Countering the Hydra

A proposal for an Indo-Pacific hybrid threat centre

Dr Lesley Seebeck, Emily Williams and Dr Jacob Wallis

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 60/2022

About the authors

Dr Lesley Seebeck is an independent consultant and an honorary professor at the Australian National University. Dr Seebeck was the CEO of the Cyber Institute, ANU, from 2018 to 2020, and has undertaken the roles of Chief Investment and Advisory Officer at the Digital Transformation Agency (2017-2018) and Chief Information Officer at the Bureau of Meteorology (2014-2017). In March 2017, she was recognised as Federal Government CIO of the Year. Dr Seebeck has extensive experience in strategy, policy, management, budget, information technology and research roles in the Australian Public Service, industry and academia. She has worked in the Departments of Finance, Defence, and the Prime Minister and Cabinet, the Office of National Assessments, and as an IT and management consultant in private industry, and at three universities. Dr Seebeck has a PhD in information technology, an MBA, a Masters in Defence Studies and a Bachelor's degree in Applied Science (Physics).

Emily Williams is a research assistant and administrative officer with ASPI's International Cyber Policy Centre. She has a Bachelor of Arts in Politics and International Relations and is currently completing a Masters of International Affairs with King's College London. She has previously worked with the FCDO at the British Embassy in Beijing.

Dr Jacob Wallis is Head of Program, Information and Operations and Disinformation with ASPI's International Cyber Policy Centre.

Acknowledgements

With special thanks to Danielle Cave, Baani Grewal, Fergus Hanson, Michael Shoebridge, Justin Bassi, Jamie Gaida, Stephan Robin and Hannah Green.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies and issues related to information and foreign interference and focuses on the impact those issues have on broader strategic policy. The centre has a growing mixture of expertise and skills, including teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity-building, satellite analysis, surveillance and China-related issues. The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The centre enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and the Indo-Pacific region, the ICPC has a capacity-building team that conducts workshops, training programs and large-scale exercises for the public and private sectors. We thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre, contact: icpc@aspi.org.au

Important disclaimer

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published June 2022. ISSN 2209-9689 (online). ISSN 2209-9670 (print).
Cover image: Alex Santafe.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

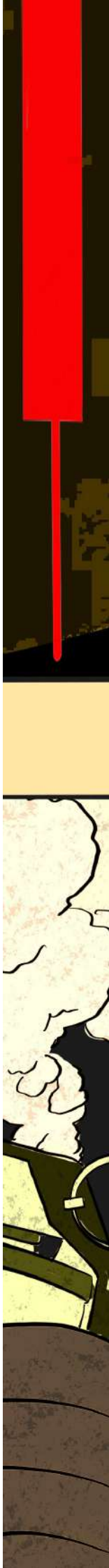
INTERNATIONAL CYBER POLICY CENTRE

Funding for this report was provided by the UK Foreign, Commonwealth & Development Office.

Countering the Hydra

A proposal for an Indo-Pacific hybrid threat centre

Dr Lesley Seebeck, Emily Williams and Dr Jacob Wallis



Policy Brief
Report No. 60/2022

Contents

What's the problem?

Enabled by digital technologies and fuelled by geopolitical competition, hybrid threats in the Indo-Pacific are increasing in breadth, application and intensity. Hybrid threats are a mix of military, non-military, covert and overt activities by state and non-state actors that occur below the line of conventional warfare. The consequences for individual nations include weakened institutions, disrupted social systems and economies, and greater vulnerability to coercion—especially from revisionist powers such as China.

But the consequences of increased hybrid activity in the Indo-Pacific reach well beyond individual nations. The Indo-Pacific hosts a wide variety of political systems and interests, with multiple centres of influence, multiple points of tension and an increasingly belligerent authoritarian power. It lacks the regional institutions and practised behaviours to help ensure ongoing security and stability. And, because of its position as a critical centre of global economic and social dynamism, instability in the Indo-Pacific, whether through or triggered by hybrid threats, has global ramifications.

Because hybrid threats fall outside the conventional frameworks of the application of state power and use non-traditional tools to achieve their effects, governments have often struggled to identify the activity, articulate the threat and formulate responses. Timeliness and specificity are problematic: hybrid threats evolve, are often embedded or hidden within normal business and operations, and may leverage or amplify other, more traditional forms of coercion.

More often than not, hybrid threat activity is targeted towards the erosion of national capability and trust and the disruption of decision-making by governments—all of which reduce national and regional resilience that would improve security and stability in the region.

What's the solution?

There's no silver-bullet solution to hybrid threats; nor are governments readily able to draw on traditional means of managing national defence or regional security against such threats in the Indo-Pacific.

Because of the ubiquity of digital technologies, the ever-broadening application of tools and practices in an increasing number of domains, it's evident that policymakers need better and more timely information, the opportunity to share information and insights in a trusted forum and models of how hybrid threats work (we provide one here). Exchange of information and good practice is also needed to help counter the amorphous, evolving and adaptive nature of hybrid threats.

We propose the establishment of an Indo-Pacific Hybrid Threat Centre (HTC, or the centre) as a means of building broader situational awareness on hybrid threats across the region.[1] Through research and analysis, engagement, information sharing and capacity building, such a centre would function as a confidence-building measure and contribute to regional stability and the security of individual nations.

While modelled on the existing NATO–EU Hybrid Centre of Excellence (CoE) in Finland, the centre would need to reflect the differences between the European and Indo-Pacific security environments. Most notably, that includes the lack of pan-regional Indo-Pacific security institutions and practice that the centre could use. There are also differences in the nature and priorities assigned to threats by different countries: the maritime domain has more influence in the Indo-Pacific than in Europe, many countries in the region face ongoing insurgencies, and there's much less adherence to, or even interest in, democratic norms and values.

That will inevitably shape the placement, funding, and operations of an Indo-Pacific HTC. A decentralised model facilitating outreach across the region would assist regional buy-in. Partnership arrangements with technology companies would provide technical insight and support. Long-term commitments will be needed to realise the benefits of the centre as a confidence-building measure. The Quad countries are well positioned to provide such long-term commitments, while additional support could come from countries with experience and expertise in hybrid threats, particularly EU countries and the UK.

As with the NATO–EU Hybrid CoE, independence and integrity are paramount. That implies the positioning of the Indo-Pacific HTC core in a strong democracy; better still would be the legislative protection of its operations and data. Accordingly, we propose scoping work to establish policy approval, legislative protection and funding arrangements and to seed initial research capability and networks.

Introduction

Hybrid threats are a mix of military and non-military, covert and overt activities by state and non-state actors that occur below the line of conventional warfare. Their purpose is to blur the lines between war and peace, destabilise societies and governments and sow doubt and confusion among populations and decision-makers. They deliberately target democratic systems and state vulnerabilities, often leveraging legitimate processes for inimical ends, and typically aim to stay below the threshold of detection, attribution and retaliation.[2] They're the same activities that the Australian Government attributes to the 'grey zone', involving 'military and non-military forms of assertiveness and coercion aimed at achieving strategic goals without provoking conflict.'[3]

Hybrid threats are increasingly of concern to governments as they grapple with the effects of digital technologies, Covid-19 and an increasingly tense geopolitical environment. Ambiguous, evolving, at the intersection of society, commerce and security, and transnational in character, hybrid threats challenge and undercut 'normal' conceptions of security. Unmet, they stoke division and anxiety in societies and states. They threaten to erode national security, sovereignty and societal resilience, leaving nations and their people vulnerable to coercion, particularly by authoritarian states and criminal elements.

The immediate targets of motivated hybrid activity are typically non-traditional, in the sense that government security apparatuses aren't expected to manage and repulse them. Hybrid activity takes advantage of other, easier targets and means of generating confusion and disruption at the nation-state level: individuals may be targeted for repression or assassination; fishing vessels harassed; intellectual property stolen; commercial advantage pillaged; researchers and journalists intimidated; ethnic communities hijacked; and elites co-opted for corrupt ends.

The Indo-Pacific region is particularly vulnerable. For example, it lacks the more practised security frameworks, cooperative mechanisms and understandings present in Europe. There's little shared awareness and understanding of the nature and consequences of hybrid threats. The region is also especially economically and demographically dynamic and socially diverse, featuring a number of competing political systems and institutions.

That offers both challenge and opportunity. In this paper, we consider the nature of hybrid threats, explore the threat landscape in the Indo-Pacific, turn our attention to the potential 'fit' of an Indo-Pacific HTC and make recommendations for the way forward.

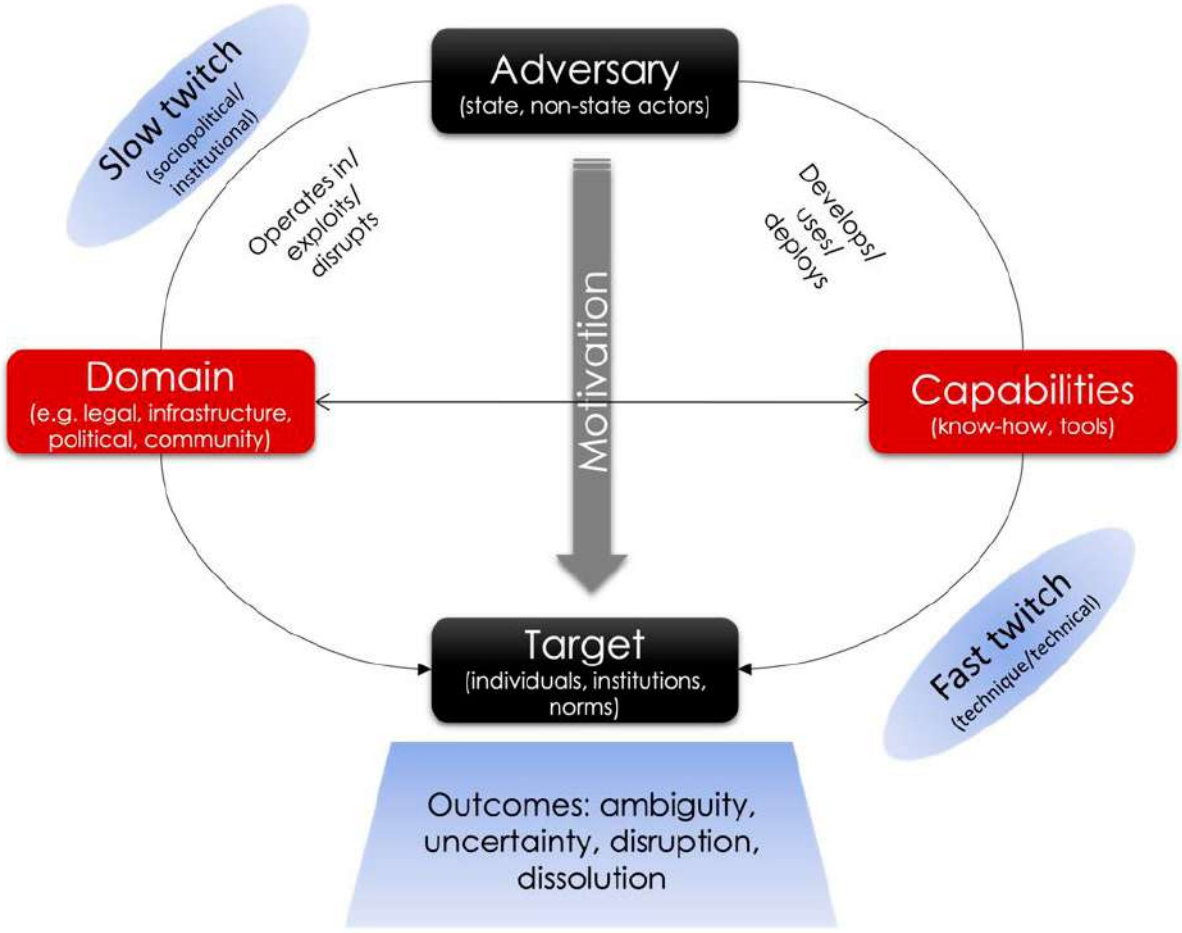
A number of the thoughts and insights incorporated in this paper emerged during ASPI's consultations with governments, businesses and civil society groups in the Indo-Pacific, as well as in Europe and the UK. We thank those respondents for their time and insights.

The nature of hybrid threats

The international security environment is increasingly contested and complex. Traditional forms of contest—conventional militaries and the tools of statecraft, such as diplomacy—are supplemented by a broadening, evolving range of means of exerting influence, coercion and disruption. Those factors often exploit technology, social inequalities and other sources of disruption, and often use existing, legitimate measures to obscure or create vulnerabilities.

A simple model helps illustrate the complexity and dynamic nature of hybrid threats and the challenge of managing them (Figure 1). The logic flow is as follows: driven by a particular motivation to achieve advantageous outcomes of ambiguity, uncertainty, disruption or dissolution in the target state, an adversary will use, exploit or disrupt a particular domain using a set of capabilities that it has developed or deployed.

Figure 1: A model of hybrid threat behaviour



Source: Diagram created by the authors.

Adversaries may be nation-states, non-state actors or partnerships of both. The focus here is on the use of hybrid or non-conventional means as a tool of the state. Non-state actors or proxies, such as hackers, propagandists for hire and private militias, may be used to obscure or directly support nation-states' aims.[4]

Much of policymakers' attention has been on the capabilities used—tools and techniques such as cybertechnologies, social media disinformation and 'wolf warrior' diplomacy. Other tools include investment, the co-optation of elites and political parties, corruption, theft, coercion and intimidation, and weaponised legal disputes.[5] These are fast-changing behaviours facilitated by technical platforms and skill sets—the same tools, attitudes and behaviours that underpin the digital economy, enable innovation and facilitate free speech and political action.

Increasingly, the domains in which hybrid threat activity occurs are gaining attention. The Hybrid CoE lists 13 instruments of national power,[6] all of which are areas in which hybrid tools may be employed or directed. The number reflects the scope of the challenge, the complexity of nations and the need for a level of granularity that enables targeted policy responses. That's also evident in other national responses to hybrid activities. For example, Australia's *Security of Critical Infrastructure Act 2018* enumerated 11 sectors as critical infrastructure.[7] Many, such as universities, food-distribution networks and data storage and processing, hadn't previously been considered as meeting those criteria.

Another insight that may be drawn from the model in Figure 1 is that the adversary/domain axis represents slower changing behaviours, often requiring sociopolitical and economic drivers for change. For example, critical infrastructure is shaped by demographics, government regulation and institutional funding, while standards development is a slow, institution-driven process. Moreover, nation-state adversaries are longstanding, patient and persistent.

Table 1 sets out common hybrid threats, many of which were identified during consultations for this paper. Some, if viewed in isolation and conducted non-clandestinely, wouldn't raise strategic concerns or could be managed using the 'normal' tools of defence and statecraft.

Table 1: Common hybrid threats

Type of activity	Definition
Abduction, detainment and disappearance	The Chinese state kidnaps and forcibly repatriates people whom it considers to be Chinese nationals, including from Western nations, and forcibly detains citizens from other countries, including as 'hostage diplomacy'.[8]
Assassination	Since 2008, North Korea has been linked to at least six attempted and two successful assassinations.[9] Assassination has been used, or attempted, by the Russian regime against journalists, opposition figures, dissidents and former intelligence officers.[10]
Co-optation	Authoritarian regimes and other hybrid threat actors may seek to co-opt elites, decision-makers or community groups in order to suppress dissent, subvert policy, entrench corruption, hide their activities or weaken democratic norms and institutions.
Coercive diplomacy	Coercive diplomacy can be defined as non-militarised coercion or the use of threats of negative actions to force the target state to change its behaviour.
Corruption	Corruption has both physical and psychological components. The physical aspects involve the diversion of funds, resources or capability, including to the threat actor, for illegitimate ends. The psychological component weakens trust in and the integrity and purpose of processes, systems and institutions, and compromises targets and accomplices.
Cyberattacks	Cyberattacks are unwelcome attempts to steal, expose, alter, disable or destroy information through unauthorised access to computer systems.

Digital divide	As flagged during consultations conducted for this report, the digital skills and literacy divide between different areas in the Indo-Pacific constitutes a vulnerability that may be exploited by threat actors as well as a potential impediment to coherent responses by national governments and at the regional level.
Disinformation	Disinformation is the intentional dissemination of false or deliberately biased, exaggerated, distorted or unbalanced information with the intent of advancing political or geostrategic objectives.
Economic coercion	Economic coercion or sanctions are damaging economic behaviour by an initiating government directed against a target government. Examples include blocking trade and reducing market access through politically motivated administrative measures.
Espionage	Traditional espionage and counterespionage have been enhanced through technology, and cyber and signals intelligence enables access to national systems and commercial secrets. Face-recognition technologies facilitate the tracking of people across borders, and 'internet of things' devices enable real-time surveillance.
Foreign interference	Foreign interference is covert influence attempting to shape decision-making, confuse debate and cloud, complicate and slow decision-making.
Human rights abuses	Human rights abuses are direct or indirect violations of rights set out in the UN Universal Declaration of Human Rights. Such abuses often exploit weaknesses in institutions and offer vulnerabilities that can be exploited by threat actors.
Information operations	Linked to disinformation, information (or influence) operations involve the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over the adversary.
Intellectual property theft	Intellectual property theft involves robbing people or companies of their ideas, research, inventions and creative expressions.
Lawfare	The introduction and use of international and domestic laws to deter criticism and gain support while managing repercussions from military action.
Militarisation of contested islands	Artificial islands in the South China Sea have now been fully militarised and armed with anti-ship and anti-aircraft missile systems, laser and jamming equipment and fighter jets.
Mercenaries and private contractors	The use of private contractors for the purpose of armed force, illicit activities and hacking enables plausible deniability.

While civil society, its infrastructure and activities may be on the front line of hybrid threats, the broader purpose of hybrid activity is to introduce ambiguity into decision-makers' understanding of their environment, drivers and priorities. Decision-making becomes more uncertain and easier to disrupt, complicate and slow, exacerbating information and speed asymmetries to the advantage of the attacker. Government becomes increasingly reactive. Often, government responses may protect elites and neglect the effect of those responses on the more vulnerable among the general public and in the wider economy. Trust in government institutions erodes, national purpose and resolve are disrupted, and the institutions of state, the broader economy and society that may facilitate a response are crippled.

That assessment aligns with definitions recognising that hybrid operations are directed not at the military, but at people and populations.[11] However, confusion may arise when disruptive activities are parallel to, or obscured by, legitimate activities, such as commercial competition, the sharing and contest of ideas, research and publication of methods and outcomes, and technological

innovation. Further, some activities, such as whistleblowing, vulnerability research and stress-testing are fundamental to resilient systems and societies, and yet may threaten the interests of some in institutions.

Consequently, motivation and intent define whether an activity is a threat. Typically, the outcome of an attack or activity is uncertainty, ambiguity or disruption. Ultimately, however, the adversary is seeking to undermine or counter the values and institutions of the targeted state, fraying its fabric and eroding its capability.

Understanding, managing and denying hybrid threats requires us to appreciate all aspects in the model and adapt the application of the model as behaviours emerge and change. A focus on a single part (such as the 'fast twitch' of cyber or disinformation campaigns on social media) or on a single adversary risks missing the overall, systems-level effects and the development of misaligned, even harmful solutions. Nor is there a silver bullet ready to resolve the problem at a systems-of-systems level, not least because of the continuously evolving, organic nature of actors' intent, targets' responses and threat behaviours.

This is best illustrated through an overview of the threat landscape in the Indo-Pacific, after which we consider how an Indo-Pacific HTC could assist governments and communities to understand and manage hybrid threats, and how that in turn contributes to regional stability and resilience.

The threat landscape

In this section, we provide a sketch of the hybrid threat landscape in the Indo-Pacific. The landscape is increasingly messy and difficult to navigate, given the difficulty in attributing hybrid threat actions by actors in the region. We first identify the primary actors in the region, before using case studies to demonstrate the integrated use of tools to achieve certain objectives. We then identify key trends and highlight areas for further research.

Actors and trends

From a review of the literature, three primary threat actors in the Indo-Pacific region emerge: China, North Korea and groups affiliated with Islamic State (IS). Russia is also active in the region, but further research is needed to determine the extent to which Russian activity can be defined as 'hybrid threat' activity. Other actors in the region have the capability to participate in these activities, but we're not yet seeing those actors conducting such activities at scale or with persistence. For example, Thailand's use of accusations of fake news[12] and the Philippines' use of troll farms[13] show that those countries have hybrid capabilities but lack the means of coercion or power projection inside and against other states. The distinction drawn here is the use of hybrid threats against targets other than domestic audiences, and situations in which conclusions about intent may be made.

That said, hybrid activity against domestic targets inherently weakens the capacity, resolve and resilience of civil society and economic prosperity in those nations, so that can't be disregarded in the longer term. Moreover, the repression of domestic populations can have spillover effects into other countries.

That's apparent in the context of violent jihadist groups. The ongoing presence and disruptive activity of such groups in Southeast Asia remains a major concern to those countries, not least because the activities of the groups and the consequences of those actions generate additional vulnerabilities and threaten state resilience. That said, it's important to note that hybrid threats and terrorism aren't the same. Ambiguity is central to hybrid threats, but the perpetrators of terrorist acts often claim responsibility for their acts.[14] It's the use of hybrid tools and tactics by nation-states and violent jihadist groups that's the focus here.

China

The strategic outlook of the Chinese Communist Party (CCP) on hybrid threats differs from the conceptualisation of hybrid threats in the West. The CCP uses the lens of 'Three Warfares'[15] in its approach:

- Broadly, *media warfare* is the use of any and all types of media to influence public opinion and gain support from domestic and international audiences for strategic objectives and military action.
- *Psychological warfare* is the use of propaganda, deception, threats and coercion to affect the enemy's ability to understand situations and make decisions. Information operations, manipulation and disinformation campaigns fall under this heading.
- *Legal warfare* (commonly referred to as 'lawfare') is the introduction and use of international and domestic laws to deter criticism and gain support while managing repercussions from military action.

First introduced in the 2003 document 'Political Work Guidelines of the People's Liberation Army', the Three Warfares framework draws on the 1999 book *Unrestricted warfare* written by two senior People's Liberation Army (PLA) officers. That book discussed the consequences of technology for a 'revolution' in military strategy, and there are indeed echoes of Sun Tzu's *The art of war* in the Three Warfares framework,[16] in as much as it emphasises the desirability of waging and winning war without resorting to armed conflict. As China scholar Peter Mattis has observed, the Three Warfares approach is about protecting and consolidating political power, rather than military capability.[17]

The Three Warfares framework broadly encapsulates the breadth of tools used by the Chinese state, but their use in the pursuit of its objectives can be more nuanced, as illustrated in the case studies in the next section. For example, psychological warfare encompasses a wide range of activities, including the building of military bases and the establishment of permanent presences in contested areas. In contrast to Western thinking, the CCP's Three Warfares doesn't distinguish between those military activities, which are more akin to traditional 'kinetic' warfare, and information operations.

It would be misleading to think that Western states have no understanding or historical expertise in hybrid activities. For example, the UK and the US developed particular hybrid capabilities during World War II against the Axis powers and the Cold War against the Soviet Union. That historical experience is often overlooked by current policymakers and analysts, who then conclude that Chinese or Russian state use of hybrid threats is somehow unique, novel and hard to come to terms with.

Similarly, other distinctions within the conceptualisation of 'hybrid threats' may be blurred in the Indo-Pacific, with consequences for the emphasis and priority that countries (in this instance, China) place on different tactics. To quote from Sun Tzu: 'If you know the enemy and know yourself, you need not fear the result of a hundred battles.'

China is the most widely reported actor in the region, when assessing incidents reported in major media outlets. That's not surprising, given China's resources, its status as the largest trading partner with all countries in the region and the subsequent impact that its actions have, all of which give it a larger representation in the available data. But it also reflects purpose and intent: Chinese actions are hardly coincidental. They tend to be orchestrated and directed by central CCP authorities and then disseminated and amplified by multiple entities in the Chinese system.

Nor does this mean that other countries or actors, such as North Korea, Russia or IS-affiliated groups, aren't conducting operations, but merely that in those cases the data isn't as readily accessible.

Further research, conducted by a dedicated HTC, is needed to better delineate and assess the full spectrum of threat activity and the broader hybrid landscape.

In news cycles, it's possible to identify increased cyberattacks and hacking activity targeting agencies of government with which China has territorial disputes following major events in the South China Sea. Similarly, economically coercive methods are employed following policy announcements that may complicate or frustrate the Chinese state's pursuit of its objectives.

The impact of different hybrid methods is difficult to quantify. Many such operations are conducted at scale and with persistence and have longer term consequences. For example, one Taiwan-based think-tank analyst reported that China is attacking Taiwan with up to 2,400 separate pieces of

disinformation every day.[18] Such long-term campaigns are insidious: they chip away at established positions and erode trust in targeted governments.

Cyberattacks, maritime coercion and economic coercion are the primary escalatory measures used by China against targets that are participating in activities contrary to the CCP's interests. Their use raises the risks associated with pushing back against Chinese behaviour, such as maritime aggression and territorial expansion in the South China Sea.

However, some of China's economic coercive methods have been counterproductive: Australia has shown resilience in the face of sanctions being levied against eight key exports and has hardened its resolve. It's unclear whether that will result in a reduction of the use of those tactics by China or spur other countries in the region to call out aggressive behaviour. At the least, however, Australia's experience and resilience against those particular hybrid threats from China demonstrate a failure of effect from China's hybrid action. That indicates that there are paths for effectively dealing with such threats.

Online disinformation, which China regularly uses against Taiwan, can reach a large audience because of the pervasiveness of internet use and the common language of the two countries. It may prove less effective in a country with low internet penetration. For example, Solomon Islands has only approximately 28.6% internet penetration[19]; we would expect other hybrid means to be used there, such as influence operations in community groups, economic incentives, diplomatic coercion and the co-optation of elites.[20]

It's also important to note that the accessibility of data on attacks differs according to the individual country's willingness to assess, understand and then call out behaviour. For example, there's a lot of data available from Australia and Taiwan, which makes it seem that those jurisdictions are the largest targets. That could well be the case, but it's likely that many incidents go unreported, given the coercive methods that are deployed against states that do not go public, the less mature legislative frameworks of some states, and less concern over the effects on companies and individuals.

Most hybrid activity incurs comparatively low cost and risk. Cyberattacks and disinformation campaigns have been favoured, especially due to their ease of use, growing sophistication and difficulty in attribution. That said, it's noticeable how quickly Western intelligence agencies were able to identify and attribute Russian cyber activity in the lead-up to the Russian invasion of Ukraine. This is an example of successful counter-hybrid activity that can provide at least one model of success in frustrating the goals of persistent hybrid threat actors.

A key characteristic of hybrid threats in the Indo-Pacific is the dynamic nature of the threats: they oscillate between escalation and de-escalation to remain 'under the radar'. As territorial disputes escalate and as new technologies evolve, we can expect to see more hybrid threat activity occurring in the region.

North Korea

The Democratic People's Republic of Korea has regularly used hybrid threat tactics since the conclusion of the Korean War. Pyongyang uses hybrid tactics to leverage outcomes pertaining to its strategic goals—a direct consequence of its isolation and comparably inferior military and political power.

North Korea's strategic objectives are much more limited than those of China: it aims primarily for regime survival, while profits from its activities are used to fund government priorities.[21] It's an expansionist power insofar as it would like to reclaim South Korean territory and reunify while keeping its governing structure intact (for example, keeping the Kim dynasty in place and not democratising in order to assimilate to South Korea's governance system). Nonetheless, North Korea remains an acute threat to security in the Indo-Pacific.[22]

As an actor, North Korea has proven adept at evolving along with new technologies—surprisingly so, for such an isolated nation. Analysts estimate that North Korea's cyber forces number some 7,000 personnel,[23] including people working on disinformation and supporting criminal activities.[24]

The tactics used by hybrid threat actors differ according to their expertise and resources. North Korea appears to favour cyberattacks coupled with regular testing of ballistic missiles to highlight its capabilities, while stopping short of triggers that would invite further sanctions and direct military confrontation.

Islamic State and IS-affiliated groups

Activities by IS and IS-affiliated groups targeting Indo-Pacific countries, primarily those with larger Muslim populations, have been given impetus by the oppression of the Rohingya and Uyghur communities by the Myanmar and Chinese governments, respectively, and the return to power of the Taliban in a fractured Afghanistan opens further space for this type of extremist actor.

IS declared a holy war against China in July 2014 on the grounds that it was fighting against the persecution of Uyghur Muslims in China's northwest Xinjiang region.[25] Pro-IS Indonesian jihadist groups (estimated to number around 18[26]) subsequently targeted Chinese Indonesians, whom IS doesn't consider to be distinct from Chinese nationals.[27]

IS's rhetoric highlighting the plight of the Uyghurs has slowed since 2017, and that's been interpreted as an effort to avoid provoking China and to help IS achieve its goals elsewhere.[28] However, that hasn't translated into a significant reduction in threat activity in Indonesia, where pro-IS groups were responsible for at least 14 terror attacks between 2016 and 2022. However, of the two attacks in Indonesia in 2021, only one was lethal, and IS stated that it was targeting Christians.[29]

Militant violence remains a concern in the Philippines,[30] and, while other separatist movements in Thailand and Malaysia differ in ideology from IS,[31] IS can be expected to look to exploit the disruption emerging from any conflict. IS and its affiliates also look to exploit disinformation and social media in their campaigns against regional governments and institutions. For example, there are suggestions that pro-IS groups have been responsible for pushing a variety of conspiracy theories asserting Chinese influence over Indonesian leaders.[32]

While IS and IS-affiliated groups are more sporadic and uncoordinated in their attacks in the region, and are thus less effective in achieving their objectives, those groups remain a major security threat to regional nations due to their use of lethal force. Moreover, IS and its affiliates are proving both resilient and adaptive by adopting new tools of influence and coercion as those tools become available.

Russia

Russia warrants mention because of its long practice of using hybrid tools, particularly *maskirovka* (Russian military deception),[33] as well as its deep expertise in hostile cyber activity.

Putin's war in Ukraine has sharpened Russia's focus on Europe. However, Russian efforts at disinformation are more widespread, appealing to audiences in the Indo-Pacific, Africa,[34] the Middle East[35] and Latin America[36] that are disaffected with the West—its effort in India being a case in point[37]. Notably, Russia is being aided and assisted in its disinformation and social media campaigns by China,[38] which is seeking to use the situation in Ukraine to further its own goals.[39]

Russia continues to increase its cyber activity.[40] Although that effort's mainly directed at the US, Europe and especially Ukraine, there are likely to be spillover effects, not least in response to counterattacks,[41] and particularly as criminal elements seek to exploit any disruption.

In the longer term, Russia's efforts to expand its influence in Southeast Asia have been limited, albeit of concern.[42] Its greatest success has been with India, which sees Russian engagement as a means of offsetting China and retaining India's singular position with regard to the West.

Case studies

Case study 1: South China Sea

China's principal objective in the South China Sea is to definitively claim and exercise sovereignty over this large, strategically important maritime space, used by one-third of the global maritime shipping trade.[43] To achieve that objective—including through its refusal to accept the Law of the Sea arbitral tribunal ruling in favour of the Philippines—the CCP has combined a number of hybrid activities.

Building artificial islands

China has built around 28 artificial islands in the South China Sea, some of which are now fully militarised,[44] despite Beijing's 2015 pledge not to do so.[45]

'Little blue men'

Similarly to Russia's use of 'little green men' in Crimea, fishing boats have been used to establish Chinese control of areas in the South China Sea, supported by reserve forces such as the People's Armed Forces Maritime Militia (PAFMM).

From late 2019 to early 2020, more than 50 PRC-affiliated fishing vessels and PAFMM vessels were escorted by China Coast Guard patrol ships in Indonesian-claimed areas in the southern South China Sea.[46]

Fishing and PAFMM vessels are primarily used to 'buzz' US Navy ships and ships of the navies of countries that have territorial claims to the areas that China also claims. While such actions are a means of making China's presence felt rather than engaging in direct confrontation, and providing China with a fiction to dismiss claims of militarisation, they risk escalation.

Military confrontation has occurred, as in 1988, when Chinese troops fired on Vietnamese Navy personnel, who were moving construction material and raising a flag on the Johnson South Reef in the Spratly Islands. Sixty-four Vietnamese soldiers were killed and nine captured.

On 14 March 2022, Vietnam chose to commemorate the anniversary of that battle[47]—a possible signal to the Chinese that the Vietnamese Government is now willing to assert maritime sovereignty over the region despite increasing Chinese provocations.

Economic coercion

At the height of tensions in 2012 over Scarborough Shoal, which is around 150 nautical miles west of the Philippines and over which both China and the Philippines claim sovereignty, China restricted fruit imports from the Philippines.[48] It subsequently offered extended economic cooperation to the Duterte government in exchange for shelving the dispute.[49]

Cyberattacks

Cyberattacks from China increased in intensity and focus following developments in the South China Sea. For example, in April and May 2019, there was an increase in cyber activity targeting the Philippines[50] following Philippines President Duterte's threat that he would send his troops on a 'suicide mission' if Beijing didn't stop harassing a Philippine-claimed island in the South China Sea.[51] FireEye, observing the overall Southeast Asia cyber landscape, found that events in the South China Sea were reflected in 'advanced persistent threat' activity directed at government and military institutions, as well as private companies.[52]

Lawfare

In 2009, China formally introduced a map that included a 'nine-dash' line delineating Chinese territorial claims in the South China Sea. In 2013, the map was updated to include a 10 dash, drawn very close to Taiwan and some Japanese islands that also hadn't traditionally been claimed by China.

The maps have been unilaterally introduced by China to denote supposed historical claims to territory: they have no basis in international law; nor do they reflect any international consensus on where territorial boundaries lie. They represent an attempt to provide further legitimacy for simply ignoring the Permanent Court of Arbitration's 2016 ruling that China had contravened the Philippine's sovereign rights in the South China Sea and that China's claims had no basis in the UN Convention on the Law of the Sea or international law.

Result

Since 2015, China has extended its reach and permanent presence significantly in the South China Sea, using hybrid tactics, and creating around 12.92 square kilometres (3,200 acres) of new land in the region.[53] It has managed to do that without inviting military intervention from any great power. It has, therefore, been extremely effective in achieving its strategic goals in the region.

Case study 2: Doklam

The 2017 stand-off between Indian and Chinese troops in Galwan, Doklam is a classic case of hybrid threat activity.

The Doklam Plateau is an important region cushioned between India, China and Bhutan but claimed by both China and Bhutan. The plateau is important for India; it overlooks a 22-kilometre land corridor connecting India's northeastern states to the rest of the country. Control over the plateau would allow China to gather intelligence on Indian military positions while also giving it the ability to cut off India's northeast from the rest of the country.

The 73-day stand-off began when Indian troops stopped Chinese troops from constructing a road in Doklam. It ended with a disengagement agreement after both powers retreated and withdrew troops. But the disengagement agreement didn't result in a slowdown of infrastructure development and troop movements along the disputed border. In June 2020, a clash occurred along the northern part of the border, resulting in the deaths of 20 Indian soldiers; the number of Chinese military casualties is unknown.

Military presence and permanent bases

ASPI has found that China and India have both continued to build up military infrastructure and presence along the disputed border.[54] China's construction accelerated following the 2017 stand-off and continued into 2021. It has included new air bases and permanent air defence positions. Infrastructure developments in the Doklam area include plans for more than 600 model villages in the next few years.[55]

Cyberattacks

During the period of heightened tensions over the border crisis in 2020, China targeted Indian Government websites and banking systems, raising the risk profile of engaging in the dispute for the Indian Government.[56]

Lawfare

Introduced in late 2021, China's Land Border Law seeks to manage Beijing's multiple land disputes in its favour, stating that the government will '[take] effective measures to resolutely safeguard territorial sovereignty and land border security, and prevent and combat any acts that damage territorial sovereignty and land borders'. Its use is to legitimise sovereignty claims and military actions that arise from disputes, including in Ladakh. Immediately before the law's introduction, China released a list of 15 'official' names for areas in the Indian state of Arunachal Pradesh in an attempt to strengthen Chinese territorial claims in the region.[57]

Result

As we've noted, the Doklam dispute is ongoing. China has been successful in building up permanent bases, but the risk of future clashes is high and will increase in intensity.

What are the consequences of inaction?

Frank Hoffman, writing in 2009, argued that we should pay less attention to terminology and more to understanding the inchoate grey space occupied by hybrid threats.[58] His call can only be reiterated: hybrid activity across the region is increasing, its use is more widespread as a consequence of the greater availability of means and tools and, in no small part as a result of increased reliance on technology, more points of leverage in national societies and economies. Purpose and intent are critical to interpreting hybrid activity, and it's evident that a number of nations, and China in particular, are harnessing hybrid tools and tactics to achieve strategic ends.

We don't suggest that it isn't possible for China to rise peacefully. It does appear, though, that core ways of operating used by the CCP to gain and hold power inside China are now the normal tools of the trade for projecting power externally, co-opting others to assist and advocate for CCP interests, and silencing, dividing and coercing those who can't be co-opted, whether they're states, civil society groups, corporations, international organisations or individuals.

So it's likely that hybrid threat activity will continue in the region, perpetrated by the actors that are outlined in this document and others that haven't been discussed. Those actors will continue to push the boundaries of acceptable behaviour while their position changes in the region, while continuing to engage in activities to further their objectives which are deemed unacceptable and undermine existing legal systems.

We consider that a regional HTC focused on collecting data, understanding the nature of hybrid activity, examining trends, shedding light on actor behaviours and building capacity will contribute to Indo-Pacific stability and security. Such a centre has a clear role in contributing to confidence-building measures that can alleviate tensions and misunderstandings that could potentially trigger conflict. Moreover, it could help governments, institutions and regional organisations to build networks, shared awareness and resilience that can help withstand the corrosive effects of hybrid threats.

The establishment of a regional HTC will signal its participants' support for national sovereignty and the rules-based order, the UN Charter and the UN's Universal Declaration on Human Rights. That's particularly pertinent in the region, given China's unwillingness to accept international jurisprudence or arbitration on its claims in the South China Sea[59]—despite the Chinese state being one of the developers of and signatories to the UN Convention on the Law of the Sea. Chinese behaviour sets a dangerous precedent that, if continued, will distort the system of international norms. We need greater international pressure to buttress rules that protect states' freedoms and sovereignty. Part of the task is improved information and a shared understanding of the nature and consequences of hybrid threat activity, which can be offered by a trusted, independent centre of analysis.

The consequences of inaction will be a systematic undermining of the configuration of the international system, an inability to arbitrate between claims made for sovereignty in the region, and the extended use of hybrid tools that fly under the radar because there's little or no research dedicated to uncovering them. It's the duty of states in the region to protect their interests and offer pushback in order to evolve progressively without capitulating to stronger, coercive powers.

Forgoing the opportunity to establish such a centre will encourage the continued behaviour of the more aggressive hybrid actors, such as China, as well as new entrants, adding to the overall sense of chaos, uncertainty and disruption in the Indo-Pacific. Given the centrality of the Indo-Pacific region for global economic prosperity and geostrategic stability, that will have global consequences.

The opportunity for a hybrid threat centre in the Indo-Pacific

The discussion in this paper illustrates the increasingly contested nature of the Indo-Pacific environment. Competitive behaviours, especially through hybrid and grey-zone activity, will continue to grow in scope and scale. And, because of the dynamic nature of the Indo-Pacific and its centrality to global prosperity and stability, the consequences of hybrid threats will be more extreme. Nonetheless, we can learn from responses elsewhere, not least where they've been tried and tested.

Europe, both at the national level and through the EU and NATO, has the most mature and developed approach to understanding and countering hybrid threats. Most notable is the establishment of the European/NATO Hybrid Centre of Excellence (CoE) based in Helsinki in 2017.

The Hybrid CoE is notable for its decentralised nature; its scope covering civilian and military domains; its emphasis on the hostile use of hybrid tools; its focus on building participating states' capability; its ability to allow member nations to share information and coordinate action; its support from its host government; its existing depth of research capability; and the autonomy of its researchers.

However, the Hybrid CoE has to contend with a considerably different security environment than exists in the Indo-Pacific. In particular, the Indo-Pacific has a more fragmented security architecture, which is a product of different historical experiences and politics. There's no regional equivalent of NATO, the Organization for Security and Co-operation in Europe or the EU. The relationships, practice and shared awareness built through those institutions enabled and supported the establishment of the Hybrid CoE. Existing organisations, such as ASEAN are deliberately limited, or, like APEC, lack the structural bracing and practice needed to bear additional weight or emerging challenges to security and prosperity.

The Indo-Pacific's fragmented strategic architecture reflects the multipolarity of regional power centres and threat actors in the region. As we've illustrated, the actor of greatest concern as an exponent of hybrid threat activities is China: it has the strongest motivation, greatest capability and an established history and practice of using hybrid activity for its strategic and political ends. But many nations use hybrid tools for domestic ends, and a number of the states in the Indo-Pacific continue to experience longstanding internal insurgencies or their after-effects, such as in Mindanao in the Philippines and the Naxal insurgency in India.

There are also differences in national, even cultural, perceptions of the threat arising from hybrid warfare. States will interpret threats differently, depending not simply on geographical proximity and regional security architecture, for example, but on their own socio-economic cohesion and military capability.[60]

Some have argued that what Western analysts describe as hybrid threats are simply business as usual in Asia, pointing to internal insurgencies and traditions such as that of Sun Tzu.[61] However, the use of hybrid tools and tactics has always formed part of warfare, whether by relatively weak or revisionist actors. Moreover, in a globally connected environment, we can expect that actors will learn from each other, spurring innovation and increased breadth and intensity of activity.

Geography makes a difference, too. The nature of the maritime environment in the Indo-Pacific exerts a greater influence on the nature of hybrid threats than can be found in the more continental focus of Europe.[62]

In short, there isn't yet a regional consensus that hybrid threats pose a risk to broader security and resilience. That extends to the values being protected. The Hybrid CoE has an explicit adherence to democratic principles in its mission and work. During our consultations, many of our respondents warned that such an explicit adherence would impede regional acceptance of an Indo-Pacific HTC.

There are strong reasons to be sceptical about such a position. For all that a number of states are wary of democratic forms and disciplines, they nonetheless benefit from democratic norms and institutions as anchors for the global rules-based order.

In particular, nations that are beset by hybrid threats such as encroachments on maritime sovereignty, insurgencies and economic coercion and that are vulnerable to some of the drivers that may be exploited by hybrid threat actors, such as digital inequality and low cyber maturity, stand to gain most from the work of such a centre. That's particularly the case if the centre were to engage in information exchange and capacity building.

So, to establish value and trust, the Indo-Pacific HTC will need a clear set of principles that support and protect the integrity of its research, its work and the interests of its members, supporters and funding partners. While those principles need not be explicitly democratic, they'll necessarily reflect the same principles that underpin democratic institutions.

That also places the location of a centre in a strong democracy. That doesn't exclude a decentralised structure: a regional network is critical to understanding the hybrid threat environment, enabling organic growth and acceptance, and capability building among member nations and organisations. But assurances based on strong governance arrangements such as those afforded in democracies (and, potentially, legislative protection such as the Hybrid CoE receives under Finnish law) will be critical to the centre's independence and integrity.

All those concerns and differences present both challenges and opportunities for a new institution that's directed at meeting some of those emerging challenges, and especially its establishment. Accordingly, we suggest the following proposal.

The proposal for an Indo-Pacific hybrid threat centre

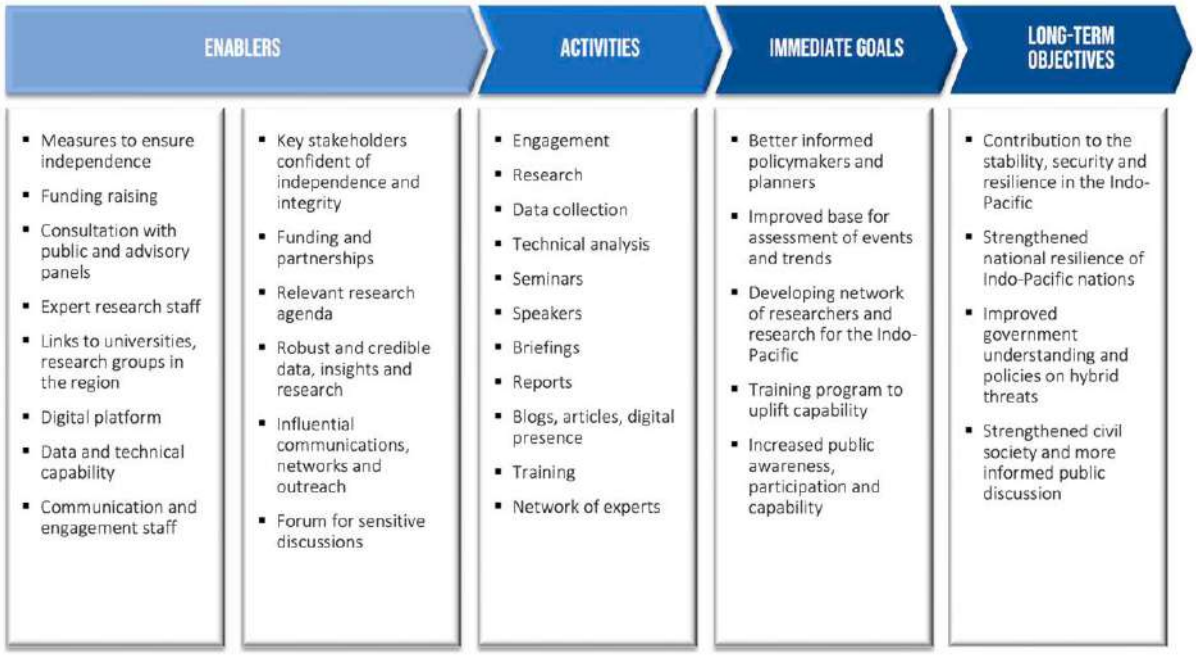
The Indo-Pacific HTC will be a centre of expert insight and analysis and will act as a coordinating point for research, dialogue, capacity building and advice on hybrid threats in the region.

The establishment and successful operation of the centre presents an opportunity to build increased resilience against hybrid threats in the Indo-Pacific through deepening understanding of hybrid activities, sharing trusted information about those threats, and building skills and expertise to strengthen analysis and policy responses to the threats.

Because many of the threats are enabled by technology, close coordination with technology companies and developers will make a key contribution to the centre and the value it's able to provide to the region, its members and its clients.

The broad approach is set in Figure 2.

Figure 2: Proposed approach

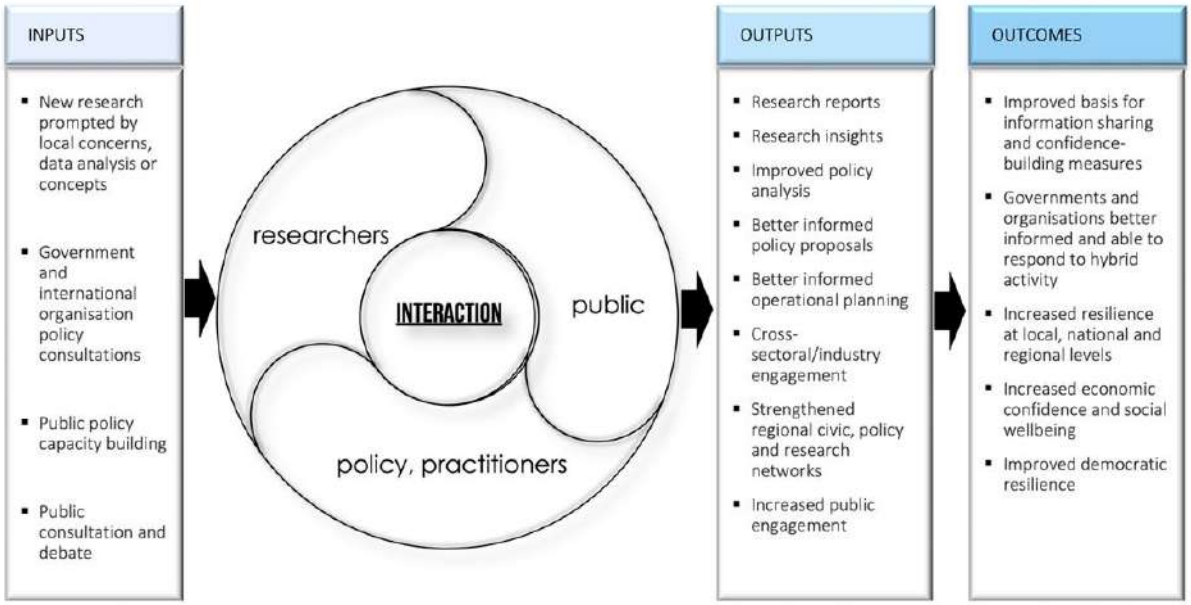


Source: Diagram created by the authors.

The Indo-Pacific HTC will undertake research, both its own and commissioned. It will engage with researchers, governments and technology platforms across the Indo-Pacific to build a better understanding of hybrid threats, to identify hybrid threat actors and their activities, and to map the domains, tools and effects of hybrid threats in the region.

Empirical research will be generated through interactions with the policy communities in member governments and through public consultation and capacity building, and will be generated internally by its experts and networks of experts (Figure 3). The creation, nurturing and maintenance of its expert network is a key task for research and insights as well as for helping to build a community and shared awareness of the hybrid threat environment. Similarly, data collection and the sharing of insights and responses between members will be a critical service of the centre in support of regional security and stability.

Figure 3: Proposed interactions



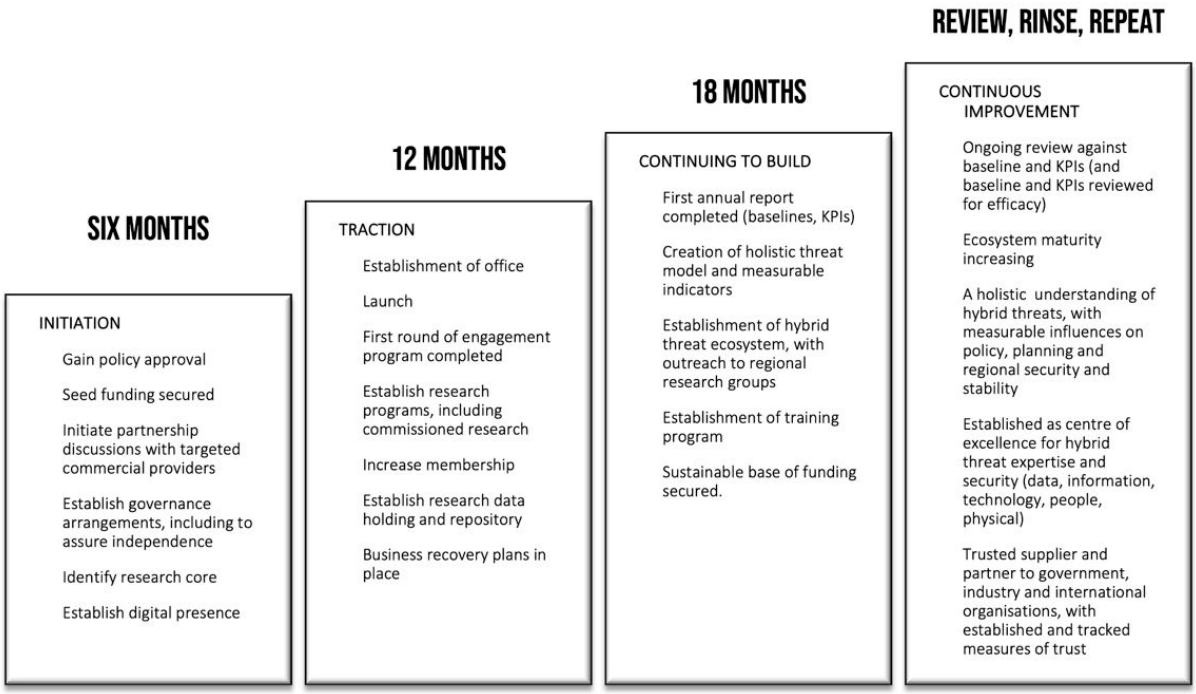
Source: Diagram created by the authors.

Implementation

The establishment of the centre will take some time, not least because partners will need to be found to secure long-term, sustainable funding. The necessary first step after or as part of policy approval will be securing seed funding: a concept in operation, rather than simply on paper, is needed to attract more support and collaborators.

A projected, and rather ambitious, schedule is set out in Figure 4. Time needs to be allowed for consultation and finding founding partners. We suggest, however, that an initial offering be constrained to partners willing to invest in the founding principles of the centre: independence and integrity.

Figure 4: Projected time frames



Source: Diagram created by the authors.

It's worth noting that the Hybrid CoE is the product of considerable preparatory work within the constructs of its enabling and supporting institutions—NATO and European Union—facilitated by shared processes, structures and relationships. That's not the case in the Indo-Pacific, which presents both challenges and opportunities.

First, there's the opportunity for the Indo-Pacific HTC to help bridge existing efforts to build architecture in the Indo-Pacific, particularly where there are overlapping spheres of purpose.

- For example, support for such a centre by the Quad could help the latter's engagement within the region and aligns with its purpose of building regional stability and resilience. An arrangement such as the Quad provides reach, but also reflects the crossover nature of the threats in focus: hybrid threats, left unattended, can harm economic prosperity, while economic weight can itself be used in a hybrid context.

Second, it opens opportunities for new models of support and funding. Specifically, because many hybrid threats leverage or exploit technology platforms, a public–private partnership with major platforms should be pursued.

- Hybrid threats are already recognised as areas of major concern by a number of the large technology companies, often as an extension of cybersecurity and disinformation efforts. For example, Microsoft's Threat Intelligence Center recently published on the hybrid war in Ukraine,[63] while Google's Threat Analysis Group focuses on the use of technology for malicious purposes by governments.[64]

Support by the technology companies would also facilitate technical support and expertise by the centre, strengthening its own offering and contribution to informed government policymaking and planning. Technology companies are often more aware of threat activity than governments, due to the use of their products and services and breadth of connectivity.

An alternative approach to establishment may be an initially decentralised model in which existing centres of expertise in the region are funded separately. Different countries may choose to focus on different concerns, reflecting extant expertise but areas of national interest. For example, Australia could focus on disinformation, Japan on critical infrastructure, and Singapore on maritime activities.

Such an alternative, decentralised approach would enable the incubation of research capacity while reflecting areas of specific national concern and so encouraging regional participation. It may also help deflect criticisms about a clearly identified HTC being 'anti-China'.

An incremental, decentralised approach, however, risks losing a whole-of-region perspective and the sharing of awareness and information that the European experience has found to be of great value in understanding and responding to current and emerging hybrid threats.

Governance

The independence and integrity of the Indo-Pacific HTC will be critical to its success. That will require a strong constitution, independence of funding, strong governance arrangements, an inclusive, critical research culture, and protection by its host nation, plus a commitment to the centre's apolitical nature.

- In the case of the Hybrid CoE, that's been assured by the Finnish Government embedding in its own laws the autonomy and inviolability of the Hybrid CoE, its operations and its information and data. There's good reason to follow that example.

The Indo-Pacific HTC will need a governing board. It will need to allow for representation of founding members, and a means of inclusion of members joining after its establishment, without any loss of its independence or compromise to its integrity.

That may mean a form of association, rather than membership. After all, the point is to build a community to contribute to regional stability and a shared awareness of hybrid threat activity.

Similarly, care will need to be taken to ensure that the centre's research and analysis aren't seen as being influenced by donors. The main means of avoiding that perception is to allow support to the general budget rather than specific projects and to have clear governance arrangements over its internal research program and over any grants the centre may offer to regional researchers as part of its network and capacity building.

Funding

Precisely because of the lack of supporting architecture and an institutional base in the Asia–Pacific, the centre will need a strong, resilient and sustainable base, including during its seed phase.

In the Indo-Pacific, there are considerably fewer ready sources of funding support directed at pan-regional and multidisciplinary initiatives than in Europe. The travel and engagement demands on the Indo-Pacific HTC will be considerably higher. Moreover, the centre will need to invest in research, analytical and capacity-building capability across a highly diverse range of maturity, institutions, cultures and threat priorities. Last, the value of the centre and its integrity will rest on its independence—and that includes sustained funding.

We aren't opposed to performance measures being used to assess the outcomes and performance of the centre—but with the caveat that sufficient time must be allowed for the centre to realise outcomes. The establishment and nurturing of matured capability, expertise, insight and analysis can take a decade or two. To that end, we recommend that the centre receive sufficient funding—a sustainable base—committed annually, and indexed, for a minimum of 10 years.

That sustainable base will need to be assessed, but it shouldn't require the centre's management and staff to have to constantly fundraise to undertake core tasks. And sufficient funding needs to be allowed for considerable travel and outreach across the region. That's in recognition of simple geography (the Indo-Pacific covers a large section of the Earth's surface), the comparative immaturity of security institutions that could otherwise be leveraged, and the need to cultivate the networks critical to engagement, situational awareness, data collection and capacity building.

Next steps

The details needed to establish an Indo-Pacific HTC are beyond the scope of this paper and will require considerable consultation with potential host governments, like-minded supporters and founders, and partners, including in the non-government and commercial sectors.

We recommend seed funding for the purpose of scoping the centre. Once that's done, the implementation path set out above can come into play.

However, we would urge early action and endorsement: hybrid activity continues to increase in the region, and an Indo-Pacific HTC could make a significant difference to regional resilience and stability.

Last, through our brief analysis, we consider that there are some areas ripe for early research by a future centre that would benefit regional awareness and security, including:

- continued tracking and mapping of the full spectrum of hybrid threat activity in the region
- identifying triggers for hybrid activity, interactions of different activities and escalation (for example, how the use of disinformation campaigns may imply other campaigns in maritime harassment, lawfare or economic coercion).

Notes

1 Danielle Cave, Jacob Wallis, 'Why the Indo-Pacific needs its own hybrid threats centre', *The Strategist*, 15 December 2021, online.
2 See NATO's definition, online, and the Hybrid Centre of Excellence's definition, online.
3 Defence Department, *Defence Strategic Update*, Australian Government, 2020, 5, online.
4 See, for example, P Stronski, *Implausible deniability: Russia's private military companies*, Carnegie Endowment for International Peace, 2 June 2020, online; E Geller, 'Chinese government recruiting criminal hackers to attack Western targets, US and allies say, *Politico*, 19 July 2021, online; J Yaffa, 'How hacking became a professional service in Russia', *The New Yorker*, 23 May 2021, online; T Maurer, *Cyber mercenaries: the state, hackers and power*, Cambridge University Press, 2018.
5 Jean-Baptiste Jeangène Vilmer, *Information defense: policy measures taken against foreign influence manipulation*, Atlantic Council, July 2021, online.
6 The Hybrid CoE instruments are infrastructure, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, diplomacy, political and information. G Giannopoulos, H Smith, M Theocharidou (eds), *The landscape of hybrid threats*, European Union and Hybrid CoE, 2020.
7 Under Section 8D, the following are defined as critical infrastructure sectors: communications sector; data storage or processing; financial services and markets; water and sewerage; energy; health care and medical; higher education and research sector; food and grocery; transport; space technology; and defence industry. It's worth noting that the focus of the legislation is cybersecurity, not the broader expanse of hybrid threat activity.
8 Zach Dorfman, 'The disappeared', *Foreign Policy*, 29 March 2018, online; Helen Davidson, 'China's act of "hostage diplomacy" comes to end as two Canadians freed', *The Guardian*, 25 September 2021, online.
9 Robert Windrem, Ken Dilanian, Abigail Williams, 'North Korea has a history of assassination attempts on foreign soil', *NBC News*, 22 November 2017, online; Fiona Broom, 'Making a murderer: the assassination of Kim Jong-nam', *The Interpreter*, Lowy Institute, 10 April 2019, online.
10 Fred Weir, 'Nemtsov joins long list of those assassinated in post-Soviet Russia', *Christian Science Monitor*, 2 March 2015, online; Julia Ioffe, 'Alexander Litvinenko and the banality of evil in Putin's Russia', *New York Times*, 21 January 2016, online; Rebecca Armitage, Lucy Sweeney, 'Why does Russia keep poisoning people? The wild history of Moscow's chemical assassination plots', *ABC News*, 16 April 2022, online.
11 See, for example, GF Treverton et al., *Addressing hybrid threats*, Swedish Defence University, 2018.
12 Janjira Sombatpoonsiri '"Fake news" and Thailand's information wars', *The Diplomat*, 3 July 2019, online.
13 Shibani Mahtani, Regine Cabato 'Why crafty internet trolls in the Philippines may be coming to a website near you', *The Washington Post*, 26 July 2019, online; Anastasia Kapetas, 'Southeast Asia on the forefront of disinformation for profit and power', *The Strategist*, 20 May 2021, online; Jacob Wallis, Ariel Bogle, Albert Zhang, Hillary Mansour, *Influence for hire: the Asia–Pacific's online shadow economy*, ASPI, Canberra, August 2021, online.
14 Thanks to Jean-Baptiste Jeangène Vilmer for drawing attention to this distinction.
15 P Charon, J-B Jeangène Vilmer, *Chinese influence operation: a Machiavellian moment*, Institute for Strategic Research, October 2021.
16 Sun Tzu, *The art of war*, trans. Brace E Barber, Penguin, 2009.
17 Peter Mattis, 'China's Three Warfares in perspective', *War on the Rocks*, 30 January 2018, online.
18 Scott Harold, Nathan Beauchamp-Mustafaga, Jeffrey W Hornung, *Chinese disinformation efforts on social media*, RAND Corporation, Santa Monica, 2021, online.
19 S Kemp, *Digital 2021: the Solomon Islands*, *Datareportal*, 12 February 2021, online.
20 JD Foukona, 'Solomon Islands gets a lesson in Chinese diplomacy', *The Interpreter*, 29 June 2020, online; A Ride, 'Solomon Islands security—blame and breakable gifts after the riots', *Australian Outlook*, Australian Institute for International Affairs, 7 December 2021, online.
21 Office of the Director of National Intelligence, *Annual threat assessment of the US intelligence community*, US Government, 9 April 2021, online.
The Republic of Korea (South Korea) has identified four strategic objectives that it believes North Korea hopes to achieve:
(a) creating a politically and ideologically stronger Korean People's Army (KPA)
(b) creating a morally stronger KPA
(c) developing the KPA into an army of sophisticated tactics
(d) making the various branches of the KPA stronger.
22 Andrew Shearer, testimony before the House Armed Services Committee hearing on the Evolution of Hybrid Warfare and Key Challenges, 22 March 2017, online.
23 Ministry of National Defense, *2020 Defense White Paper*, South Korean Government, 2021, online.
24 Ed Caesar, 'The incredible rise of North Korea's hacking army', *The New Yorker*, 21 April 2021, online.
25 'Islamic State Leader Abu Bakr al-Baghdadi encourages emigration, worldwide action', Site Intelligence Group, 1 July 2014, online.
26 Muh Taufiqurrohman, 'The road to ISIS', *Counter Terrorist Trends and Analysis*, May 2015, 7(4):17–25, online.
27 Prakoso Permono, Muhamad Syauqillah 'Pro-IS Indonesian militant groups and supporters', *Counter Terrorist Trends and Analysis*, March 2021, 13(2):24–29, online.
28 Elliot Stewart, 'The Islamic State stopped talking about China', *War on The Rocks*, 19 January 2021, online.
29 'Global Terrorism Index 2022: Measuring the impact of terrorism', Institute for Economics & Peace, March 2022, online.
30 'Addressing Islamic militancy in the southern Philippines', report 323, Crisis Group, 18 March 2022, online.
31 'Jihadism in southern Thailand: a phantom menace', International Crisis Group, 21 September 2016, online.
32 Prakoso Permono, Muhamad Syauqillah, 'Pro-IS Indonesian militant groups and supporters', *Counter Terrorist Trends and Analysis*, March 2021, 13(2):24–29, online.
33 Thomas Rid, *Active measures: the secret history of disinformation and political warfare*, MacMillan, 2020,
34 Africa Center for Strategic Studies, *Mapping disinformation in Africa*, US Department of Defense, 26 April 2022, online.
35 Elene Jenadze, *The digital Middle East: another front in Russia's information war*, Middle East Institute, 19 April 2022, online.
36 Lara Jakes, 'As protests in South America surged, so did Russian trolls on Twitter, US finds', *New York Times*, 20 January 2020, online; David Klepper, Amanda Seitz, 'Russia aims Ukraine disinformation at Spanish speakers', *AP News*, 8 April 2022, online.
37 Felix Chang, *India's neutrality and strategic relations with China, Russia and the West*, Foreign Policy Research Institute, 25 April 2022, online.
38 Elizabeth Dwoskin, 'China is Russia's most powerful weapon for disinformation warfare', *Washington Post*, 8 April 2022, online.
39 Samantha Hoffman, Matthew Knight, *China's messaging on the Ukraine conflict*, ASPI, Canberra, 23 May 2022, online.
40 Tom Burt, 'The hybrid war in Ukraine', Microsoft, 27 April 2022, online; Microsoft, *Special Report: Ukraine*, 27 April 2022, online.
41 Mike Burgess, 'Russia is being hacked at an unprecedented scale', *Wired*, 27 April 2022, online.

42 Beba Cibralic, Aaron Connelly, 'Russia's disinformation game in Southeast Asia', *The Interpreter*, 23 July 2018, online.
43 'How much trade transits the South China Sea?', *ChinaPower*, Center for Strategic and International Studies, 2022, online.
44 Jim Gomez, Aaron Favila, 'AP exclusive: US admiral says China fully militarized isles', *AP News*, 22 March 2022, online.
45 Jeremy Page, Carol E Lee, Gordon Lubold, 'China's president pledges no militarization in disputed islands', *Wall Street Journal*, 25 September 2015, online.
46 Secretary of Defense, *Military and security developments involving the People's Republic of China, 2021: annual report to Congress*, US Government, 2021, online.
47 'Breaking from the past, Vietnam marks South China See battle anniversary', *Radio Free Asia*, 14 March 2022, online.
48 Andrew Higgins, 'In Philippines, banana growers feel effect of South China Sea dispute', *Washington Post*, 10 June 2022, online.
49 Department of Defense, *Annual report to Congress: Military and security developments involving the People's Republic of China in 2017*, US Government, May 2017, online.
50 Tim Starks, 'F5 releases patches for nearly two dozen vulnerabilities, some critical', *Cyberscoop*, 10 March 2021, online.
51 Ben Westacott, Brad Lendon, 'Duterte threatens "suicide mission" if Beijing oversteps in South China Sea', *CNN*, 5 April 2019, online.
52 'Southeast Asia: an evolving threat landscape', FireEye, 2015, online.
53 Asia Maritime Transparency Initiative, *China Island Tracker*, Center for Strategic and International Studies, 2022, online.
54 Nathan Ruser, Baani Greal, *A 3D deep dive into the India–China border*, ASPI, Canberra, online.
55 Manoj Joshi, 'Closer to the edge: China is populating the rugged Himalayan frontier; India should, too', *The Tribune*, 23 November 2021, online.
56 David Sanger, Emily Schmall, 'China appears to warn India: Push too hard and the lights could go out', *New York Times*, 28 February 2021, online.
57 A Krishnam, 'China issues 'official' names for 15 places in Arunachal Pradesh', *The Hindu*, 31 December 2021, online.
58 Frank Hoffman, 'Hybrid vs compound wars', *Armed Forces Journal*, 1 October 2009, online.
59 Claims that have been upheld by international courts, such as the 2016 Permanent Court of Arbitration ruling in The Hague, that China had not exercised exclusive rights to the waters in the South China Sea and that it had violated the Philippines' sovereign rights in its exclusive economic zone, have simply been ignored. China didn't accept the tribunal's jurisdiction in this matter, and has continued with its activities and claims in the region. As an example of the effectiveness of Chinese compellence, President Duterte described the ruling as 'just a piece of paper', hoping to curry favour with China. John Feng, 'Philippines' Duterte says court ruling against China is trash to be thrown away', *Newsweek*, 6 May 2021, online.
60 F Hare, 'The cyber threat to national security: why can't we agree?', in C Czosseck, K Podins (eds), *Conference on Cyber Conflict Proceedings 2010*, CCD COE Publications, Tallinn, Estonia, 2010.
61 D Talat, 'Hybrid threats & warfare in South Asia', *Modern Diplomacy*, 8 January 2021, online.
62 C Aoi, M Futumura, A Patalano, 'Introduction hybrid warfare in Asia: its meaning and shape', *The Pacific Review*, January 2019, 31(6):693–713, online.
63 Burt, 'The hybrid war in Ukraine'.
64 Shane Huntley, 'How we're tackling evolving online threats', Google, 16 October 2020, online.

Acronyms and abbreviations

APEC	Asia–Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
CCP	Chinese Communist Party
CoE	centre of excellence
EU	European Union
HTC	hybrid threat centre
IS	Islamic State
NATO	North Atlantic Treaty Organization
PAFMM	People's Armed Forces Maritime Militia
PLA	People's Liberation Army
Quad	Quadrilateral Security Dialogue
UN	United Nations

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE