Strategising tech diplomacy for Malaysia

By Samantha Khoo

Foreword by Datuk Prof Dr Mohd Faiz Abdullah

October 2025

Institute of Strategic & International Studies (ISIS) Malaysia

ISIS Malaysia

ISIS Malaysia was established on 8 April 1983 with a mandate to advance Malaysia's strategic interests. As an autonomous research organisation, we focus on foreign policy and security; economics and trade; social policy and nation-building; technology and cyber; and climate and energy.

We actively conduct Track 2 diplomacy, promoting the exchange of views and opinions at the national and international level. We also play a role in fostering closer regional integration and international cooperation through various forums, such as the Asia-Pacific Roundtable, ASEAN Institutes of Strategic & International Studies network, Council for Security Cooperation in the Asia-Pacific, Pacific Economic Cooperation Council, Network of East Asian Think-Tanks, Network of ASEAN-China Think-Tanks and ASEAN-Australia-New Zealand Dialogue.

Contributor

Samantha Khoo is a researcher in the Cyber and Technology Policy Programme. Her scope of research includes cybersecurity, social media regulation and artificial intelligence governance. She has published a thematic brief on cybersecurity in Southeast Asia and several other pieces on digital safety and security sector governance. She is a former YSEALI fellow under the technology and innovation 2025 cohort and serves as a policy group member within the Global Majority team for the Centre for AI and Digital Policy.

Abstract

As digital technologies increasingly shape global governance, economic power and societal norms, diplomacy must evolve beyond traditional state-to-state interactions and reactive digital policies to engage the growing influence of multinational tech companies, platform providers and transnational standards bodies. This research note examines how Malaysia can develop a coherent national tech diplomacy strategy that moves beyond fragmented digital engagement to assert meaningful agency in the global digital order. Adapting the Cyber-Diplomacy and Cybersecurity Awareness Framework (CDAF) into a context-specific CDAF-D+ model, the paper maps Malaysia's institutional landscape across seven functional pillars of tech diplomacy: internet governance, data policy, cyber legislation, cyber diplomacy, cybercrime, cyber risk management, and AI governance. The framework offers a blueprint for aligning domestic digital governance with external diplomatic priorities, while avoiding the need to build new agencies. Drawing on precedents, such as Switzerland's innovation-governance model and India's NEST unit, the paper presents a flexible yet actionable framework for aligning domestic digital capabilities with external strategic objectives. It proposes interventions, including the deployment of digital envoys, creation of a national tech diplomacy scorecard and integration of diplomatic functions into existing inter-ministerial platforms. The paper demonstrates how Malaysia can operationalise tech diplomacy through a whole-of-government approach. By doing so, it offers a replicable model for other middle-income countries seeking to build diplomatic capacity, protect digital sovereignty and help shape the rules of the emerging global tech order.

Foreword

Technology is no longer just a matter of infrastructure or innovation. It has become a domain of power that increasingly dictates how influence is exercised, how norms are set and how governance is negotiated across borders. Today, decisions that shape public life are as likely to emerge from platform algorithms and transnational standards bodies as from parliaments or ministries. For states navigating this new terrain, diplomacy must evolve.

In her 2018 book *Digital Democracy, Analogue Politics*, Kenyan writer and political analyst Nanjala Nyabola makes it distinctly clear that technology is never neutral and platforms that shape public discourse are largely owned and governed by profit-driven corporations operating within powerful global economies.[1] This insight cuts to the core of today's diplomatic challenge: states are no longer negotiating solely with one another but increasingly with platforms, protocols and private actors whose interests may not align with democratic governance or regional priorities. If governments, particularly those from the Global South, do not take an active role in shaping the architectures and norms of the digital order, they risk becoming subject to systems designed without them in mind. This is not merely a question of voice or representation but a matter of sovereignty, security and strategic relevance.

This research note responds to that challenge. It argues that tech diplomacy is no longer optional, especially for countries like Malaysia, positioned at the crossroads of digital transformation, geopolitical competition and regional rule-setting. As technology continues to reshape how power is distributed and decisions are made, Malaysia must develop the institutional strategies, diplomatic architecture, and regulatory foresight to engage not only with other states, but also with the private technology companies, platform providers, industry consortia, and technical standard-setting bodies that are now actively shaping global norms and digital rulemaking.

What follows is not a prescriptive policy roadmap but a strategic research note that aims to provoke reflection and guide institutional foresight. It encourages Malaysia to move beyond fragmented digital engagement towards a more cohesive and anticipatory diplomatic posture. The note calls for greater institutional clarity, international assertiveness and a recalibration of how the state engages with global technology actors and governance frameworks. This research note challenges the prevailing notion that only the most powerful or technologically advanced countries have a say in shaping the global digital order. It contends that all states, regardless of size or economic standing, have both the capacity and responsibility to influence how technology is governed. In doing so, they can ensure that the global digital future is not simply inherited but shaped deliberately and inclusively.

Datuk Prof Dr Mohd Faiz Abdullah
Chairman
Institute of Strategic & International Studies (ISIS) Malaysia

Executive summary

- As digital power shifts from governments to technology companies, platform providers and standards bodies, states must rethink their diplomatic strategies. This research note argues that tech diplomacy, defined as a state's strategic engagement with global technology actors, platforms and norm-setting institutions, is now a foreign policy imperative. In an increasingly polylateral digital environment, fragmented regulatory responses are no longer sufficient.
- Using Malaysia as a case study, the note proposes a whole-of-government tech diplomacy framework (CDAF-D+) to coordinate cross-border digital engagement and elevate Malaysia's normative voice in multilateral, regional and corporate-led digital forums. These pillars include internet governance, data governance, cyber legislation, cyber diplomacy, AI governance, cybercrime and attacks, and cyber risk management. The addition of AI governance reflects the urgency of developing clear national positions on artificial intelligence across ethical, regulatory and geopolitical domains.
- Through a detailed mapping of Malaysia's institutional landscape, including MOFA, MOSTI, MDEC, MCMC, PDPD, NACSA and others, the paper proposes a coordinated whole-of-government approach. This includes the creation of an interministerial tech diplomacy task force, while leveraging on platforms like the National Digital Economy and Fourth Industrial Revolution Council to align domestic and international technology governance efforts.
- Finally, the paper outlines practical pathways to operationalise tech diplomacy, including strengthening interagency coordination, enhancing diplomatic training and building strategic partnerships with international forums and private technology actors. It also recommends the use of national policy platforms to align domestic and foreign digital agendas and proposes a tech diplomacy scorecard to monitor institutional readiness and global engagement. These measures aim to equip governments with the tools to move from reactive participation to proactive norm shaping in the global digital order.

Glossary

Abbreviation	Definition
4IR	Fourth Industrial Revolution
AI	Artificial Intelligence
ADGMIN	ASEAN Digital Ministers Meeting
AMMTC	ASEAN Ministerial Meeting on Transnational Crime
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
GPAI	Global Partnership on Artificial Intelligence
IEC	International Electrotechnical Commission
IGOs	Intergovernmental Organisations
ISO	International Organisation for Standardization
ITU	International Telecommunication Union
MCMC	Malaysian Communications and Multimedia Commission
MDEC	Malaysia Digital Economy Corporation
MOFA	Ministry of Foreign Affairs
MOSTI	Ministry of Science, Technology and Innovation
NACSA	National Cyber Security Agency
NAIO	National AI Office
OECD	The Organisation for Economic Co-operation and Development
PDPD	Department of Personal Data Protection
RCEP	Regional Comprehensive Economic Partnership
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNESCO	The United Nations Educational, Scientific and Cultural Organisation
UN GDC	United Nations Global Digital Compact

Table of Contents

1 Introduction

As emerging technologies reshape the distribution of power and norms across global systems, diplomacy is no longer confined to negotiations between states. It must now contend with new actors, such as technology firms, standards bodies, industry consortia and digital platforms, whose influence often exceed that of traditional states. Companies like Apple, Microsoft and Nvidia possess market capitalisations that exceed or are comparable to the GDPs of entire countries, such as the United Kingdom and France, positioning them as pivotal actors in global governance and even rivals of sovereign states in levels of influence.[2] This shift calls for a re-conceptualisation of diplomatic practice, one that integrates innovation, governance and geopolitical strategy.

As such, traditional diplomacy, which is primarily centred around intergovernmental negotiations and treaties, is increasingly insufficient to address the speed, scale and stakeholder complexity of technological transformation. A new form of statecraft, known as tech diplomacy, has thus emerged to address the unique challenges and opportunities of this digital transformation. Not merely a branch of digital policy, it reorients foreign policy to account for how technologies, such as artificial intelligence (AI), 5G, quantum computing and data infrastructures, shape sovereignty, security and global order. While the concept gained traction following Denmark's 2017 TechPlomacy initiative, its relevance has widened, especially for middle-income countries seeking to exert normative agency amid growing asymmetries in the global digital order.

As such, this research note is guided by the following questions:

a. what institutional and strategic conditions are required for Malaysia to build an effective national tech diplomacy framework?

b. how can Malaysia operationalise tech diplomacy to align its digital policies with broader foreign policy objectives?

2 Literature review

2.1 Definitions, etymology and conceptual overlap

While relatively budding, tech diplomacy is quickly gaining traction because of its urgency in global policy debates. To understand this emergence, it is first necessary to revisit the foundational role of diplomacy itself. Traditionally, diplomacy functions as a tool of statecraft, allowing states to pursue national interests, negotiate influence and shape the international order through peaceful engagement rather than coercive means.[3] It allows for governments to form alliances, mediate conflicts, assert sovereignty and influence global norms through intergovernmental negotiations, treaties and multilateral cooperation.

However, the accelerating pace of technological change, coupled with the growing geopolitical influence of private technology firms, has exposed the limitations of conventional diplomacy. Emerging technologies are increasingly governed not by intergovernmental treaties alone but by corporate actors, technical standards bodies and global digital platforms. The field is notably polylateral, involving governments, tech companies, standards bodies and civil society, marking a departure from diplomacy's state-centric traditions.[4]

As such, Bjola and Kornprobst propose an "analytical triangle" spanning technological processes, agency (actor interaction) and global order.[5] This framework reveals how diplomacy must not only contend with technologies like AI, quantum computing and blockchain but also with the informal rules and background knowledge (e.g. algorithmic bias, digital colonialism) that shape their governance. The result is a form of diplomacy that is simultaneously technical, political and discursive, reflecting the complex realities of governing emerging technologies. In this evolving environment, tech diplomacy has emerged as a necessary and adaptive mode of engagement.

Despite its growing importance in the field of international relations, tech diplomacy remains loosely defined, often overlapping with adjacent domains, such as digital diplomacy, cyber diplomacy and science diplomacy. These overlaps have made it difficult to standardise terminology or scope, though distinct differences remain in terms of focus, actors and tools. Most conceptualisations frame tech diplomacy as the practice of international engagement between governments and tech companies to influence and negotiate norms, regulations and partnerships concerning emerging technologies.

The etymology of the term "tech diplomacy" stems from the broad abbreviation "tech" for "technology" and "diplomacy" in its traditional form.[6] In reality, tech diplomacy extends beyond state-to-state relations. Former Brazilian director of science, technology, innovation and intellectual property Eugenio Vargas Garcia defines tech diplomacy as "the conduct and practice of international relations, dialogue and negotiations on global digital policy and emerging technological issues among states,

the private sector, civil society and other groups".[7] The field is notably polylateral, involving governments, tech companies, standards bodies and civil society, marking a departure from diplomacy's state-centric traditions.

While tech diplomacy is often conflated with terms, such as digital diplomacy, cyber diplomacy and science diplomacy, important distinctions exist between them. Digital diplomacy focuses on communication tools, such as social media for public diplomacy, while cyber diplomacy focuses on international efforts to establish norms and frameworks for cybersecurity and internet governance.[8] Science diplomacy, meanwhile, emphasises international collaboration in scientific research and innovation.[9]

Tech diplomacy, on the other hand, draws elements from all three, is rooted in negotiating influence over emerging technologies and is as much about geopolitical leverage as it is about economic strategy and standards setting.[10] It also adds a new element to the mix, which is innovation.[11] This element is about innovating, regulating and integrating technology within diplomatic practices. This is as tech diplomacy often involves actors who do not typically participate in traditional diplomacy, such as AI ethicists and product engineers. This expansion of diplomatic engagement complicates the lines between lobbying, foreign policy and technological collaboration. Table 1 summarises these differences.

Term	Focus area	Key actors	Tools
Digital diplomacy	Use of digital platforms in diplomacy	States, embassies	Social media, websites
Cyber diplomacy	Cybersecurity, cyber norms, cyber threats	States, IGOs, NGOs	UNGGE, OEWG
Science diplomacy	International scientific cooperation	Scientists, ministries	Research networks, bilateral science accords
Tech diplomacy	Engagement with the tech sector on emerging tech policy as part of foreign policy	Governments, tech companies, civil society	Tech envoys, digital attachés

Table 1: Comparative analysis of tech diplomacy and its conflating terminology.[12]

Recent scholarship has underscored the evolution of tech diplomacy as both a conceptual and practical response to the power asymmetries introduced by emerging technologies. Schmidt distinguishes tech diplomacy from adjacent fields by identifying "innovation power" as its defining feature referring to the capacity to not just regulate or communicate technology but to actively co-create and govern its development.[13]

For the purposes of this paper, tech diplomacy is defined as a state's engagement with private technology actors to influence, negotiate, and co-develop standards, norms, and responsible practices, rather than state-to-state relations over technology issues. This distinction clarifies the focus on diplomacy directed at the corporate sector, which complements but is analytically separate from traditional interstate digital negotiations.

Denmark is widely credited with popularising the formal use of the term in 2017 through its Techplomacy initiative, where it appointed a tech ambassador to Silicon Valley.[14] However, it was not the first country to formalise a diplomatic role engaging with emerging technologies. Australia, for example, appointed its first cyber affairs ambassador in 2016 as part of a national cybersecurity strategy, signalling an early recognition of the need to embed technological issues within foreign policy.[15]

Denmark's move, however, was distinctive in its framing. This is as it explicitly extended diplomatic engagement to include multinational technology companies as quasi-sovereign actors, placing them as equivalent to states in terms of influence over digital infrastructure, standards and societal norms. Since then, several countries have appointed tech diplomats in some way, shape or form, such as France's digital ambassador, the Netherlands' cyber ambassador and Brazil's tech ambassador, reflecting varying institutional priorities and geopolitical goals. As Schwab reminds us, the Fourth Industrial Revolution (4IR) is not only exponential in pace, but structurally disruptive across sectors and borders.[16] Against this backdrop, the institutionalisation of tech diplomacy reflects a recalibration of global governance, where legitimacy, authority and rulemaking are increasingly co-produced across sectors. In this sense, tech diplomacy is not just a tool of foreign policy, it is itself a battleground for digital sovereignty, innovation ethics and global influence.

2.2 Strategic imperatives for tech diplomacy

The trajectory of foreign policy is being reshaped by rapid technological innovation. Emerging technologies, such as AI, blockchain and quantum computing are fundamentally transforming societies, economies and political systems. These developments extend beyond domestic governance, increasingly redefining international diplomacy and global cooperation. Framed as part of 4IR, this wave of innovation transcends borders and impacts on nearly every sector, demanding new forms of strategic engagement.

The influence of large multinational tech companies also continues to expand, with some companies surpassing the economic and political clout of traditional state actors. These companies not only define industry standards but also exert growing influence over both domestic policymaking and international relations, often surpassing the regulatory capabilities of national governments and creating the need for new forms of diplomatic engagement. Furthermore, emerging technologies have

enabled non-state actors to play significant roles in shaping global norms and driving political agendas. As seen with 5G, these developments are now intrinsic to national security and geopolitical competition.

The Tech Diplomacy Academy at Krach Institute underscores the importance of integrating technological, commercial and foreign policy expertise to steer trusted technologies towards the goal of democratic resilience and peace.[17] It warns that, if left ungoverned, these emerging technologies could destabilise democratic institutions and international order. With the rise of AI-generated disinformation[18] and the subsequent threat of quantum computing to break modern encryption,[19] it is crystal that critical technologies have the potential to pose significant risks to global security. As such, there is a need for tech diplomacy to be embedded into core foreign policy processes to address these threats and ensure cross-sectoral cooperation.

2.3 Gaps in the literature

Despite the proliferation of writing on both digital and cyber diplomacy, academic literature on tech diplomacy in the Global South remains limited. Most frameworks originate from European contexts and reflect high-income country policy environments. There is growing recognition that countries in the Global South must not merely be rule-takers but must also actively participate in shaping the international tech order.[20] This is to ensure that global digital norms, policies and advancements are inclusive, equitable and responsive to their unique development needs and priorities. In the context of Malaysia, this means translating national development goals into coordinated international strategies.

This paper adopts a working definition of tech diplomacy as "a state's strategic engagement with technology actors, both domestic and international, to shape the rules, standards and norms governing emerging technologies in ways that promote national interests, digital sovereignty and multilateral cooperation". The definition is adopted because of Malaysia's desire to become a regional digital hub as well as its active participation in ASEAN's digital governance architecture. By focusing on the state's role in balancing between private sector innovation and public regulatory interests, this definition provides for a malleable yet actionable basis for the development of a national tech diplomacy strategy.

2.4 Importance of tech diplomacy for Malaysia

Malaysia's strategic position in the global technology landscape underscores the growing need for tech diplomacy. As a key player in the global semiconductor industry, Malaysia sits as its sixth largest exporter globally, commanding 13% of the global market share for packaging, assembly and testing.[21] These functions are foundational to the development

of frontier technologies, such as AI, 5G and Internet of Things (IoT) applications, making Malaysia a critical player in the architecture of modern global economy.

Additionally, the government has been actively driving digital transformation through initiatives, such as the Malaysia Digital Economy Blueprint, also known as MyDigital, which aims to accelerate the adoption of emerging technologies.[22] Building on these efforts, the launch of Malaysia's National AI Roadmap 2021-2025 and the establishment of a National AI Office represent a strategic deepening of Malaysia's commitment to institutionalising the governance of emerging technologies.[23] While foundational frameworks, such as the Communications and Multimedia Act 1998, provide regulatory oversight for telecommunications infrastructure, these recent initiatives reflect a deliberate shift towards anticipatory and cross-sectoral governance capable of engaging with complex, evolving technological systems. These developments reflect an understanding that economic competitiveness and national development hinges on strategic development with technology.

In tandem with its strategic role in the global supply chain and ongoing digital transformation, Malaysia is also cultivating a dynamic innovation ecosystem, underpinned by a growing start-up landscape and targeted talent development initiatives. The country has seen a notable expansion in sectors, such as fintech, e-commerce and digital services, with Kuala Lumpur and Penang emerging as key innovation hubs that attract venture capital investments and regional tech firms.[24] The government's emphasis on upskilling talent through initiatives such as the Malaysia Tech Entrepreneur Programme and partnerships with global tech firms has strengthened its competitive edge.[25] While challenges remain, such as digital infrastructure gaps and talent retention, Malaysia's continuous efforts to enhance its technological capabilities and attract high-value investments position itself as a strong contender in the global digital economy.

While Malaysia has made commendable strides in digital transformation through frameworks, such as the MyDigital Blueprint and the National AI Roadmap, its international digital engagement remains fragmented and reactive. Cross-border issues, ranging from AI governance and cross-jurisdictional data flows to cybersecurity and platform regulation, are currently addressed in a siloed fashion by individual ministries and agencies.

Regionally, Malaysia has been deeply engaged in ASEAN's digital governance structure, including through the ASEAN Digital Ministers' Meeting (ADGMIN), ASEAN Ministerial Track on Cybersecurity (AMTC) and ASEAN Ministers Responsible for Information (AMRI). Malaysia also continuously engages in frameworks, such as the ASEAN Digital Master Plan 2025[26] and the ASEAN Cybersecurity Cooperation Strategy.[27] However, participation in regional initiatives has largely focused on infrastructural development and e-commerce facilitation, rather than on asserting normative influence over the governance of emerging technologies.

Despite that, Malaysia's presence in global multilateral forums is sporadic although it has participated in a few global norm-setting platforms on technology. In 2023, at the Open-Ended Working Group on Security and Use of Information and Communications Technology, Malaysia emphasised the importance of a unified, rules-based approach to cyberspace governance. It also highlighted the need for inclusive participation from developing countries and reaffirmed Malaysia's commitment to advancing regional cyber coordination through ASEAN initiatives, such as Regional Computer Emergency Response Team (CERT) and ASEAN Norms Implementation Checklist.[28]

Malaysia also supported UN General Assembly Resolution 78/241 on Lethal Autonomous Weapons Systems (LAWS) in December 2023, where it called for voluntary legal reviews of autonomous weapons systems under the Convention on Certain Conventional Weapons (CCW) framework. Similarly, Malaysia participated in the Responsible AI in the Military Domain (REAIM) workshops and its subsequent REAIM Summit 2024 in Seoul, where Defence Minister Khaled Nordin urged local industry players to pioneer AI adoption in the military sector, highlighting the Malaysia Armed Forces' potential to leverage on domestically developed AI technologies.[29]

However, Malaysia's presence in global multilateral forums, such as UNESCO's AI ethics deliberations and OECD-led digital economy discussions, remains limited and inconsistent, despite these being key venues where international standards are shaped. Although Malaysia has long-standing memberships in bodies like the International Telecommunication Union (ITU) and the International Organisation for Standardisation (ISO), its participation is not comprehensive. For instance, while Malaysia aligns with ISO 25237:2017 on personal health data protection,[30] it does not currently engage in the ISO/IEC Joint Technical Committee on Artificial Intelligence, where critical norms for AI governance are being developed.

Howbeit this broad pattern of norm endorsement and participation in regional and international forums, Malaysia's engagements are often largely transactional and issue-specific, concentrating on digital infrastructure development and e-commerce facilitation rather than sustained involvement in AI safety, platform governance or the proactive shaping of global standards. To capitalise on its strategic position and close this gap between presence and influence, Malaysia's foreign policy must evolve beyond conventional digital diplomacy into a cohesive, multi-stakeholder tech diplomacy paradigm that is forward-looking, coordinated and capable of systematically advancing national interests in the governance of emerging technologies.

This decentralised and ad hoc approach has constrained Malaysia's ability to project influence in the digital domain and to safeguard its long-term technological and geopolitical interests. As such, Malaysia must shift from piecemeal digital engagement to structured tech diplomacy. Tech diplomacy does not solely address regulatory alignment or digital facilitation but involves playing a proactive role in shaping the international rules, standards and platforms that govern emerging technologies. In a world where companies, such as Meta, Google and OpenAI, influence encryption protocols, content moderation policies and AI ethics frameworks, Malaysia needs to position itself as an active interlocutor.

This emerging gap between technological transformation and diplomatic response, referred to by scholars as a "diplomatic deficit", is precisely what tech diplomacy aims to bridge. As emphasised in the literature, states must adapt to a hybrid diplomatic environment shaped not just by intergovernmental processes but by negotiations with tech platforms, standards-setting bodies and civil society.[31]

While Malaysia has been active in digital infrastructure development and cyber policy, its foreign policy mechanisms have yet to internalise tech diplomacy as a core domain. Coordination across ministries remains reactive, siloed and domestically focused, with minimal sustained engagement in global rule-shaping platforms. This represents not just a governance challenge but a diplomatic gap, one that limits Malaysia's strategic influence in emerging tech orders.

As countries enter geopolitical contestations over technological standards, Malaysia's participation in tech governance must be framed through the lens of sovereignty and multilateralism. Effective tech diplomacy offers an opportunity for Malaysia to safeguard its strategic autonomy, secure technology collaborations and build partnerships that shape norms rather than simply adapt to them post hoc.

Through investing in such a structured tech diplomacy approach, Malaysia has the opportunity not only to elevate its global profile but also to move from a reactive posture to one of active norm entrepreneurship. This shift would help ensure that both national and broader Southeast Asian interests are not sidelined in the governance of emerging technology regimes. The CDAF-D+ framework proposed here offers a pathway to operationalising this ambition by aligning institutional mandates, building sustained multi-stakeholder engagement and translating domestic capabilities into coherent international influence.

3 Methodology

This research adopts a qualitative desk research methodology, synthesising secondary sources from policy documents, academic literature, think-tank analyses and case studies for conceptual adaptation. These methods were chosen to create a holistic and context-sensitive framework for tech diplomacy in Malaysia.

3.1 Outlining the cyber-diplomacy and cybersecurity awareness framework (CDAF)

A significant component of the methodology involves adapting and applying the Cyber-Diplomacy and Cybersecurity Awareness Framework (CDAF) developed by Zwarts, Du Toit, and Von Solms.[32] CDAF was designed to build the diplomatic and cybersecurity capacities of developing countries. This paper adapts the "diplomacy in cyberspace" component to assess and propose a roadmap for Malaysia's tech diplomacy. The following six pillars are used to structure analysis and guide institutional design.

CDAF pillar	Adapted for tech diplomacy in Malaysia
Internet governance	Diplomatic literacy in global internet institutions
Data governance	Cross-border data flows, data localisation, privacy frameworks
Cyber legislation	Understanding of digital laws and treaties
Cyber diplomacy	Negotiation, norms-setting and multilateral tech engagement
Cybercrime and attacks	Protection of diplomatic and strategic infrastructure
Cyber risk management	Institutional preparedness and digital sovereignty planning

Table 2: Outline of the CDAF pillars and their adaptation for tech diplomacy within Malaysia, created by the author.

Table 2 outlines CDAF's core pillars and how they can be tailored for tech diplomacy. The CDAF model supports a phased development approach that allows policymakers to track progress from reactive coordination to proactive norm entrepreneurship.

This framework will also help identify gaps in diplomatic expertise, policy coherence and stakeholder engagement by enabling a strategic blueprint for capability development. Through the integration of this model with policy analysis, this method ensures theoretical robustness and practical relevance. The qualitative approach allows for flexibility when tailoring recommendations for Malaysia's developmental status, institutional capacity and diplomatic positioning in ASEAN.

3.2 Case studies: Denmark and Singapore

While appointing dedicated tech envoys and establishing institutional structures are visible markers of tech diplomacy, it is essential to recognise that such measures are instrumental as they serve broader strategic objectives, such as safeguarding national regulatory autonomy, promoting adherence to domestic laws, securing technological advantage and shaping global norms. Each country's model reflects different strategic priorities, ranging from economic competitiveness to geopolitical influence and domestic regulatory enforcement.

Denmark's appointment of a tech ambassador in Silicon Valley marked the acknowledgement of the role of private tech giants in shaping global norms, values and policy architecture the way states do. Australia, Switzerland and France adopted similar strategies, with each defining specialised diplomatic functions that cover a broad portfolio, including digital trade, cybersecurity, AI regulation, and data flows.[33] Essentially, Denmark's proactive recognition of tech companies as crucial players in global governance and the necessity of establishing direct and dedicated channels to engage with them put them at the top of an aspirational holistic tech diplomacy model. The "tech ambassador" model offers a blueprint for countries aiming to understand, influence and partner with the private sector on digital issues, rather than just regulating them.

In ASEAN, Singapore is arguably the most mature tech diplomacy actor, even without a dedicated "tech ambassador" as per the Danish model. Singapore demonstrates a deeply integrated strategy whereby technology policy is intrinsically linked to its economic and foreign policy. Singapore hosts significant regional headquarters for major tech companies like Google, Microsoft, Amazon and Meta, underscoring its role as a key global digital and innovation hub.[34]

Singapore also actively pursued digital economy agreements with partners, such as,[35] Chile and New Zealand,[36] which intrinsically involve negotiating rules and standards for technology-driven trade and cross-border data flows. It is also a leader in setting global baseline digital trade rules at the WTO through the Joint Statement Initiative on E-Commerce,[37] directly engaging with other nations on tech-related trade governance.

Its "Smart Nation" initiative, while domestic, functions as an international branding tool that projects Singapore as a regulatory and technological innovator, directly attracting tech investments and partnerships. The presence of multilateral institutions and numerous tech companies makes Singapore an ideal test bed for embedding diplomatic functions related to technology governance within regional and global tech ecosystems.

Singapore demonstrates the power of a clear national technological vision as a tool for international engagement and branding, directly attracting tech companies and talent. Furthermore, its ability to attract and integrate major tech players within its ecosystem provides valuable insights into fostering public-private dialogue on technology policy and leveraging on technological innovation for diplomatic advantage.

Assessing the maturity and effectiveness of tech diplomacy initiatives requires evaluating their impact beyond institutional structures. For example, Denmark's early efforts culminated in the Tech Ambassador's Office successfully influencing compliance with Danish and EU regulatory standards among major platforms and securing direct engagement channels with Silicon Valley firms.

Similarly, Singapore's approach has contributed to high compliance rates with domestic data protection laws and strengthened its position in global initiatives, such as the Christchurch Call to Action, a cross-border commitment to eliminate terrorist and violent extremist content online. These examples demonstrate that mature tech diplomacy combines symbolic representation with sustained efforts to align corporate behaviour with national and multilateral priorities.

For Malaysia, these case studies help to highlight the importance of leveraging on domestic tech regulations as foundational elements for international influence. These case studies also suggest that Malaysia could align national digital initiatives with foreign policy to attract investment and engage on global tech governance issues.

3.3 Malaysia's digital ecosystem

Malaysia's institutional ecosystem is rich with potential actors and frameworks relevant to tech diplomacy. However, these components remain disconnected and underutilised for foreign policy purposes. Tables 3 and 4 below outline key digital frameworks and stakeholders within the Malaysian ecosystem that can be utilised and their relevancy to establishing a solid tech diplomacy landscape in the country.

3.3.1 Key frameworks

Framework	Purpose	Relevancy for tech diplomacy
MyDigital Blueprint	Accelerate digital transformation, position Malaysia as regional digital economy leader	Informs Malaysia's aspiration for regional leadership, attracts foreign investment, creates foundation for international partnerships and shapes regional digital norms.
Personal Data Protection Act (2010)	Safeguard privacy of Malaysians in commercial transactions	Aims to build trust in digital ecosystem, aligns with global data protection standards, crucial for cross-border data flows and attracting privacy-conscious tech investments
Communications and Multimedia Act (1998)	Regulate communications and multimedia industries, enhance online safety, mitigate security risks	Aims to create a safer online environment attractive for international digital businesses and could influence stance on global platform governance
Fintech regulatory frameworks (under Bank Negara)	Facilitate fintech innovation while preserving financial stability and consumer protection	Could position Malaysia as attractive fintech hub, draw foreign investment and expertise, inform policy development, enhance cross-border digital financial services and security
National AI Framework (Consists of the National AI Roadmap 2021-2025, the National AI Governance and Ethics (AIGE) Guidelines 2024, National AI Office (NAIO) and the upcoming AI Technology Action Plans)	Could promote responsible and ethical AI development, drive economic growth, ensure global competitiveness	Could serve as a direct instrument for shaping global AI governance, foster international partnerships, secure access to AI resources, facilitate knowledge sharing and attract AI talent and/or investment

Table 3: Key frameworks that can be utilised to build Malaysia's tech diplomacy, created by the author.

3.3.2 Key actors

Actor	Mandate	Potential interest in tech diplomacy
Ministry of Foreign Affairs (MOFA)	Conduct foreign relations, articulate foreign policy, coordinate international issues	Global tech governance, multilateral cooperation, strategic non-alignment, enhancing Malaysia's international stature
Ministry of Digital	Spearhead digital transformation, digital economy, data protection	Digital sovereignty, regional digital leadership, attracting tech investment, fostering digital talent, shaping digital norms
Ministry of Investment, Trade and Industry (MITI)	International trade, industry development, investment promotion	Attracting FDI in high-tech industries, strengthening supply chains, regional trade integration, economic resilience
Ministry of Science, Technology and Innovation (MOSTI)	Advance STI, develop startup ecosystem, foster deep tech	Innovation, R&D, tech commercialisation, start-up growth, human capital development in STI
Ministry of Communications	Oversee content, information, broadcasting, and MCMC	Online safety, content regulation, managing digital narratives, media development
National Cyber Security Agency	Formulate and coordinate national cybersecurity policies, strategies, and operations; oversee critical infrastructure protection; serve as national lead on cybersecurity incident response	Strengthening Malaysia's cyber resilience, engaging in cross-border threat intelligence sharing, contributing to global cybersecurity norms and confidence-building measures, advancing sovereign digital security interests in multilateral forums
National AI Office (NAIO)	Centralised authority for Malaysia's AI agenda, policy, governance, investment.	Responsible AI development, AI competitiveness, ethical AI, talent pipeline, international AI partnerships.
Malaysian Communications and Multimedia Commission (MCMC)	Regulate communications and multimedia industries.	Network security, consumer protection, competition, content regulation, digital infrastructure.

Actor	Mandate	Potential interest in tech diplomacy
Department of Personal Data Protection (PDP)	Enforce the Personal Data Protection Act 2010, oversee compliance with data protection regulations, manage cross-border data transfer mechanisms	Engaging in international data protection frameworks (e.g. ASEAN Data Management Framework, APEC CBPR), promoting interoperability of privacy standards, negotiating adequacy decisions and data transfer agreements, contributing to global debates on personal data governance
Bank Negara Malaysia (BNM)	Monetary and financial stability, financial sector development	Fintech innovation, financial inclusion, digital payments, cybersecurity in finance, anti-fraud
Malaysia Digital Economy Corporation (MDEC)	Lead digital economy, attract investment, develop talent	Digital hub of ASEAN, tech investment, talent development, business digitalisation, international market access for tech companies
Attorney-General's Chambers (AGC)	Draft and review legislation, provide legal advice to the government, represent Malaysia in international legal negotiations and treaty-making	Developing and harmonising digital laws and treaties, negotiating international legal frameworks on cybersecurity, data protection and AI ethics, ensuring compliance with international obligations, contributing to norm-setting on legal aspects of emerging technologies
Royal Malaysia Police (PDRM)	Enforce national laws, investigate cybercrime, protect public order and security	Cross-border cybercrime cooperation, participation in international law enforcement networks (e.g. Interpol, ASEANAPOL), shaping norms on digital evidence handling, combating online extremism and transnational criminal networks
Academia/think-tanks	Research, policy advice, expert commentary, knowledge sharing	Evidence-based policymaking, ethical tech development, capacity building, international academic collaboration

Actor	Mandate	Potential interest in tech diplomacy
Private sector/tech companies	Innovation, investment, market adoption, service delivery	Business growth, market access, regulatory clarity, talent pool, digital infrastructure development

Table 4: Key actors that can be utilised to build Malaysia's tech diplomacy, created by the author.

4 Adapting and applying CDAF to Malaysia for tech diplomacy

4.1 Application and adaptation of CDAF

This paper aims to adapt and apply CDAF to serve as a blueprint for building a robust tech diplomacy infrastructure. To suit the context of Malaysia, this paper proposes an expanded model, dubbed CDAF-D+, that evolves CDAF's six pillars into seven operational domains of state-led strategic engagement with tech actors. The seventh pillar on AI governance aims to respond to the global race to shape AI standards, ethics and safety protocols. This adaptation shifts the focus from general digital issues to targeted interactions with stakeholders that shape emerging tech norms, architectures and ecosystems.

4.2 Role and purpose of CDAF-D+ model

While the CDAF-D+ model provides a structured framework for mapping institutional mandates, it is important to clarify that it is not intended as a checklist that, once filled, guarantees tech diplomacy readiness. Rather, it should be understood as a dynamic diagnostic and planning tool. Each pillar represents a focus area where governments can assess their current capacities, identify capability gaps and design strategies for engagement. This approach recognises that institutional priorities, technological challenges and global norms will continue to evolve, requiring periodic reassessment and recalibration.

Unlike many existing frameworks, which often emphasise cybersecurity or public diplomacy alone, CDAF-D+ explicitly integrates domains, such as AI governance, cross-border data regulation and platform governance, which are increasingly central to the geopolitical influence of private technology actors. In doing so, it offers a more comprehensive template that allows governments to build a balanced approach encompassing regulatory, economic, and normative dimensions of emerging technologies.

In practice, applying CDAF-D+ could involve conducting a baseline assessment for each pillar, for example, evaluating Malaysia's level of participation in international AI standards-setting or its legislative readiness to address cross-border data transfer

disputes. From this baseline, policymakers can prioritise investments in institutional capacity (such as creating a dedicated AI standards liaison office under NAIO) and develop specific diplomatic initiatives (such as seeking observer status in ISO JTC1/SC42 or coordinating ASEAN contributions to the Global Partnership on AI). Progress could then be tracked through an internal monitoring tool or scorecard that maps milestones and outcomes to each pillar.

Crucially, CDAF-D+ is designed to be a living framework, supporting an iterative process of capacity building and strategic alignment. It should not be seen as a finite set of steps to be completed but rather as a reference architecture to guide Malaysia's evolving engagement in global technology governance.

The following sections illustrate how this framework could be operationalised through institutional mapping, interagency coordination and targeted diplomatic initiatives.

4.3 Case studies: operationalising tech diplomacy and making CDAF-D+ work

Several countries have begun to institutionalise tech diplomacy through models that align closely with the CDAF-D+ framework, offering instructive precedents for Malaysia. One example is Switzerland, which has adopted what is often called the "AI Trinity" approach. This model integrates Zurich's technological innovation ecosystem with Geneva's global governance footprint, underpinned by the principle of communal subsidiarity.[38] Zurich, home to a high concentration of tech start-ups, research institutions and tech R&D hubs, anchors Switzerland's capabilities in AI model development, platform governance and digital infrastructure.[39] Geneva, by contrast, hosts major international institutions including the UN and ITU, and serves as the base for the Geneva Science and Diplomacy Anticipator (GESDA), which anticipates science and technology trends to inform global policy.[40] This dual-hub model enables a coordinated whole-of-government approach to tech diplomacy that leverages on both innovation and governance capital.

A second case is India, which in 2020 established the New and Emerging Strategic Technologies (NEST) Division within its Ministry of External Affairs. This institutional innovation signals a strategic pivot towards embedding technology issues in the heart of foreign policy. The NEST Division coordinates India's positions on AI, data governance, platform regulation and cybersecurity in global fora, while also linking domestic ministries to external diplomatic missions.[41] Notably, it also facilitates dialogue with non-state actors, such as private tech companies, academics, and civil society, reflecting the polylateral nature of tech diplomacy.[42] By streamlining domestic expertise with foreign policy priorities, India's approach exemplifies how emerging economies can assert agency in shaping global tech norms.

Both Switzerland and India demonstrate that tech diplomacy is not confined to major powers. Instead, it is a feasible and strategic pathway for countries like Malaysia to operationalise tech engagement through structured institutional coordination. Their

experiences show how the CDAF-D+ pillars, particularly those relating to institutional alignment, international norm-setting and platform governance, can be embedded into foreign policy practice.

4.4 Envisioned strategy and coordination for Malaysia

To engage meaningfully in global technology governance, Malaysia must develop a structured, whole-of-government approach to tech diplomacy. The CDAF-D+ model offers a framework to translate domestic regulatory capacities into sustained international engagement. Rather than managing general digital policy, the model outlines how specific institutional mandates can be mobilised to shape global technology norms, standards and governance frameworks.

Table 5 outlines how each pillar under CDAF-D+ can anchor Malaysia's diplomatic efforts in priority domains. It does so by aligning lead institutions to functional roles in external engagement, thereby enabling Malaysia to act, not just as a rule-taker, but as an active contributor to the evolving digital order.

CDAF-D+ pillar	Lead institution(s)	Role in tech diplomacy	Strategic engagement focus
Internet governance	MCMC	Represent Malaysia in multilateral fora, such as Cybersecurity Tech Accord or Microsoft's Digital Geneva Convention, to shape digital public good governance	Work with industry and platforms on global standards. Participate in ASEAN Digital Ministers' Meeting (ADGMIN) and Global Digital Compact process; propose a joint ASEAN position on content moderation and data fairness
Data governance	PDP, MDEC	Develop regulatory positions on cross-border data flows and digital trade	Coordinate positions for ASEAN, OECD and APEC engagement, and develop structured dialogues with multinational tech companies on data protection compliance and cross-border transfer standards. Develop Data Transfer Assessment Framework for ASEAN data sandboxing; pilot B2B data transfer MOUs with cloud providers (e.g., AWS, Google Cloud)

CDAF-D+ pillar	Lead institution(s)	Role in tech diplomacy	Strategic engagement focus
Cyber legislation	AGC, NACSA	Ensure legislative support for emerging technologies and digital rights	Align legal frameworks to international digital economy norms, including cross-border data transfer standards, e-commerce regulations, cybersecurity obligations, digital trade agreements (e.g. CPTPP, RCEP), and adherence to global instruments, such as UNCITRAL Model Law on Electronic Commerce and OECD AI Principles
Cyber diplomacy	MOFA, NACSA	Shape bilateral and multilateral tech norms, manage tech relations with other states	Host diplomatic engagements with tech firms, pursue representation in tech-related IGOs, increase Malaysia's presence at OEWG and UN GDC talks
Cybercrime	PDRM	Address transnational digital crime and surveillance frameworks	Coordinate with regional and global enforcement, especially private-sector threat sharing. Formalise framework for public-private threat intelligence exchanges with telcos, platforms, and cybersecurity vendors
Cyber risk management	CyberSecurity Malaysia, NACSA	Identify systemic technological risks, especially those involving platform infrastructure	Support regional tech contingency planning and resilience drills through expanding the National Cyber Drill (X-Maya). Potentillay develop a critical tech infrastructure risk register with cross-agency inputs.
AI governance	NAIO, MOSTI, MOFA	Lead Malaysia's engagement on global AI ethics, safety and governance	Shape contributions to GPAI, UNESCO AI Ethics and other global frameworks

Table 5: Author's mapping of the CDAF-D+ pillars for institutional domain for Malaysia's tech diplomacy.

The aim of each pillar is not to manage general digital policy but to serve as a guide on how Malaysia could shape and engage the trajectory of technological development through tech diplomacy. As an example, MOFA would not merely represent Malaysia's digital rights but act as an active agent in negotiating and influencing how AI frameworks, cybersecurity norms and platform governance standards are defined. Similarly, MDEC and MCMC's industry-facing work would be strategic in building long-term partnerships with tech companies and regulatory consortia.

Image 1 illustrates Malaysia's strategic and institutional pathways for operationalising the CDAF-D+ model of tech diplomacy. It maps the principal entities responsible for different domains of technology governance and highlights their respective mandates, areas of international engagement and coordination linkages. Rather than implying a single chain of command, the framework provides a blueprint for how domestic capabilities can be aligned with external responsibilities across a distributed ecosystem of specialised agencies.

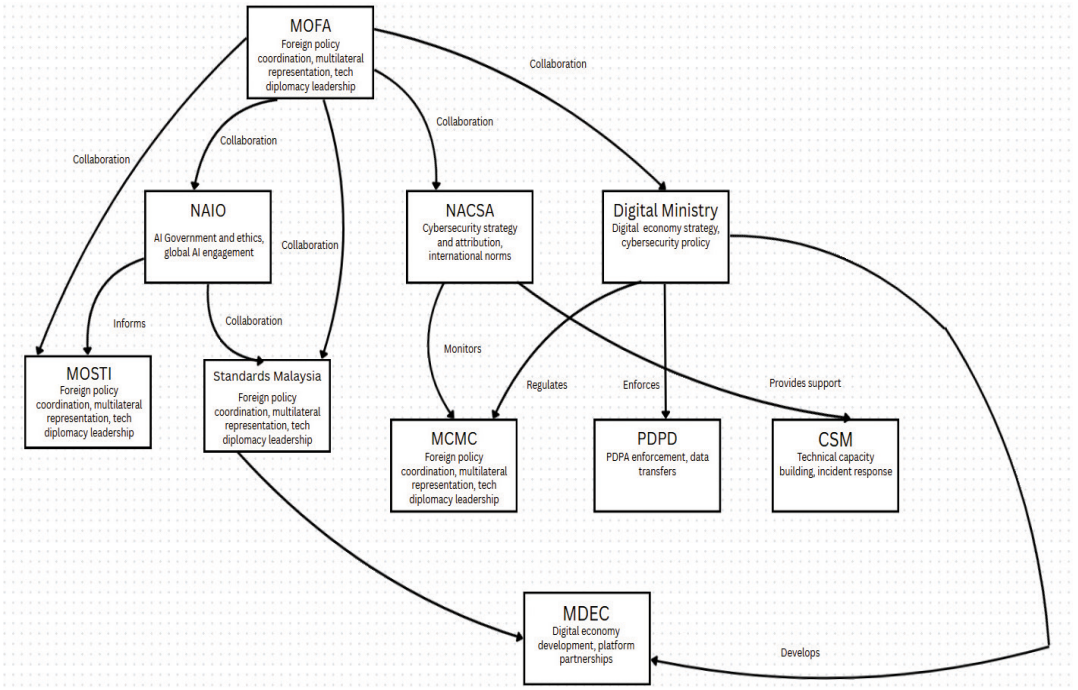

Image 1: Malaysia's strategic and institutional pathways for operationalising the CDAF-D+ model for tech diplomacy, created by author.

To avoid misinterpretation of institutional mandates, it is important to clarify that Malaysia's technology governance architecture is decentralised. While MOFA plays a coordinating and representational role in multilateral forums, it does not serve as the exclusive channel for engagement with private technology actors. Agencies, such as MDEC, MCMC, PDPD, NAIO, Standards Malaysia and NACSA each maintains direct partnerships and regulatory relationships with the private sector.

CyberSecurity Malaysia, as the technical arm under NACSA, provides operational support and capacity building but does not lead attribution or norms negotiation, which falls under NACSA's remit. The inclusion of Standards Malaysia is critical, as it serves as Malaysia's primary liaison to the ISO and IEC platforms and works alongside MDEC and other bodies to localise and adapt standards. This model reflects a deliberate strategy of balancing regulatory specialisation with coordinated foreign policy alignment, ensuring that Malaysia's engagement in global technology governance remains responsive, credible and feasible.

Malaysia also has an opportunity to shape the global architecture of AI governance through active participation in the United Nations' newly launched governance mechanisms. In 2025, the UN established two major initiatives, the Global Dialogue on AI Governance and Independent International Scientific Panel on AI, to catalyse inclusive and multistakeholder engagement on the future of AI governance. These efforts were inaugurated at a high-level UN General Assembly meeting, marking the first time all 193 member states were given an opportunity to co-shape global AI rules. The initiatives aim to address a growing regulatory vacuum: as AI capabilities scale rapidly, 118 countries still lack representation in any major international AI governance forum.

Malaysia is well positioned to contribute substantively to these efforts, particularly in algorithmic transparency, ethical alignment and cross-border data governance. Participation would reinforce Malaysia's credibility as a Global South voice advocating for development-oriented, inclusive AI norms. By strategically linking NAIO, MOFA, and domestic research and policy institutions, Malaysia can demonstrate both internal policy coherence and external leadership. This engagement also aligns with broader global shifts towards trustworthy AI ecosystems, now recognised as essential for enabling safe, inclusive and sustainable AI deployment.[43] Active involvement in these forums would strengthen Malaysia's voice in shaping the rules of global AI governance, while enhancing domestic institutional readiness and multilateral credibility.

The stakeholder mapping and framework visualisation reinforces the importance of having clearly defined institutional roles and structured coordination mechanisms. By mapping governmental agencies against the CDAF-D+ pillars, Malaysia can adopt a whole-of-government approach that aligns domestic capabilities with international engagement priorities. Crucially, this framework integrates existing national policy instruments, such as the MyDigital Blueprint, National AI Roadmap and sectoral regulatory mandates into a coherent foreign policy strategy. This approach ultimately streamlines capabilities and avoids the need to reinvent the wheel, ensuring that established expertise and institutional mandates can be mobilised effectively.

To operationalise this model, Malaysia should consider embedding tech diplomacy coordination within existing inter-ministerial structures. The National Cybersecurity Committee, which already convenes cross-agency actors on digital risk, and National Digital Economy and 4IR Council, which oversees strategic digital transformation initiatives, are ideal platforms for monitoring CDAF-D+ implementation. Embedding

tech diplomacy functions into these bodies could elevate Malaysia's preparedness to engage global partners, tech multinationals and norm-setting platforms in a proactive, structured way.

The CDAF-D+ model is a proposed framework to operationalise tech diplomacy at the national level by aligning Malaysia's institutional architecture with the evolving realities of global technology governance. It maps critical domains, such as AI ethics, platform governance, cybersecurity and cross-border data flows, against responsible agencies to enable a coordinated diplomatic response. All recommended actions in the revised CDAF-D+ pillar mapping are designed to leverage on existing Malaysian institutions, avoiding the need to create new bureaucratic structures.

By anchoring initiatives within ASEAN platforms and regional frameworks, Malaysia can build soft power and enhance its credibility through collective multilateral engagement. At the global level, alignment efforts focus on Malaysia's current memberships in organisations, such as OECD, ITU and UNESCO, as well as ongoing bilateral and industry partnerships, including those facilitated through MyDigital. Crucially, the strategy emphasises pilotable and scalable actions – such as cross-border data sandboxing, regional cyber drills and the appointment of tech attachés – that can deliver immediate diplomatic value while remaining within the bounds of Malaysia's resource capabilities.

5 Recommendations

Ideally, the state needs to operate as both a convenor and a strategic partner to actors. This means intervening where necessary to preserve sovereignty and public interest but also co-creating regulatory environments that support innovation and attract investment. To move beyond ad hoc coordination and build a resilient national tech diplomacy capability, Malaysia must treat the CDAF-D+ model not as a checklist but as a living framework guiding continuous institutional development and alignment.

The following recommendations outline practical steps to operationalise this approach:

a. Clearly delineated institutional mandates for each domain of tech diplomacy, ensuring that responsibilities for engagement, standards development and cross-border negotiation are explicitly assigned and updated regularly.

b. Aligning national policy with diplomatic objectives, such as digital sovereignty and cross-border data flows, including integrating technology engagement into MOFA's bilateral and multilateral strategy documents and linking domestic regulatory agendas to foreign policy priorities, such as digital sovereignty and cross-border data flows.

c. Deploying digital envoys to priority sites for digital multilateralism and tech industry engagement, such as Geneva and San Francisco, as well as regional ASEAN forums to build sustained relationships with both states and leading technology companies. These attachés can sustain institutional memory, signal intent and serve as bridges between domestic regulators and international actors.

d. Integrating technology engagement into MOFA's foreign policy planning and bilateral or multilateral strategy documents.

e. Developing a specialised tech diplomacy track within its administrative and diplomatic service or a training partnership with local universities and policy institutes to build capacity in AI governance, platform regulation and standards diplomacy.

f. Leverage on existing inter-ministerial platforms, such as National Cybersecurity Committee and National Digital Economy and 4IR Council to coordinate strategies across agencies and monitor the implementation of tech diplomacy initiatives.

g. Develop a national tech diplomacy scorecard and monitoring framework to track Malaysia's engagement with technology companies, assess progress across each CDAF-D+ pillar, and evaluate its influence in shaping global norms and standards over time.

h. Foster public-private collaboration by partnering with technology companies and industry associations as stakeholders in foreign policy, and by establishing regular dialogues and joint working groups to anticipate emerging governance challenges.

This would ensure that Malaysia is not just prepared for emerging tech challenges but also positioning itself as a rule-maker.

6 Further research avenues

While this research note centres on Malaysia's national tech diplomacy architecture, the strategic potential of the CDAF-D+ model extends beyond national borders. As a digitally proactive member of ASEAN, Malaysia is well positioned to serve as a first mover and convenor for advancing a regional approach to tech diplomacy. The CDAF-D+ framework offers a flexible template for strengthening ASEAN's collective voice in global technology governance.

Future research could examine how CDAF-D+ might be adapted across ASEAN member states to enable coordinated diplomatic stances in key multilateral forums, such as the United Nations, UNESCO or the OECD's digital economy workstreams. This could involve developing regionwide engagement principles on cross-border data governance, AI ethics and platform accountability. This makes the model not only a governance framework but also a diplomatic strategy to bridge national ambition with regional opportunities.

That said, operationalising a regional tech diplomacy strategy is not without its hurdles. ASEAN's consensus-based decision-making model, varying levels of digital maturity across member states and entrenched norms of national sovereignty complicate efforts towards collective external representation. Research should thus explore how tech diplomacy functions, such as shared standard-setting dialogues, joint attaché placements, or interoperability testbeds, could be embedded into existing ASEAN mechanisms (e.g. ADGMIN, AMTC and ASEAN Digital Economy Framework Agreement).

A key research question emerges: how can the CDAF-D+ model be modularised and scaled to facilitate ASEAN's collective diplomatic positioning on emerging technologies? Answering this would require analysing not only technical governance alignment but also the political feasibility of shared foreign policy instruments for digital affairs.

Ultimately, integrating tech diplomacy into ASEAN's architecture could offer a new axis of regional integration, one that empowers the bloc to shape norms, secure digital sovereignty and resist the passive adoption of standards set by external powers. As Malaysia refines its domestic model, there is an opportunity to lead ASEAN towards becoming a more coherent and credible actor in the global digital order.

7 Conclusion

As emerging technologies increasingly underpin global governance, economic influence and societal transformation, the role of diplomacy must evolve accordingly. Malaysia, like many middle-income states, can no longer afford to approach digital engagement as a reactive or siloed exercise. Instead, it must proactively shape the international norms, standards, and platforms that will govern the technologies of the future. Tech diplomacy is not merely a soft power tool or regulatory accessory; it is a strategic necessity.

The CDAF-D+ model presented here offers a practical and adaptable framework to build Malaysia's national tech diplomacy capacity. By mapping critical domains of technology governance, such as AI, data flows, platform accountability and cybersecurity against institutional responsibilities, the model provides a blueprint for whole-of-government coordination aligned with foreign policy objectives. Crucially, this does not require building new agencies from scratch. Instead, it leverages on existing strategies, such as MyDigital Blueprint and National AI Roadmap, and integrates them into a coherent, externally facing posture.

Malaysia's strength lies in its ability to act as both a regional bridge and a credible convener. With clear institutional mandates, sustained inter-agency coordination and targeted international representation, Malaysia can build long-term relationships with global technology actors, shape multilateral norms and position itself as a rule-maker, not merely a rule-taker, in the digital age. The framework also offers a modular foundation for ASEAN-wide collaboration, allowing Malaysia to catalyse regional alignment without sacrificing national sovereignty.

Ultimately, this research note underscores that tech diplomacy is no longer the exclusive domain of technology superpowers. As the governance of technology becomes inseparable from the governance of life, states that fail to shape the rules of engagement risk being shaped by them. For Malaysia, the path forward is clear: build diplomatic muscle in the digital realm, assert strategic agency and anchor national ambitions in a global vision of inclusive, rules-based technology governance.

Endnotes

[1] Nyabola, N. (2018). Digital Democracy, Analogue Politics : How the Internet Era Is Transforming Kenya. London, UK: Zed Books: in association with International African Institute, Royal African Society [and] World Peace Foundation.

[2] Kurbalija, J. and Ittelson, P. (2024). Tech Diplomacy: Actors, Trends, and Controversies. [online] Diplo. Available at: https://www.diplomacy.edu/resource/tech-diplomacy-actors-trends-and-controversies-full-book/.

[3] Berridge, G.R. (2022). Diplomacy. Cham: Springer International Publishing. doi: https://doi.org/10.1007/978-3-030-85931-2.

[4] Klynge, C., Ekman, M. and Waedegaard, N.J. (2020). Diplomacy in the Digital Age: Lessons from Denmark's TechPlomacy Initiative. The Hague Journal of Diplomacy, 15(1-2), pp.185–195. doi: https://doi.org/10.1163/1871191x-15101094.

[5] Bjola, C. and Kornprobst, M. (2025). Studying Tech Diplomacy — Introduction to the Special Issue on Tech Diplomacy. Global Policy. doi: https://doi.org/10.1111/1758-5899.70035.

[6] Kurbalija, J. and Ittelson, P. (2024). Tech Diplomacy: Actors, Trends, and Controversies. [online] Diplo. Available at: https://www.diplomacy.edu/resource/tech-diplomacy-actors-trends-and-controversies-full-book/.

[7] Garcia, E.V. (2022). What is Tech Diplomacy? A Very Short Definition | Beyond the Horizon ISSG. [online] Behorizon.org. Available at: https://behorizon.org/what-is-tech-diplomacy-a-very-short-definition/#.

[8] Mesquita, R. and Victor, R. (2024). War, Words, and Wealth: Exploring the Differences between Cyber, Digital, and Tech Diplomacy. OSF Preprints. [online] doi:https://doi.org/10.31219/osf.io/ms3n9.

[9] The Royal Society and AAAS (2010). New Frontiers in Science Diplomacy Navigating the Changing Balance of Power. [online] pp.11–17. Available at: https://www.aaas.org/sites/default/files/New_Frontiers.pdf.

[10] Ittelson, P. and Rauchbauer, M. (2023). Tech Diplomacy Practice in the San Francisco Bay Area. [online] Available at: https://www.diplomacy.edu/wp-content/uploads/2023/04/TECH-DIPLOMACY-PRACTICE-in-Bay-area-report_US-letter-web-1.pdf.

[11] Schmidt, E. (2023). Innovation Power. Foreign Affairs. [online] 28 Feb. Available at: https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics.

[12] Kurbalija, J. and Ittelson, P. (2024). Tech Diplomacy: Actors, Trends, and Controversies. [online] Diplo. Available at: https://www.diplomacy.edu/resource/tech-diplomacy-actors-trends-and-controversies-fullbook/.

[13] Schmidt, E. (2023). Innovation Power. Foreign Affairs. [online] 28 Feb. Available at: https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics.

[14] Satariano, A. (2019). The World's First Ambassador to the Tech Industry. The New York Times. [online] 3 Sep. Available at: https://www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html.

[15] Australian Government Department of Foreign Affairs and Trade (2016). Ambassador for Cyber Affairs. [online] Australian Government Department of Foreign Affairs and Trade. Available at: https://www.foreignminister.gov.au/minister/julie-bishop/media-release/ambassador-cyber-affairs

[16] Schwab, K. (2024). The Fourth Industrial Revolution: What It Means, How to Respond. Edward Elgar Publishing eBooks, pp.29–34. doi:https://doi.org/10.4337/9781802208818.00008.

[17] Tech Diplomacy (2024). Krach Institute Launches Tech Diplomacy Academy. [online] Krach Institute for Tech Diplomacy. Available at: https://techdiplomacy.org/news/krach-institute-unveils-tech-diplomacy-academy/.

[18] Endert, J. (2024). Generative AI Is the Ultimate Disinformation Amplifier. [online] DW Akademie. Available at: https://akademie.dw.com/en/generative-ai-is-the-ultimate-disinformation-amplifier/a-68593890.

[19] Seiler, G. (2024). Quantum Computing and the Future of Encryption. Scholarly Review Journal, SR Online: Showcase(Winter 2024/2025). doi:https://doi.org/10.70121/001c.127168.

[20] Zwarts, H., Du Toit, J. and Von Solms, B. (2022). A Cyber-Diplomacy and Cybersecurity Awareness Framework (CDAF) for Developing Countries. European Conference on Cyber Warfare and Security, 21(1), pp.341–349. doi:https://doi.org/10.34190/eccws.21.1.226.

[21] Khazanah Nasional Berhad (2024). Moving up the Semiconductor and Advanced Manufacturing Value Chain: Khazanah's Dana Impak Continues Strategic Investments to Enhance Malaysia's Semiconductor Ecosystem | Khazanah Nasional Berhad |. [online] Khazanah.com.my. Available at: https://www.khazanah.com.my/news_press_releases/moving-up-the-semiconductor-and-advanced-manufacturing-value-chain-khazanahs-dana-impak-continues-strategic-investments-to-enhance-malaysias-semiconductor-ecosystem/

[22] Government of Malaysia (2021). Malaysia Digital Economy Blueprint. [online] Available at: https://ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf.

[23] Ministry of Science, Technology and Innovation (2023). Artificial Intelligence Roadmap 2021-2025. [online] Available at: https://mastic.mosti.gov.my/publication/artificial-intelligence-roadmap-2021-2025/.

[24] Birch, M. (2024). Malaysia, the Rising Startup Tiger of Asia. [online] Linkedin.com. Available at: https://www.linkedin.com/pulse/malaysia-rising-startup-tiger-asia-mark-birch-yeghe/

[25] Malaysia Digital Economy Corporation (2022). Malaysia Tech Entrepreneur Programme (MTEP). [online] mdec.my. Available at: https://mdec.my/mtep.

[26] ASEAN Secretariat (2021). ASEAN Digital Master Plan 2025. [online] Available at: https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf.

[27] ASEAN Secretariat (2022). ASEAN Cybersecurity Cooperation Strategy (2021-2025). [online] Available at: /https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

[28] Permanent Mission of Malaysia to the United Nations New York (2021). Sixth Substantive Session of the UNOEWG on ICT Security 2021-2025. [online] Kln.gov.my. Available at: https://www.kln.gov.my/web/usa_un-new-york/news-from-mission/-/blogs/statement-sixth-substantive-session-of-the-oewg-on-security-of-and-in-the-use-of-information-and-communication-technologies-2021-2025

[29] The Star (2024). Local Military Industry Players Urged to Adopt AI. [online] The Star Online. Available at: https://www.thestar.com.my/news/nation/2024/09/10/local-military-industry-players-urged-to-adopt-ai

[30] International Organisation for Standardization (2017). ISO 25237:2017. [online] ISO. Available at: https://www.iso.org/standard/63553.html.

[31] Bjola, C. and Kornprobst, M. (2025). Studying Tech Diplomacy—Introduction to the Special Issue on Tech Diplomacy. Global Policy. doi:https://doi.org/10.1111/1758-5899.70035.

[32] Zwarts, H., Du Toit, J. and Von Solms, B. (2022). A Cyber-Diplomacy and Cybersecurity Awareness Framework (CDAF) for Developing Countries. European Conference on Cyber Warfare and Security, 21(1), pp.341–349. doi:https://doi.org/10.34190/eccws.21.1.226.

[33] Kurbalija, J. and Ittelson, P. (2024). Tech Diplomacy: Actors, Trends, and Controversies. [online] Diplo. Available at: https://www.diplomacy.edu/resource/tech-diplomacy-actors-trends-and-controversies-full-book/.

[34] Suruga, T. and Tanaka, A. (2023). Southeast Asia's Digital battle: Chinese and U.S. Big Tech Face off over $1tn Market. [online] Nikkei Asia. Available at: https://asia.nikkei.com/Spotlight/The-Big-Story/Southeast-Asia-s-digital-battle-Chinese-and-U.S.-Big-Tech-face-off-over-1tn-market

[35] Department of Foreign Affairs and Trade (2020). Australia-Singapore Digital Economy Agreement. [online] Australian Government Department of Foreign Affairs and Trade. Available at: https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement.

[36] New Zealand Ministry of Foreign Affairs and Trade (2020). Overview of the DEPA. [online] New Zealand Ministry of Foreign Affairs and Trade. Available at: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/overview

[37] Ministry of Trade and Industry (2024). WTO Joint Statement Initiative on Electronic Commerce Achieves Stabilised Text. [online] Mti.gov.sg. Available at: https://www.mti.gov.sg/Newsroom/Press-Releases/2024/07/WTO-Joint-Statement-Initiative-on-Electronic-Commerce--achieves-stabilised-text

[38] Kurbalija, J. (2025). Advancing Swiss AI Trinity: Zurich's Entrepreneurship, Geneva's Governance, and Communal Subsidiarity - Diplo. [online] Diplo. Available at: https://www.diplomacy.edu/blog/advancing-swiss-ai-trinity-zurichs-entrepreneurship-genevas-governance-and-communal-subsidiarity/

[39] Greater Zurich Area (2025). Higher BigTech Density than Silicon Valley: Welcome to Greater Zurich. [online] Greater Zurich Area. Available at: https://www.greaterzuricharea.com/en/news/higher-bigtech-density-silicon-valley-welcome-greater-zurich?fbclid=IwY2xjawMTXhxleHRuA2FlbQIxMABicmlkETFPWUxZWVp3MDZBdFUzRFJ0AR5dCMxCNLGLglfFBd1fEH94USQt508DgqNN23NdhjqoopqWSbPOUe96GFIlGA_aem_H6OFp0SWQGpUe2uWLiv4UA

[40] Mottaz, P. (2022). The Geneva Science and Diplomacy Anticipator Is Putting Science on the Global Diplomatic Agenda. [online] Mailchi.mp. Available at: https://mailchi.mp/thegenevaobserver.com/crowdfunding-drones-to-help-ukraine.

[41] Ministry of External Affairs (2025). New, Emerging & Strategic Technology (NEST) Division: Brief about the NEST Division. [online] www.mea.gov.in. Available at: https://www.mea.gov.in/Images/CPV/BriefNestDivision.pdf.

[42] Singh, A. (2023). The 'Tech' Moment in India's Foreign Policy. [online] South Asian Voices. Available at: https://southasianvoices.org/the-tech-moment-in-indias-foreign-policy/.

[43] Elliott, D. (2025). The UN's New AI Governance Bodies Explained. [online] World Economic Forum. Available at: https://www.weforum.org/stories/2025/10/un-new-ai-governance-bodies/.

INSTITUTE OF STRATEGIC &
INTERNATIONAL STUDIES
(ISIS) MALAYSIA

Address 1, Persiaran Sultan Salahuddin,
50480 Kuala Lumpur, Malaysia
Phone 603 2693 9366
E-mail info@isis.org.my

www.isis.org.my | ISIS_MY

ISISMalaysia | isis-malaysia

isis_malaysia