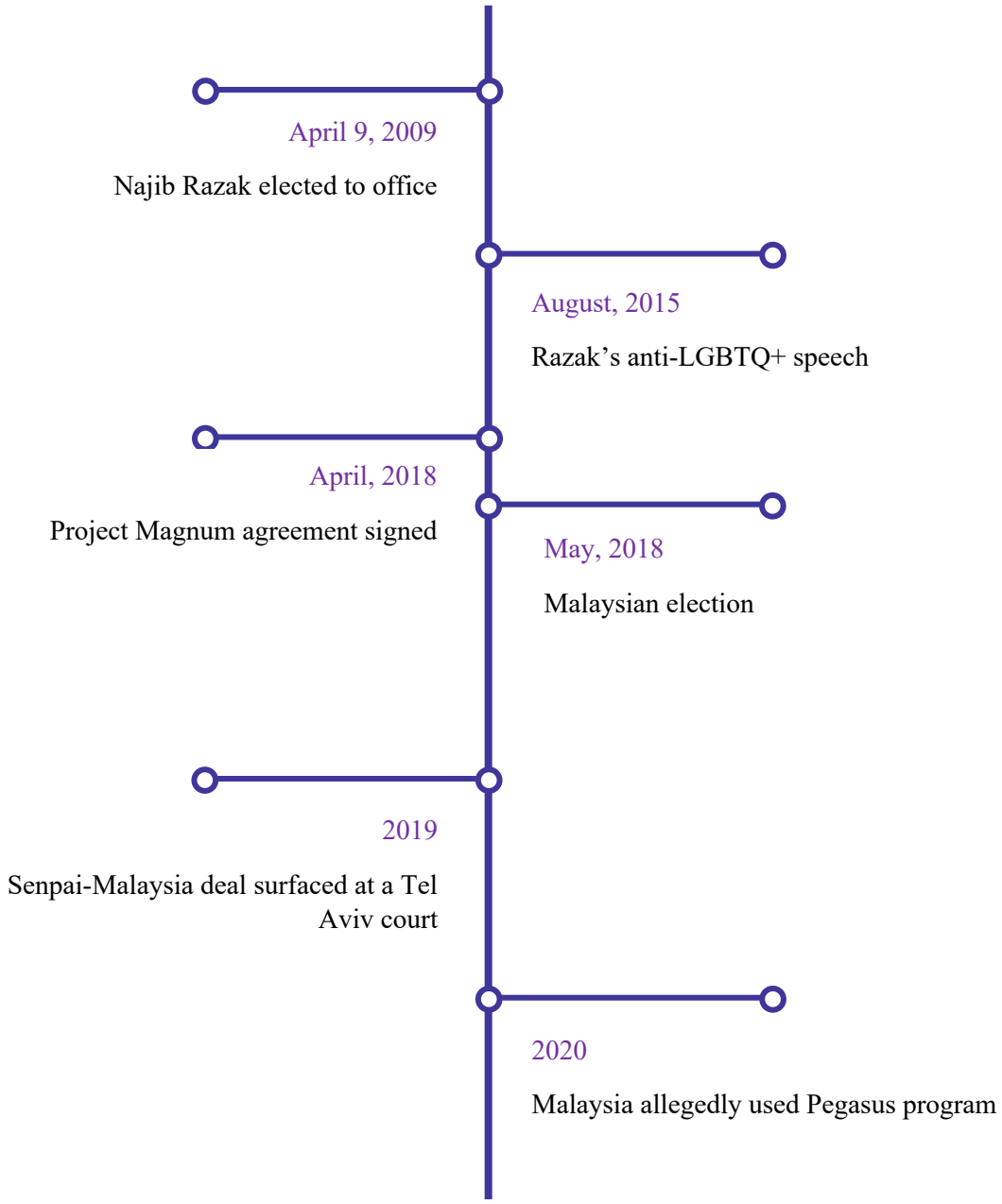
Actor Profile

Malaysia's democratic environment and government surveillance practices reflect a blend of progression and constraint. Ranked partly free by Freedom House,[66] Malaysia exhibits a mix of democratic features such as regular elections and active civil society, alongside restrictions on freedom of expression and assembly. The country operates under a federal constitutional monarchy, which has seen dominant party rule for decades, influencing political competition and governance.

Historically, Malaysia's governance has been marked by the use of laws and regulations to maintain political stability and control dissent. This includes surveillance and cybersecurity measures purportedly aimed at protecting national security, but which have raised concerns regarding privacy and freedom. The government has been criticized for surveilling and curbing dissenting voices, including opposition politicians, activists, and journalists, under the guise of preventing fake news and sedition.[67]

Recent years have shown signs of political change, notably the 2018 general elections that resulted in the first change of government since independence.[68] This shift promised reforms towards greater transparency and less censorship. However, challenges remain, including navigating the balance between national security interests and individual freedoms. The ongoing debate on government surveillance reflects broader concerns about the state of democracy in Malaysia, highlighting the tension between maintaining order and respecting human rights.

Key Events Timeline



Technical Analysis

RogueEye

It is important to note that the technical details of RogueEye have not come to light, only explicit details regarding the transaction in the Israeli Court system. As a result, any examination within the MITRE ATT&CK framework will rely on assumptions and comparisons with more widely known spyware.

Furthermore, it's important to highlight that RogueEye's primary function is to gather data from openly accessible online platforms, such as social networks, and subsequently analyze it to produce intelligence reports. However, due to RogueEye's capability to scan compromised phones, the MITRE ATT&CK framework below is structured around this technical aspect of RogueEye.

Tactics	Technique ID	Usage
Drive By Compromise:	T1456	Speculated that RogueEye was distributed through a website or app by exploiting vulnerabilities in the Web browser or code of applications on iOS devices.[69] This is based on similar capabilities on Pegasus, that has deliver software through messaging apps like WhatsApp to surveil users.[70]
Execution:	T1658	Speculated that RogueEye can compromise iPhone iOS without user interaction code as per similarities with Pegasus and other spyware.[71]
Persistence:	T1645	Speculated that RogueEye modifies the system partition to maintain persistence.[72]
Privilege Escalation:	T1404	Speculated that RogueEye exploits iOS vulnerabilities to escalate privileges.[73]
Credential Access:	T1517	Speculated that RogueEye collect data within notifications sent by the operating system or other applications these may contain sensitive data such as one-time authentication codes sent over SMS, email, or other mediums.[74]
Discovery:	T1420, T1426, T1421	Speculated that RogueEye enumerates files and search within file systems, disables competing jailbreaking software, and tracks network connections.[75]
Collection:	T1517, T1533, T1636	Speculated that RogueEye has the ability to gather contacts, capture SMS messages, access calendar capture call logs as well as access sensitive data in files.[76]

Pegasus (iOS)

Pegasus is a spyware developed by the Israeli company NSO Group, primarily sold to government clients for the purpose of conducting surveillance on individuals. Pegasus infiltrates devices unnoticed and gain comprehensive access to the device's operations, including capturing keystrokes, intercepting communications, tracking the device, and even utilizing the camera and microphone for espionage purposes.

It typically begins with a crafted SMS or iMessage that includes a link. If the recipient clicks on this link, it triggers the download of malicious software that then compromises the device. This exploitation process aims to achieve full control over the device's operating system, employing techniques known as "rooting" for Android devices and "jailbreaking" for Apple iOS devices. Pegasus has been reported to be more effective on Apple devices due to the consistency in their operating systems and the fast adoption of updates by users, making it a lucrative target for hackers looking to exploit the latest version of iOS, despite the perceived higher security of Apple devices. The spyware can also target Android devices, although its effectiveness might be reduced compared to iOS due to the diversity in Android versions and the varying degrees of security across different devices.[77]

Tactics	Technique ID	Usage
Drive By Compromise:	T1456	Pegasus was distributed through a website by exploiting vulnerabilities in the Safari Web browser on iOS devices[78]
Execution:	T1658	Pegasus can compromise iPhone running iOS 16.6 without and user interaction code.[79]
Persistence:	T1645	Pegasus modifies the system partition to maintain persistence.[80]
Privilege Escalation:	T1404	Pegasus exploits iOS vulnerabilities to escalate privileges.[81]
Discovery:	T1430, T1426, T1421	Pegasus updates and tracks phone location, monitors victim status, disables competing jailbreaking software, and tracks network connections.[82]
Collection:	T1429, T1430, T1409, T1636	Pegasus has the ability to record audio, track location, gather contacts, capture SMS messages and capture call logs as well as access sensitive data in files.[83]
Command and Control:	T1644	Pegasus uses SMS for command and control.[84]

Effects

Immediate Aftermath

The procurement of surveillance systems like RogueEye and the use of Pegasus software, likely led to increased scrutiny of Malaysia's government surveillance practices. These revelations have the potential to intensify public and international concerns about privacy infringement and the erosion of civil liberties. The exposure of such surveillance capabilities may have further eroded trust between the government and its citizens, particularly among opposition groups, activists, and marginalized communities targeted by these activities.

The controversy could also prompt calls for greater transparency and accountability in the government's use of surveillance technologies. It might lead to demands for legal and regulatory reforms to ensure surveillance practices are in line with international human rights standards. Additionally, these revelations may strain Malaysia's diplomatic relations, given the sensitive nature of utilizing Israeli-developed software and the complex international dynamics involved.

Strategic Logic

Political: The exposure of spyware in Malaysia has brought attention to the distribution of political power and authority within the government institutions. This scrutiny is particularly focused on the National Security Council Act of 2016, which has been criticized for undermining checks and balances by granting the Prime Minister unchecked authority with designating security areas that allow the enforcement of special measures without parliamentary approval. This has raised concerns about the potential for abuse of power, especially in the realm of cybersecurity enforcement. For instance, with the government having unchecked power under this Act, there are worries that cyber-related incidents or threats could be used as justification for the declaration of security areas, further increasing concerns about overreach. Even with a new government in place, the Act remains in effect, and concerns persist regarding accountability in the exercise of government powers. This can lead to political turmoil, erode trust in government institutions, and affect international relations with other states.

Military: While the exposure of spyware is more a civilian matter, it can still have military implications. For example, the revelation of Malaysia's supposed main spyware sheds light on the intelligence-gathering capabilities of the country, particularly as it was utilized by the Special Branch, the main intelligence arm of the government, which collaborates closely with military intelligence. This exposure raises concerns about providing adversaries with crucial insights into the country's defense capabilities and vulnerabilities. Given the technical complexity of spyware like RogueEye and Pegasus, adversaries may exploit various vulnerabilities in this software to potentially turn the technology against Malaysia.

Moreover, akin to other dual-use technologies such as drones, small arms, nuclear materials, or biological agents, the proliferation of spyware poses a global security risk. There is a pressing need for the development and enforcement of stringent regulations and export controls to govern the development and sale of spyware.

Economic: The exposure of government surveillance carries significant implications. Both domestic and international corporations may hesitate to engage in business activities in regions where surveillance practices are prevalent. Such security risks can erode confidence in the stability and security of the business environment, dissuading potential investors and partners.

A key concern arises from the potential infiltration of spyware into the mobile phones of employees. In such instances, sensitive data, including financial records and personal information of employees and clients, could be accessed and manipulated by the government or risk being leaked. The exposure of such confidential information undermines the trust and credibility of businesses but could result in financial losses for affected entities.

Social: No serious impact on the social environment.

Information: The information landscape in Malaysia has undergone significant changes following the exposure of government surveillance activities. Media outlets, particularly news platforms, have played a crucial role in shaping public discussions about surveillance practices within the country. There has been intense scrutiny from the media, highlighting concerns over the misuse of governmental powers and raising public awareness about the potential impacts on privacy and civil liberties. Moreover, Media outlets have been key in spreading information about government surveillance practices, stimulating public debate, and influencing public opinion. As a result, media engagement will continue to be essential in addressing public concerns and shaping perceptions regarding cybersecurity risks and government surveillance practices in Malaysia.

Infrastructure: The exposure of spyware can have potential effects on the communication system and infrastructure of the country. Firstly, the presence of spyware raises concerns regarding the security and reliability of telecommunications networks and internet infrastructure. This could lead to a decline in trust among citizens, potentially resulting in reduced usage of digital communication platforms. Secondly, concerning infrastructure, the revelation of government spyware underscores vulnerabilities in critical infrastructure systems. If government surveillance tools can breach private systems, it prompts questions about the security of other vital services such as power grids, transportation networks, and healthcare systems, and the possibility for adversaries to exploit similar weaknesses.

Short- and Long-Term Government Response

The government has remained relatively silent regarding their response to the exposure of their spyware usage. Former Prime Minister Najib Razak has explicitly denied allegations of utilizing an Israeli cybersecurity system for spying on Malaysian civilians, regardless of the evidence.

Consequently, there has been no official government policy response to the situation, suggesting minimal change within the country.

National Security Interests for Canada

Given that Malaysia's surveillance activities are primarily domestic in nature, there isn't significant concern for Canada apart from political interest in international laws pertaining to surveillance and privacy rights. Canada has consistently aimed to uphold human rights standards, and therefore, this doesn't pose a substantial national security risk for Canada, as it's unlikely that Malaysia would attempt to utilize its intelligence software on Canada.

Canada may assess the repercussions of Malaysia's revealed surveillance on trade and economic collaborations with Malaysia. For instance, Canadian businesses could face risks from spyware software, potentially leading to issues like intellectual property theft or corporate espionage. Although this poses a potential for financial losses or adverse effects on economic engagements, such as trade, investment, or business operations, it does not represent a significant national security risk.

Case Study 2: DragonForce Malaysia

Context

Summary

Since 2012, Anonymous has spearheaded campaigns protesting the Israeli government's actions in the Israeli-Palestinian conflict.[85] These operations, collectively known as OpIsrael, utilize a variety of techniques with varying degrees of sophistication. However, in recent years, with the decline of Anonymous and waning support for OpIsrael, a new group of pro-Muslim hacktivists from Southeast Asia, called "Dragon Force Malaysia," has emerged to fill the void.[86] With over 13,000 members communicating through a private forum, Dragon Force Malaysia has initiated several campaigns targeting Israeli organizations, including the recent OpsPetir.[87] These campaigns involve activities such as website defacements, denial-of-service attacks, and data leaks.[88] While not attaining the same level of notoriety as OpIsrael, these actions, along with others like OpsBedil, present a heightened risk for the region.

Actor Profile

DragonForce Malaysia is not considered an advanced or a persistent group, nor are they sophisticated. However, they make up for it with their organizational skills and ability to quickly disseminate information.[89] Despite their basic competence, they rely on common tools like basic attack scripts and virtual machines running Kali or Parrot Linux for their attacks.[90]

While DragonForce Malaysia operates independently of state sponsorship, it presents several concerns for Malaysia that could have far-reaching effects within the country's cyber landscape. While they have not targeted the Malaysian government thus far, this does not rule out the possibility. DragonForce is recognized as a vigilante group and participates in politically motivated hacking endeavors.

DragonForce Malaysia is heavily dependent on scripts to launch its attacks. See known tools below:

CyberTroopers

Developed by DragonForcce Malaysia memebers; Utilized in OpsPetir 2023.

CyberTroopers is an obfuscated Python program, which includes functionality to download lists of free and open proxy and SOCKS services on the internet from free-proxy-list[.]net and proxyscrape[.]com.

The collected proxy and SOCKS services are leveraged to spoof and randomise the origin of the attacks and increase the complexity of detection and mitigation for L7 application attacks/[91]

Figure 1: CyberTrooper DDoS Tool

Slowloris

Developed by "RSnake"; Confirmed use in 2022 OpBedil.

A denial-of-service tool that causes a server to become overwhelmed by sending HTTP headers in small, slow chunks.[92] This tactic forces the server to wait for the headers to arrive, eventually leading to resource exhaustion and an inability to handle legitimate requests.[93]

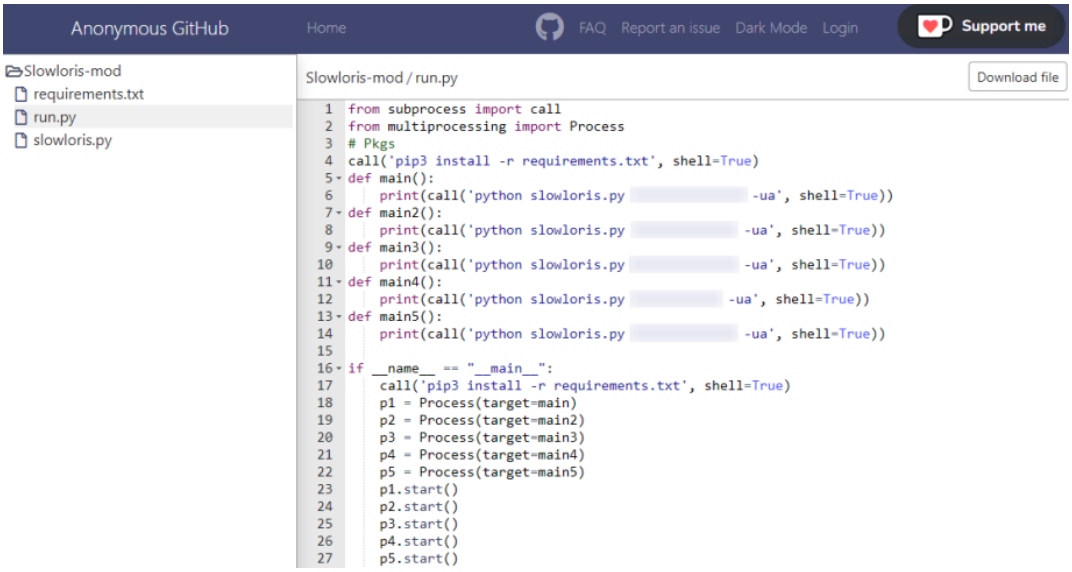


Figure 2: Slowloris Tool Used by DragonForce

DDosTool

Developed by “Waitercinta”; Confirmed use in 2022 OpBedil.

This simple Python script performs a UDP Flood leveraging datagram sockets and packets with a payload of 1,490 randomly generated bytes.[94] The payload does not change during the execution of the attack until the tool is stopped and restarted. The destination port is sequentially altered for every sent packet between 1 and 65,534 starting at the port passed as argument.[95]

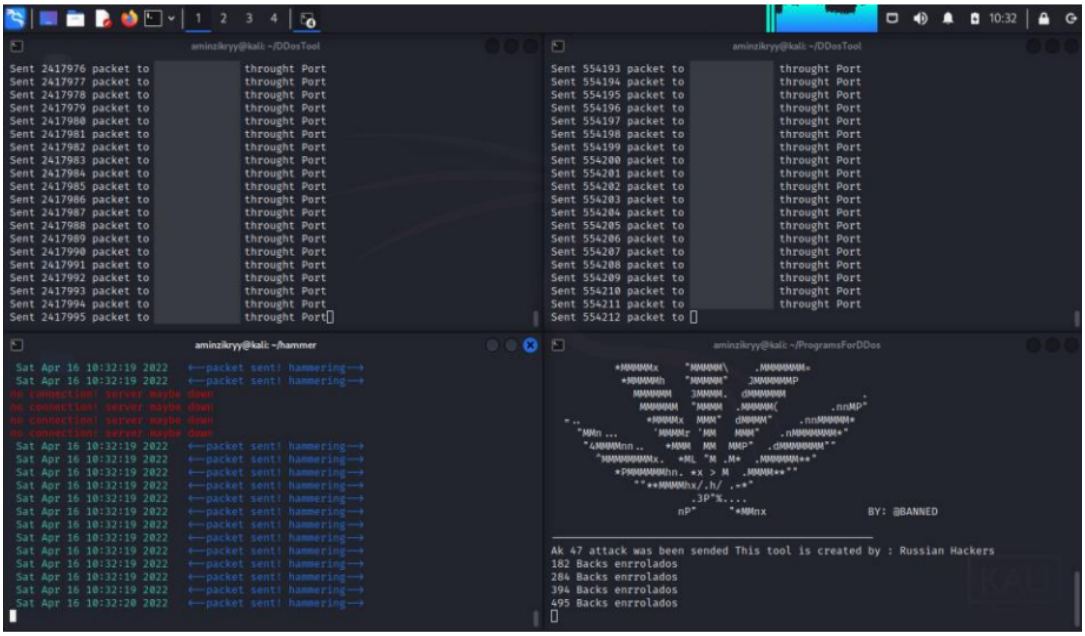


Figure 3: DDoSTool Screenshot

DDoS-Ripper

Developed by “Palahsu”; Confirmed Use in 2022 OpBedil.

A Python script to execute application-level attacks on web servers via direct and indirect paths. This script uses two concurrent attack vectors, each comprising 135 independent threads tasked with inundating the target server with HTTP requests. The first attack vector is a direct path HTTP GET request to the target IP leveraging a random user-agent header chosen from a predefined list and a static set of headers imported from a text file named “headers.txt.”

```
uagent.append("Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0) Opera 12.14")
uagent.append("Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:26.0) Gecko/20100101 Firefox/26.0")
uagent.append("Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913 Firefox/3.5.3")
uagent.append("Mozilla/5.0 (Windows; U; Windows NT 6.1; en; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)")
uagent.append("Mozilla/5.0 (Windows NT 6.2) AppleWebKit/535.7 (KHTML, like Gecko) Comodo_Dragon/16.1.1.0 Chrome/16.0.912.63 Safari/535.7")
uagent.append("Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)")
uagent.append("Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1")
uagent.append("Mozilla / 5.0(X11;Linux i686; rv:81.0) Gecko / 20100101 Firefox / 81.0")
uagent.append("Mozilla / 5.0(Linuxx86_64;rv:81.0) Gecko / 20100101Firefox / 81.0")
uagent.append("Mozilla / 5.0(X11;Ubuntu;Linuxi686;rv:81.0) Gecko / 20100101Firefox / 81.0")
uagent.append("Mozilla / 5.0(X11;Ubuntu;Linuxx86_64;rv:81.0) Gecko / 20100101Firefox / 81.0")
uagent.append("Mozilla / 5.0(X11;Fedora;Linuxx86_64;rv:81.0) Gecko / 20100101Firefox / 81.0")
```

Figure 4: Predefined list of user-agent headers leveraged by DDoS-Ripper

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
```

Figure 5: HTTP request headers used by DDoS-Ripper (as defined in headers.txt)

The second attack vector uses an indirect path strategy, utilizing a Facebook crawler and w3.org markup validation web services as bots to increase the load on the target server. This vector involves 135 threads randomly selecting between two predefined URIs:

https://validator.w3.org/check?uri=<target server>	URL[1]
https://www.facebook.com/sharer/sharer.php?u=<target server>	URL[2]

When queried, the w3.org markup validation website (URI [1]) generates a new web request from w3.org to validate the markup of the target URI. On the other hand, the Facebook sharer URI (URI [2]) prompts the Facebook crawler to request Open Graph tags from the target website, examining metadata such as description and potential images specified by the target's meta properties.

Hammer

Developed by TermuxHackz; Confirmed use in 2022 OpBedil.

A Python-based tool intended for use on mobile devices via Termux, an Android terminal emulator. The core script, named 'hammer.py,' mirrors the functionality of the DDoS-Ripper script discussed earlier, including the utilization of Facebook sharer and w3.org markup validation service bots.[96] However, DDoS-Ripper includes additional user-agent headers and offers more comprehensive help information.[97]

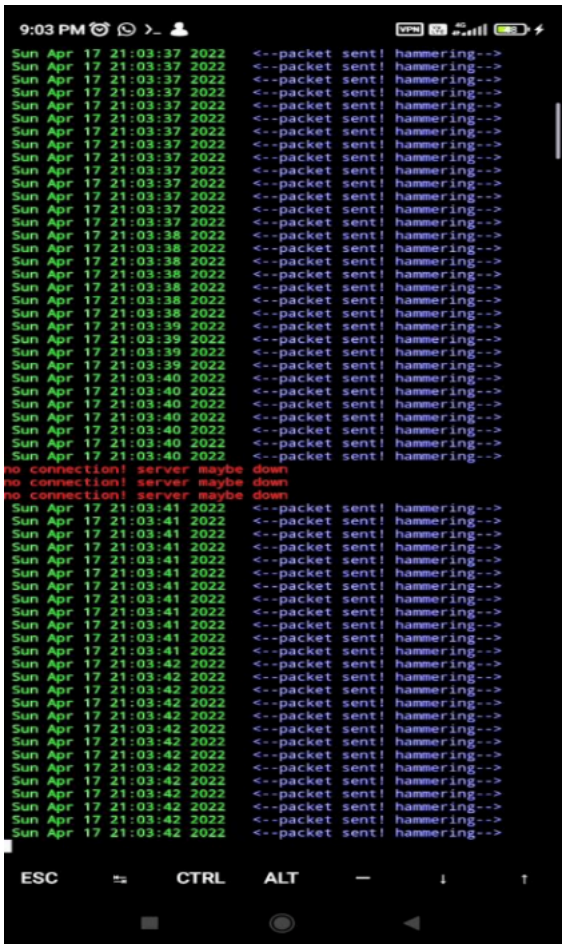
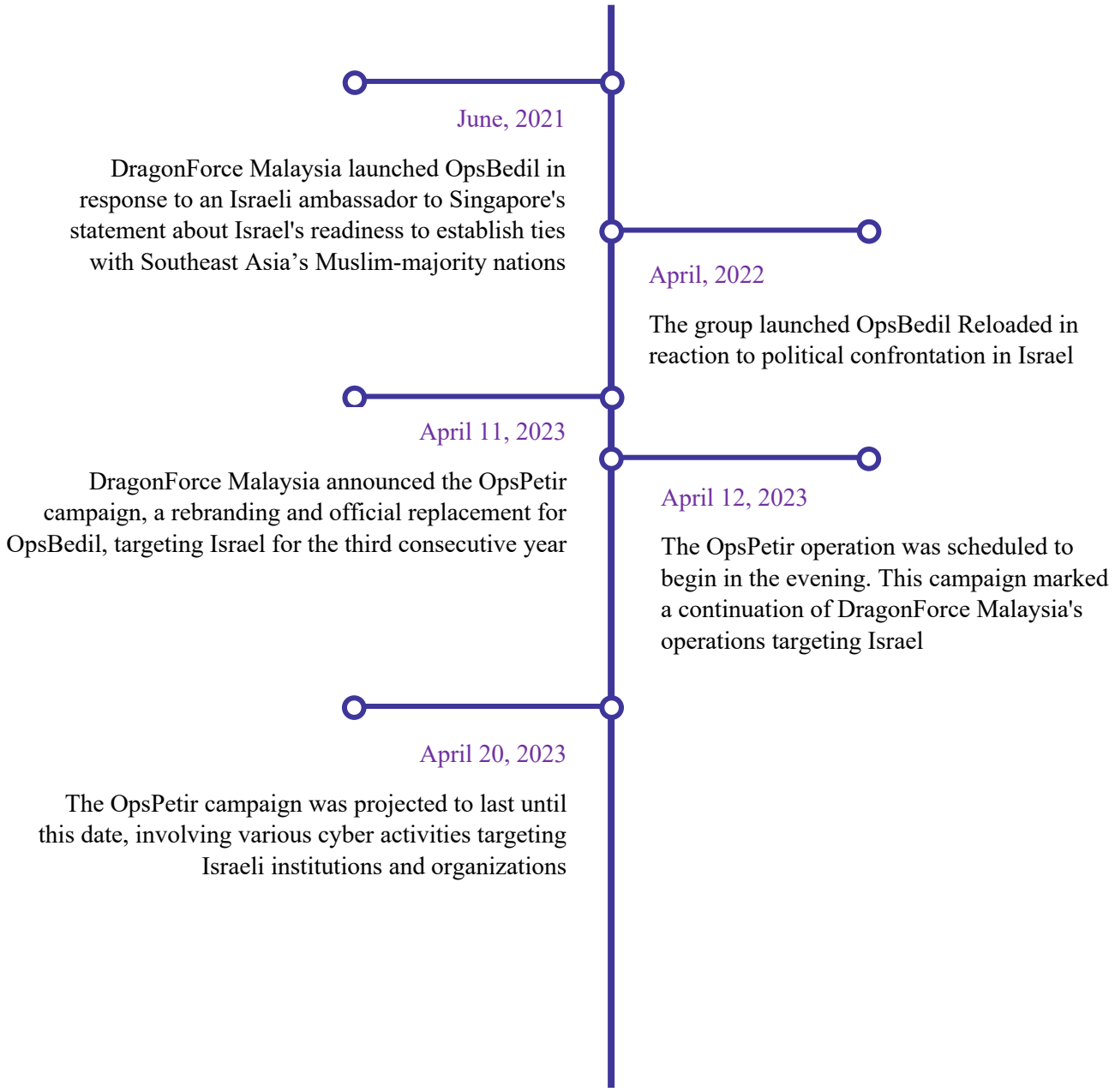


Figure 6: Screenshot of Hammer

Key Events Timeline

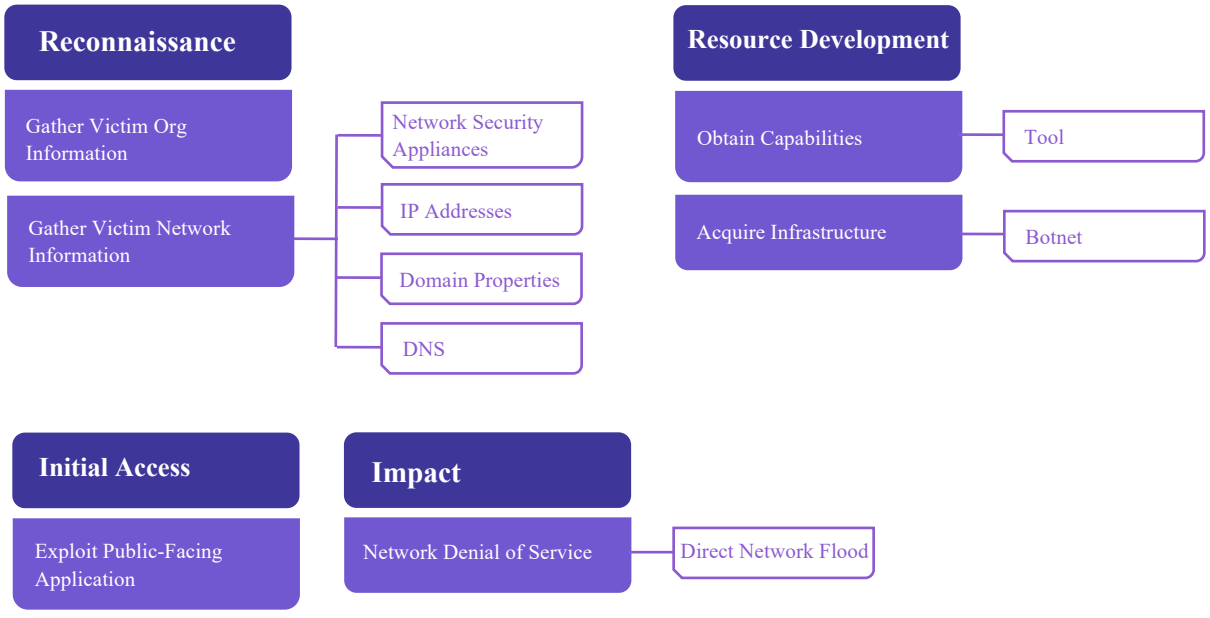


Technical Analysis

DDoS

DDoS attacks aim to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. In the context of their operations, such as #OpsPatuk against Indian organizations,[98] DragonForce has targeted a wide range of sectors, including financial organizations, government entities, and educational institutions.

To execute their DDoS attacks, DragonForce, along with associated hackers, might utilize compromised machines or botnets to generate massive volumes of traffic, aiming to take down websites or online services. This approach seeks to create high-profile disruptions, drawing attention to their political or social causes.[99]



In analyzing DragonForce's DDoS attacks, it is important to note that our assessment is limited to a tactical-level analysis. We lack full details and the capability to perform an in-depth analysis, and our insights are based on observable behaviors and reported methodologies. This analysis does not delve into the strategic intent or operational details of the attacks, given the constraints in data and access. Therefore, the conclusions presented should be regarded as a surface-level overview of DragonForce's tactical approach to DDoS attacks:

Tactics	**Technique ID**	**Usage**
Reconnaissance	T1591, T1590	DragonForce Malaysia **very likely** conducted thorough reconnaissance to gather information about the victim network. It is **probable** that this reconnaissance involved identifying network properties, security measures, IP addresses, and other relevant details to inform their strategy.[100]
Resource Development:	T1588	Following reconnaissance, the group would have proceeded to develop their resources for the attack. This **likely** involved selecting and preparing the botnet and tools they intended to utilize. Among the tools considered were Slowlorris, DDoSTool, DDoS-Ripper, and Hammer.[101]
Initial Access:	T1190	The initial objective was to exploit vulnerabilities in public-facing applications. This involved scanning the target organization's network to identify weaknesses in their Internet-facing hosts or systems.[102]
Impact:	T1498	DragonForce flooded networks with traffic generated through their various DDoS tools. As a result, DragonForce effectively disrupted the availability of services hosted on targeted systems. This disruption led to significant downtime for the affected networks.[103]

Effects

Immediate Aftermath

The immediate aftermath of DragonForce Malaysia's activities, particularly after launching a cyber attack named Operation Storm of Al-Aqsa against Israel, includes significant consequences and heightened alertness within the financial sector in Malaysia. Bank Negara Malaysia (BNM) confirmed the authenticity of a Pro-Israel hacktivist list circulating on social media, highlighting the real threat posed by potential retaliatory attacks against Malaysian organizations in response to DragonForce's operations. BNM issued a precautionary routine alert through the Financial Sector Cyber Threat Intelligence Platform (FinTIP), urging financial institutions to secure their systems against possible disruptions to financial services.

Despite no concrete evidence of planned retaliatory DDoS attacks against Malaysian organizations, BNM's alert was part of a broader effort to mitigate risks and prepare for potential cyber threats. The leaked FinTIP document also mentioned a range of Pro-Israel hacktivist groups known for targeting Malaysian entities, suggesting a heightened state of vigilance.

DragonForce's actions had tangible repercussions, including the successful breach of several websites and banking institutions in Israel. The group not only infiltrated these entities but also exposed banking information of undocumented immigrants, leading to unauthorized purchases of luxury goods using the leaked information. This series of events culminated in the suspension of DragonForce's accounts on the X application, illustrating the extensive impact and the ensuing digital warfare between hacktivist groups with opposing political stances.[104]

Strategic Logic

Political: Dragon Force Malaysia's activities represent a political interest as they are engaged in politically motivated hacking endeavors targeting Israeli organizations. While they have not targeted the Malaysian government yet, their actions could potentially lead to political tensions if they expand their scope to include domestic targets. Moreover, there may be implications for Malaysia's diplomatic relations with Israel and other countries affected by the group's activities. Moreover, it's important to note that the power wielded by this group does not a threat to the pose Malaysian government.

Military: The Malaysian government, particularly the defense sector, may not be overly concerned since the group is not an APT and has not targeted domestic entities. Additionally, due to the group's reliance on scripts, their level of sophistication is limited, thus minimizing the potential for significant harm. Nevertheless, Malaysia should maintain vigilance, as with the proliferation of cyber tools there arises the possibility of heightened concerns within the military regarding the potential targeting of critical infrastructure or sensitive military networks. This could have a potential impact on the safety and security of the Malaysian people.

Social: Dragon Force Malaysia has gained support as a self-proclaimed pro-Muslim group, targeting organizations perceived as adversaries to Muslim interests. Their significant following is largely attributed to their religious stance. However, Dragon Force's actions raise concerns about the potential for escalating tensions and conflicts between different religious or ethnic groups, both online and offline. While such outcomes are unlikely, it's essential for the Malaysian government to monitor the situation closely.

Economic: Dragon Force has primarily focused on Israeli institutions, which could present an economic threat to them. However, domestically, the economic impact may not be substantial. Nevertheless, both domestic and international corporations with ties to Israel might be reluctant to conduct business in affected regions due to the group's actions. This hesitation could potentially impact both the private and public sectors economically.

Information: The impact of DragonForce on Malaysia's information landscape concerning their actions against Israel has been notable. DragonForce commands a substantial following across Southern Asia and has notably impacted discussions among the public concerning Israeli actions in Gaza.This underscores the power of cyber groups or "hacktivists" in shaping political opinions. While this doesn't pose a significant risk to the Malaysian Government, it warrants monitoring due to the organization's capacity to gather, disseminate, and attract a considerable following. Consequently, it presents a potential risk to the information environment.

Infrastructure: No major risk.

Short- and Long-Term Government Response

The Malaysian government has demonstrated its dedication to bolstering cybersecurity measures and addressing cybercriminal activities through its 2020-2024 cyber strategy. This commitment involves enhancing cybersecurity infrastructure as part of broader efforts to combat cyber threats. While not specifically targeting groups like DragonForce, these initiatives signify proactive steps towards addressing cybersecurity challenges. Key objectives of the strategy include:[105]

1. Implementing robust cybersecurity measures to protect critical infrastructure and sensitive data from cyber threats and attacks;
2. Developing cybersecurity policies and regulations;
3. Strengthening incident response capabilities;
4. Enhancing cybersecurity awareness and education; and
5. Strengthening global corporation.

National Security Interests for Canada

Given Canada's historical support for Israel, there's a possibility that Dragon Force may target Canada for political reasons. However, due to their limited sophistication, their attacks, such as website defacements, don't pose significant national security risks. Nonetheless, it's important to monitor the situation, as cyberattacks always carry some level of risk. Given Dragon Force Malaysia is as a self-proclaimed pro-Muslim group, their significant following could raise concerns about the potential for escalating tensions and conflicts between different religious or ethnic groups. Given the current climate in Canada, both online and offline, it's imperative to closely observe this scenario to preempt any potential targeting of Canada by the group, which could exacerbate existing ethnic divides and tensions.

Assessments

Based on latest data as of: March 8, 2024

Vulnerabilities

One of the main vulnerabilities in Malaysia's cybersecurity landscape stems around the concentration of power within the state apparatus. With the exposure of spyware usage by the Malaysian state, this underscore concerns regarding unchecked authority. Such unchecked authority not only undermines transparency and accountability but also poses risks to civil liberties and individual privacy rights. The concentration of power within the state apparatus can lead to political turmoil, erode public trust in government institutions, and strain international relations. While this issue may not directly pertain to cyber defense or operational matters, it represents a significant area of concern that could have far-reaching implications for the state and its future trajectory. The concentration of power within the state apparatus poses inherent risks that extend beyond the realm of cybersecurity. It undermines the principles of democracy, accountability, and transparency and compromising the state as a whole. Therefore, there is a **moderate risk** of political instability, although the probability of such events occurring is relatively **low** given the positive direction of the new government. Nevertheless, there is still concern about Malaysia's current trajectory due to the lingering imbalance of state power.

Another major vulnerability in Malaysia was exposed with the spyware being exposed in use. This creates a unique opportunity for adversaries to exploit vulnerabilities in state-controlled surveillance mechanisms, potentially compromising national security and undermining cybersecurity efforts. Of particular concern is the potential interest of strategic actors like China, who may seek to capitalize on such vulnerabilities to advance their geopolitical interests in the Asia-Pacific region. The sophisticated surveillance capabilities afforded by the exposed spyware could offer strategic advantages to entities with vested interests in the region, thereby underscoring the need to address and strengthen Malaysia's cybersecurity infrastructure. This level of concern is **elevated** because of China's previous targeting of Malaysia and the likelihood of continued actions in the future. Consequently, this situation could pose elevated risks to both infrastructure and cybersecurity.

Finally, asymmetric powers like DragonForce present a vulnerability for Malaysia, particularly its cyber attacks on Israeli institutions. These attacks have the potential to provoke retaliatory measures or consequences from the affected parties, that could inadvertently draw Malaysia in disputes. While DragonForce claims to operate independently of state sponsorship, this could still lead to reputational damage if Malaysia's association with DragonForce is viewed unfavorably by other nations. Furthermore, the rise of hacktivist groups such as DragonForce underscores the necessity for enhanced cybersecurity measures, as demonstrated by their successful execution of cyberattacks against foreign targets. This vulnerability presents a **low level of concern** and **unlikely** to drag Malaysia into any disputes.

Threats

Cyber Threats:

Cyber threats pose a significant risk of politically motivated attacks from asymmetric powers in Malaysia targeting Canadian institutions, government agencies, or infrastructure. These attacks could lead to various security breaches, including the potential for data breaches, intellectual property theft, or cyber espionage, all of which could severely affect Canadian interests. The nature of these threats underscores the need for heightened cybersecurity measures and vigilance among Canadian entities to protect against such insidious cyber activities, ensuring the safeguarding of sensitive information and critical infrastructure against international cyber threats.

Foreign Adversaries:

Malaysia's exposed spyware can be exploited by foreign adversaries like China. With access to Malaysia's compromised surveillance infrastructure, these adversaries could infiltrate sensitive networks, steal valuable data, or launch disruptive cyberattacks. This not only compromises Malaysia's national security but also poses a threat to international cybersecurity. This could result in data breaches, economic espionage, posing significant risks to Canada's national security and economic interests.

Economic Impact on Canadian Businesses:

The economic impact on Canadian businesses due to the risks associated with investments or operations in Malaysia is a growing concern, primarily due to uncertainties surrounding surveillance practices and cybersecurity vulnerabilities. These uncertainties may lead to a potential reluctance among Canadian companies to engage in business activities within Malaysia, thereby impacting trade and investment flows. This could result in significant economic losses for Canada, highlighting the importance of addressing these cybersecurity and surveillance concerns to maintain robust international business relations and economic stability between the two nations.

Recommendations

Highlights:

1. Canada should engage diplomatically with Malaysia to address concerns related to surveillance practices and cyber threats posed by hacktivist groups. This can involve advocating for greater transparency, accountability, and adherence to international norms and standards in cybersecurity and human rights.

2. Canada should expand capacity-building efforts and extend assistance to Malaysia to expand its cybersecurity capabilities and resilience against cyber threats. Given the region's significance to Canada politically and strategically, such support is essential.

3. Canada should establish information-sharing mechanisms between Canada and Malaysia to facilitate the exchange of cyber threat intelligence, best practices, and mitigation strategies.

4. Canada should continue enhancing its cybersecurity defenses to safeguard its critical sectors.

Canada should approach Malaysia not as a direct threat but as a partner in addressing shared cybersecurity challenges. Prioritizing collaboration with Malaysia can effectively address mutual vulnerabilities outlined previously and reduce risks for both countries. However, Canada's cybersecurity strategy should include vigilant monitoring of cyber activities originating from or targeting Malaysia, including hacktivist groups like DragonForce, to assess potential risks. This approach ensures the protection of critical sectors like energy, finance, and telecommunications against cyber threats from Malaysia or other foreign actors. Furthermore, Canada must continue to focus on developing and acquiring emerging cybersecurity technologies to enhance its cyber defense capabilities and proactively mitigate evolving threats.

Canada should proactively monitor the trajectory of Malaysia's technological partnerships, especially its deepening involvement with China's Digital Silk Road initiative[106] and the activities of Malaysian cyber actors linked to Chinese state interests.[107] If Malaysia's collaboration with China indicates a substantial pivot towards Chinese cyber and technological spheres, this could signal an elevated risk of cyber threats. In such an event, Canada should reassess its engagement level and consider appropriate countermeasures to safeguard against potential threats emanating from this realignment. Continual assessment of Malaysia's geopolitical technological stance is crucial to pre-emptively identify and respond to any developments that may challenge Canada's cybersecurity interests.

Notes

[1] PricewaterhouseCoopers (PwC) Malaysia. "2024 Digital Trust Insights Report." PwC Malaysia, 2023. PDF. https://www.pwc.com/my/en/assets/publications/2023/pwc-malaysia-2024-digital-trust-insights-report.pdf.

[2] Ibid.

[3] Ignatius, Cynthia. “Cyber Threat Intelligence for Malaysia’s Digital Transformation.” BusinessToday, April 20, 2022. https://www.businesstoday.com.my/2022/04/20/cyber-threat-intelligence-for-malaysias-digital-transformation/.

[4] The Malaysian Insider. “Putrajaya Bought Spyware from Hacking Team, Leaked Info Shows.” The Edge Malaysia, July 2015. https://theedgemalaysia.com/article/putrajaya-bought-spyware-hacking-team-leaked-info-shows.

[5] Kumar, Bhavesh. “Singaporean and Malaysian Governments Accused of Using Spyware for Digital Surveillance of Citizens: IFSEC Insider.” IFSEC Insider | Security and Fire News and Resources, August 10, 2015. https://www.ifsecglobal.com/cyber-security/the-singapore-and-malaysia-government-connection-with-hacking-team-exposed-both-countries-using-spyware-for-digital-surveillance/.

[6] Rozario, Keith. “What Malaysia Bought from Spyware Maker Hacking Team.” Digital News Asia, July 16, 2015. https://www.digitalnewsasia.com/insights/what-malaysia-bought-from-spyware-maker-hacking-team.

[7] National Cyber Security Agency (NACSA). "Malaysia Cyber Security Strategy (MCSS) 2020-2024." National Cyber Security Agency, 2020. https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

[8] Ibid.

[9] Cyber Capabilities and National Power: A Net Assessment. *Policy File*. International Institute for Strategic Studies, 2021. https://web-opti-prod.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf.

[10] “Market Intelligence: Malaysia Cybersecurity.” International Trade Administration, April 2021. https://www.trade.gov/market-intelligence/malaysia-cybersecurity.

[11] “Cyber Security in the Digital Transformation Age.” Malaysian Investment Development Authority (MIDA), July 26, 2021. https://www.mida.gov.my/cyber-security-in-the-digital-transformation-age/.

[12] “Research & Development (R&D).” Malaysian Investment Development Authority (MIDA), January 30, 2024. https://www.mida.gov.my/industries/services/research-development-rd/.

[13] Malaysian Communications and Multimedia Commission. "MCMC-MyConvergence Vol. 22." Last modified 2023. Malaysian Communications and Multimedia Commission. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/MCMC-MyConvergence-Vol-22.pdf.

[14] National Security Council. 2020. “Malaysia Cyber Secuirty Strategy 2020-2024.” 2020.https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf. 6-7.

[15] Ibid. 7.

[16] Daim, M. 2020. “Bahagian Siber Dan Elektromagnetik Pertahanan (BSEP).” Air Times News Network. 2020. https://www.airtimes.my/tag/bahagian-siber-dan-elektromagnetik-pertahanan-bsep/.

[17] Ibid.

[18] Oon, Amanda. “How Malaysia Is Fighting Organised Cyber Crime.” GovInsider, June 2020. https://govinsider.asia/intl-en/article/haji-amirudin-abdul-wahab-cybersecurity-malaysia-fighting-organised-cyber-crime.

[19] Ibid.

[20] Lee, Julian. 2024. “Shedding Light on Malaysia’s Special Branch.” Www.iias.asia. International Institute for Asian Studies. 2024. https://www.iias.asia/the-review/shedding-light-malaysias-special-branch.

[21] Nixon, Alex. 2022. “Malaysia Cyber Threat Landscape 2022 | Kroll Cyber Risk.” Kroll. 2022. https://www.kroll.com/en/insights/publications/cyber/apac-state-incident-response/malaysia.

[22] Ibid.

[23] Council on Foreign Relations. 2023. “Tracking State-Sponsored Cyberattacks around the World.” Council on Foreign Relations. 2023. https://www.cfr.org/cyber-operations/.

[24] Ibid.

[25] Ibid.

[26] National Security Council. 2020. “Malaysia Cyber Secuirty Strategy 2020-2024.” 77.

[27] Ibid.

[28] Ibid.

[29] Ibid. 45.

[30] Government of Malaysia. 2016. “Laws Of Malaysia Act 776 National Security Council Act 2016.” https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/Akta-MKN-2016-BI.pdf. 9.

[31]National Security Council. 2020. “Malaysia Cyber Secuirty Strategy 2020-2024.” 2020. https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf. 77.

[32] The International Institute For Strategic Studies, “Cyber Capabilities and National Power: A Net Assessment,” The International Institute For Strategic Studies (The International Institute For Strategic Studies, June 28, 2021), https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/.153.

[33] Ibid.

[34] Ibid. 153-154.

[35] Malaysian Ministry of Defence, “Defence White Paper,” *Ministry of Defence - Malaysia* (Malaysia: Malaysia Nasional Library, 2020), https://www.mod.gov.my/images/mindef/article/kertas_putih/KPP2.pdf. 28.

[36] Ibid. 53.

[37] The International Institute for Strategic Studies, “Cyber Capabilities and National Power: A Net Assessment,” 154-155.

[38] Malaysian Ministry of Defence, "Defence White Paper,". 72.

[39] Reuters, "Malaysia – Driven by Digital Evolution," Reuters (Reuters, February 8, 2024), https://www.reuters.com/plus/malaysia-driven-by-digital-evolution.

[40] The International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," 154.

[41] National Digital Department of Malaysia, "National Digital Network (Jendela)," *National Digital Department of Malaysia*, 2024, https://www.malaysia.gov.my/portal/content/31120.

[42] Reuters, "Malaysia – Driven by Digital Evolution."

[43] Malaysian Ministry of Defence, "Defence White Paper," 5.

[44] The International Institute For Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment,". 154.

[45] Malaysian Ministry of Defence, "Defence White Paper. 28.

[46] The International Institute For Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," 155.

[47] The International Institute For Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," 156.

[48] Malaysian Ministry of Defence, "Defence White Paper," 34.

[49] Malaysian Ministry of Defence, "Defence White Paper," 60.

[50] National Cyber Security Agency (NACSA). "Malaysia Cyber Security Strategy (MCSS) 2020-2024." National Cyber Security Agency, 2020. PDF.

[51] "Malaysia, US to Strengthen Cooperation on Cybersecurity, Digital Economy, Says Minister." Malay Mail, November 18, 2021. https://www.malaymail.com/news/malaysia/2021/11/18/malaysia-us-to-strengthen-cooperation-on-cybersecurity-digital-economy-says/2021900.

[52] Ibid.

[53]Ganon, Tomer, and Hagar Ravet. "Exclusive Israeli Cyber Startup Senpai Helped Malaysia's Corrupt Leader Spy on Opposition." CTech. Calcalist, 2020. https://www.calcalistech.com/ctech/articles/0,7340,L-3828013,00.html.

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] Ibid.

[58] Ibid.

[59] Ibid.

[60] Ibid.

[61] Ibid.

[62] Marczack et al., "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles." The Citizen Lab, December 1, 2020. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

[63] Ibid.

[64] Ibid.

[65] Webmaster, M. T. 2023. "Malaysia Uses Israeli Spyware to Monitor Citizens." Malaysia Today. November 8, 2023. https://www.malaysia-today.net/2023/11/08/malaysia-uses-israeli-spyware-to-monitor-citizens/#:~:text=According%20to%20Khalid%2C%20the%20Israeli.

[66] "Malaysia: Freedom in the World 2021 Country Report." Freedom House. Accessed March 7, 2024. https://freedomhouse.org/country/malaysia/freedom-world/2021.

[67] Ibid.

[68] Kamaruddin, Nurliana, and Roy Anthony Rogers. "Malaysia's Democratic and Political Transformation." Asian affairs, an American review (New York) 47, no. 2 (2020): 126–148.

[69] The MITRE Corporation. "Collection, Tactic TA0035 – Enterprise." attack.mitre.org, 2020. https://attack.mitre.org/tactics/TA0035/.

[70] Ganon, Tomer, and Hagar Ravet. "Israeli Cyber Startup Senpai Helped Malaysia's Corrupt Leader Spy on Opposition."

[71] The MITRE Corporation. "Collection, Tactic TA0035 – Enterprise."

[72] Ibid.

[73] Ibid.

[74] Ibid.

[75] Ibid.

[76] Ibid.

[77] Musotto, Robert, and Paul Haskell-Dowland. "How You Can Tell If Your Phone Is Being Monitored." How does the Pegasus spyware work, and is my phone at risk? - ABC News, July 22, 2021. https://www.abc.net.au/news/2021-07-22/how-does-pegasus-spyware-work-and-is-my-phone-at-risk/100315390.

[78] The MITRE Corporation. "Pegasus for IOS, Software S0289." attack.mitre.org, 2022. https://attack.mitre.org/software/S0289/.

[79] Ibid.

[80] Ibid.

[81] Ibid.

[82] Ibid.

[83] Ibid.

[84] Ibid.

[85] Radware "Radware Threat Advisory: OpsBedil Reloaded 2022 by DragonForce Malaysi," 2022. https://www.radware.com/getattachment/77d38291-3e8a-4890-a7ec-f36a1f1ac597/Alert-DFM-OpsPetir-042023.pdf.aspx

[86] Ibid.

[87] Ibid.

[88] Radware. "Radware Cybersecurity Advisory: DragonForce Malaysia: OpsPetir" 2.

[89] Ibid.

[90] Ibid.

[91] Ibid.

[92] Radware "Radware Threat Advisory: OpsBedil Reloaded 2022 by DragonForce Malaysia" 6.

[93] Ibid.

[94] Ibid. 7.

[95] Ibid. 7.

[96] Ibid. 10.

[97] Ibid. 10.

[98] Sharwood, Simon. "Malaysia-Linked Hacktivists Make Ongoing Attacks on India." The Register - Biting the hand that feeds IT, June 15, 2022. https://www.theregister.com/2022/06/15/dragonforce_malaysia_india_attacks/.

[99] Windsor, Carl, Simran Kothari, Ankita Dasgupta, and FortiRecon Team. "Guidance on an Ongoing Hacktivist Operation #Opspatuk Conducted by the Malaysian Hacktivist Threat Group 'dragonforce' against Indian Organizations: Fortiguard Labs ." Fortinet Blog, June 15, 2022. https://www.fortinet.com/blog/threat-research/guidance-on-hacktivist-operation-opspatuk-by-dragonforce.

[100] The MITRE Corporation. "Reconnaissance, Tactic TA0043 - Enterprise." attack.mitre.org, 2020. https://attack.mitre.org/tactics/TA0043/.

[101]The MITRE Corporation. "Resource Development, Tactic TA0043 – Enterprise." attack.mitre.org, 2020. https://attack.mitre.org/tactics/TA0043. https://attack.mitre.org/tactics/TA0042/.

[102]The MITRE Corporation. "Initial Access, Tactic TA0001 – Enterprise." attack.mitre.org, 2019. https://attack.mitre.org/tactics/TA0001/.

[103]The MITRE Corporation. “Impact, Tactic TA0040 – Enterprise.” attack.mitre.org, 2019. https://attack.mitre.org/tactics/TA0040/.

[104] Sarji, Nurul Atikah. “BNM Confirms Pro-Israel Hacktivist List Legit, Alert Part of Precautionary Routine.” Sinar Daily, October 27, 2023. https://www.sinardaily.my/article/211685/focus/national/bnm-confirms-pro-israel-hacktivist-list-legit-alert-part-of-precautionary-routine.

[105] National Cyber Security Agency (NACSA). "Malaysia Cyber Security Strategy (MCSS) 2020-2024." National Cyber Security Agency, 2020.

[106] Carrozza, Ilaria, and Giacomo Bruni. “China’s Digital Silk Road and Malaysia’s Technological Neutrality.” The Diplomat, August 2023. https://thediplomat.com/2023/08/chinas-digital-silk-road-and-malaysias-technological-neutrality/.

[107] “Seven International Cyber Defendants, Including ‘Apt41’ Actors, Charged in Connection with Computer Intrusion Campaigns against More than 100 Victims Globally.” Office of Public Affairs, September 16, 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

Image Attributions

Cover page image: City Lights Skyline royalty-free stock illustration. Free for use. Image by Brigitte Werner from Pixabay.

Suggested citation:

Project GAIA. “Open-Source Global Conflict Analysis Report: February 2024.” Cyber Analytics and Security Research, March 8, 2024.

Cyber Analytics and Security Research (CASR) is a student-led research group based in Ottawa, Canada. We aim to facilitate industry alignment and cross-discipline research projects for the cybersecurity field by developing a cybersecurity-focused student talent pool, building a network with key government/private stakeholders in cybersecurity, and to provide support to student-led research projects.

Project GAIA is one of the student-driven programs facilitated through CASR. The project is designed to offer open-source analysis training to our student analysts. And it focuses on documenting the organizing and methodological process of experimental open-source practices.

GAIA:EP2402RV01