The Hague Centre
for Strategic Studies

Responding to China's Hybrid Threats

Strategic Postures for Small and Middle Powers

Benedetta Girardi, Noemie Jacq, Fiona De Cuyper and Laura Jasper

January 2026

The Hague Centre
for Strategic Studies

Responding to China's Hybrid Threats

Strategic Postures for Small and Middle Powers

Authors:
Benedetta Girardi, Noemie Jacq, Fiona De Cuyper and Laura Jasper

Contributors:
Sofia Romansky, Elton Hogklint and Emma Genovesi

Quality Assurance:
Tim Sweijs

January 2026

The research was made possible through a financial contribution from the Taipei Representative Office in the Netherlands to the Hague Centre for Strategic Studies (HCSS).

Table of Contents

Executive summary

Hybrid threats have become a defining feature of contemporary security environments, allowing actors to pursue strategic objectives below the threshold of conventional warfare. While much of the public debate in Europe has focused on Russia, the People's Republic of China (PRC) has likewise developed and refined a broad hybrid toolkit that it deploys across multiple regions. In Europe and the Asia-Pacific, small and middle powers (SMPs) are particularly vulnerable to these activities due to their limited capabilities, structural dependencies, and geographical or economical positions.

This study examines how the PRC employs hybrid threats against SMPs in Europe and the Asia-Pacific, and how those states respond. It argues that hybrid threats can be countered with ad-hoc approach, but only on a case-by-case basis, which is less efficient and sustainable in the long run. An ad-hoc approach ultimately does not build towards resilience, which is especially necessary in the case of SMPs targeted by hybrid threats. Rather, responses to hybrid pressure should be shaped by a comprehensive strategic posture of SMPs.

The report helps SMPs move from ad-hoc responses towards coherent strategic posturing against Chinese hybrid threats. It does so by proposing a framework that enables SMPs to identify their prevailing strategic approach, understand its implications and corresponding countermeasures, as well as reflect on alternative postures. The study does not prescribe how SMPs should respond to hybrid threats; instead, it shows how they can prepare themselves to respond more coherently and consciously. By linking threat patterns to strategic positioning, it encourages SMPs to consider hybrid threats as a structural component of the PRC's foreign policy toolkit rather than as isolated disruptions. Finally, the research gives SMPs recommendations to prepare coherent and comprehensive hybrid threat postures based on four overarching strategies.

The PRC's approach to hybrid threats is rooted in a long-standing strategic culture that emphasises indirect and non-kinetic means of influence. The doctrinal foundations of this approach include concepts such as the "unrestricted warfare" and the "Three Warfares" doctrines, which foreground the importance of shaping perceptions, narratives, and legal frameworks. In practice, the PRC employs a combination of tactics from a variety of domains in a synchronised and locally enabled manner.

The study is based on an original HCSS database of confirmed PRC hybrid threat incidents targeting 50 SMPs in Europe and the Asia-Pacific.[1] The database maps incidents across five main domains of hybrid activity: (1) digital and information warfare, (2) economic statecraft, (3) paramilitary operations, (4) physical destruction and violence, and (5) legal and political activities. For each incident, it records the actor, target, sector, timing, and intended effect. This enables a comparative, threat-based overview of how the PRC adapts its tactics to country-specific vulnerabilities, patterns of dependency, and regional dynamics.

[1] Chinese Latent Activity and Related Interference Scanner, The Hague Centre for Strategic Studies, https://claris.app.hcss.nl/.

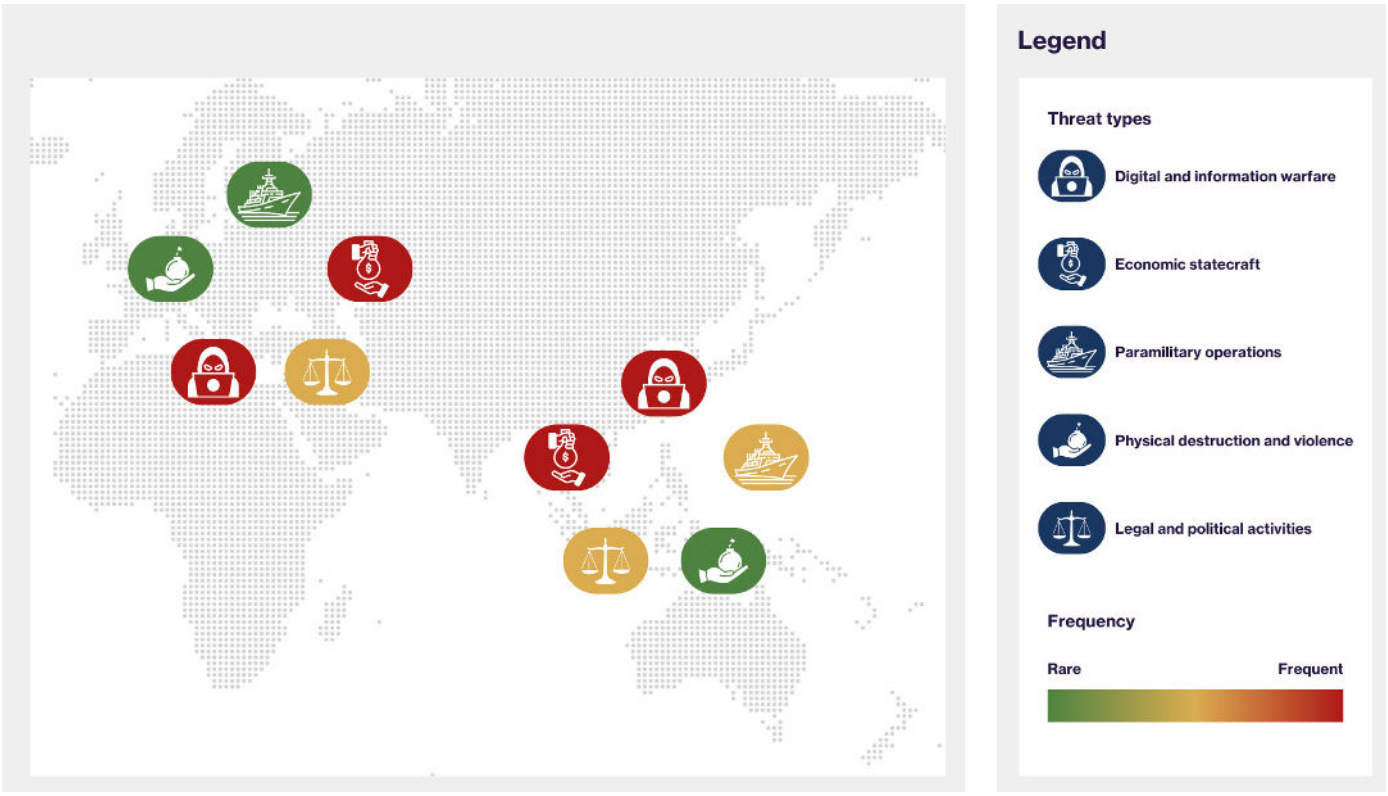
Table 1: Summary of hybrid threats categorisation

Category	Core Characteristics	Principal tactics
Digital and information warfare	Central pillar of hybrid activity enabled by global digital dependence	Cyber espionage, infrastructure intrusions, disinformation and misinformation
Economic statecraft	Use of economic statecraft and opaque financial tools to create leverage	Trade embargoes, investment restrictions, supply-chain manipulation, money laundering, bribery, capital flight
Paramilitary operations	Activities in the grey zone using non-state proxies or deniable units	Intimidation, sabotage, infiltration of protests, support to unrest
Physical destruction and violence	Targeted attacks below conventional warfare thresholds	Sabotage of infrastructure, vandalism, harassment, coercion, assassinations
Legal and political activities	Manipulation of legal frameworks and political systems to generate strategic advantage	Use of domestic laws for external claims, exploitation of legal ambiguity, political subversion, espionage.

The analysis shows that, in both Europe and the Asia-Pacific, the PRC relies heavily on **digital and information warfare**. Cyber espionage, infrastructure intrusions, and foreign information manipulation and interference (FIMI) have become central pillars of Chinese hybrid activity, exploiting high levels of digital dependence and vulnerabilities in critical systems. **Economic statecraft**, combining conventional trade and investment tools with more opaque financial practices, is another core pillar of Chinese hybrid activity, particularly where SMPs are structurally dependent on trade, loans, or infrastructure financing from the PRC. **Legal and political activities**, including lawfare and political undermining, complement these efforts by shaping legal frameworks, influencing political elites, and constraining collective responses within the societies of SMPs.

At the same time, the regional manifestations of Chinese hybrid threats are not uniform. In the Asia-Pacific, the PRC's hybrid activities are closely tied to its core territorial and strategic interests. The use of **paramilitary operations** in the South China Sea, coordinated cyber and information campaigns targeting Taiwan, and more frequent physical and maritime incidents underscore a more intense and proximate hybrid pressure. In Europe, hybrid activity is more heavily concentrated in cyber espionage, economic coercion, malign finance, and influence operations aimed at shaping EU and NATO debates, securing access to strategic infrastructure, and softening political resistance to PRC preferences. **Physical destruction and violence** tactics are less used by the PRC, with the notable exception of few cable cutting incidents.

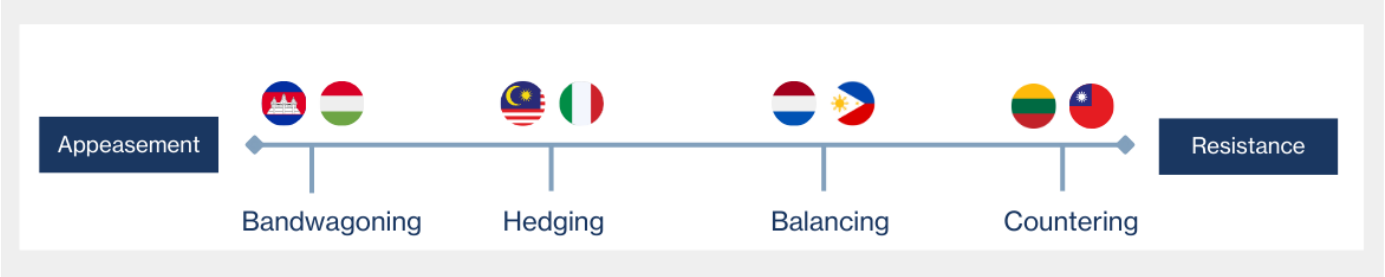
Figure 1: Frequency of Hybrid Threats used by PRC in Europe and Asia-Pacific



Just like the hybrid toolbox of the PRC is diverse, so are the responses that it requires. SMPs' responses can be broadly organised along four strategic approaches, which are further deepened in the report through dedicated case studies:

- **Bandwagoning**, where SMPs align closely with the PRC, often to secure economic benefits or political support, and downplay or tolerate hybrid activities while still investing in detection capabilities (e.g., Hungary, Cambodia).
- **Hedging**, where SMPs seek to maintain cooperative ties with the PRC while simultaneously cultivating relations with other powers to avoid overdependence and manage hybrid risks (e.g., Italy, Malaysia).
- **Balancing**, where SMPs strengthen resilience and align more clearly with other powers or alliances to counter PRC influence, while often preserving some level of pragmatic engagement (e.g., the Netherlands, the Philippines).
- **Countering**, where SMPs adopt more explicit and confrontational measures to deter, expose, and respond to PRC hybrid threats, sometimes at considerable economic or political cost (e.g., Taiwan, Lithuania).

Figure 2: Strategic responses to hybrid threats: case studies results



States' responses to hybrid threats thus vary by strategic posture, but even the most accommodating strategies retain important defensive elements.

Bandwagoning emphasises restraint and alignment, yet it still prioritises detection and preparation in order to understand vulnerabilities and the PRC's leverage; however, attribution is deliberately muted or avoided, with incidents downplayed or handled privately to minimise escalation and preserve stable relations.

Hedging adopts a flexible and calibrated approach, combining cautious signalling, selective and largely diplomatic attribution, and measured responses that balance risk management with resilience-building.

Balancing involves proactive and coordinated deterrence, characterised by clear red lines, strong detection and attribution capabilities, and robust collective responses designed to impose costs and shape long-term behaviour.

Countering reflects the most assertive posture, with explicit deterrence, rapid public attribution, and decisive use of economic, cyber, and military tools, accepting high costs in order to confront and neutralise hybrid threats directly.

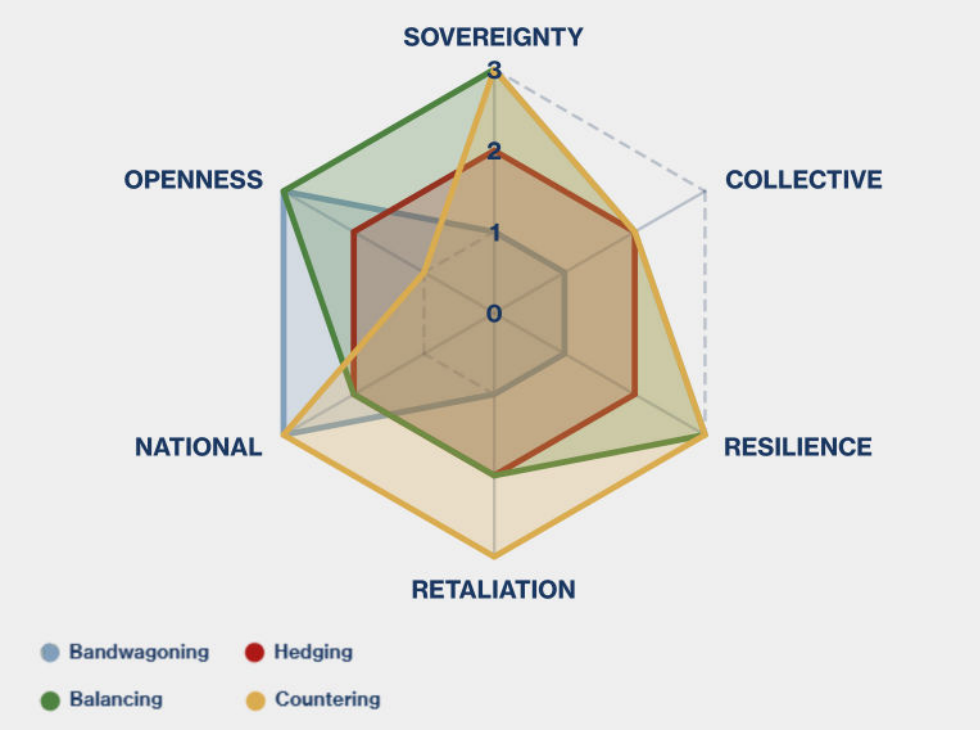
A key finding is that, while responses can be categorised in the four abovementioned strategies, they mostly occur in reactive and ad-hoc manners. Many SMPs still tend to respond to hybrid incidents on a case-by-case basis, without reference to an overarching strategy. Such ad-hoc responses are not efficient in the long term, particularly vis-à-vis the PRC, given the latter's wide array of tools, synchronised implementation, and ability to exploit a country's dependencies and vulnerabilities. A more strategic, long-term oriented approach is hence needed for SMPs to be able to respond to hybrid threats in a way coherent with the state's foreign policy and position in the international system.

While making a choice of strategy, SMPs in Europe and the Asia-Pacific must however navigate three structural dilemmas that shape the risks and feasibility of bandwagoning, hedging, balancing, or countering the PRC's hybrid threats. First, the **sovereignty–retaliation** dilemma forces states to choose between defending sovereign or principled positions and avoiding economic, diplomatic, or coercive retaliation, often encouraging caution. Second, the **openness–resilience** dilemma arises because economic openness and integration support growth but simultaneously expose states to foreign interference, coercion, and security vulnerabilities. Third, the **collective–national** dilemma concerns whether to rely on collective

mechanisms to share risk and deter coercion, which can dilute national control, or to act independently, which preserves autonomy but leaves states more exposed to retaliation.

These trade-offs, entailing region-specific exposure to economic and physical coercion as well as differing levels of institutional support, mean that each strategy carries distinct costs, vulnerabilities, and retaliatory implications.

Figure 3: Dilemmas in SMPs posturing



Bandwagoning eases the sovereignty–retaliation trade-off by minimising confrontation and short-term coercive pressure, but it deepens dependence, constrains national autonomy, and weakens long-term resilience.

Hedging seeks to balance sovereignty, openness, and retaliation risks through flexibility and ambiguity, preserving room for manoeuvre while accepting only partial resilience and the risk of strategic incoherence.

Balancing prioritises sovereignty and resilience through national or collective deterrence, reducing long-term vulnerability but raising immediate economic and political costs, particularly where institutional support is limited.

Countering most forcefully asserts sovereignty and addresses openness-related vulnerabilities by actively resisting coercion and hybrid threats, yet it amplifies retaliation and escalation risks across all three dilemmas, making it the most demanding posture in terms of capacity and political resolve.

In light of this, the report concludes with practical recommendations designed to help policy-makers in SMPs move towards a more deliberate and coherent counter-hybrid posture. The recommendations are tailored to each of the four archetypical strategies, offering options even to those SMPs who feel forced to bandwagon with the PRC:

1. Bandwagoning

1.1 Identify and strengthen key points of interconnection with the PRC
Identify key points of interconnection with the PRC and strengthen areas such as trade relations to generate spillover benefits that enhance the state's overall strategic position and reduce disruptive effects of hybrid threats.

1.2 Map and stress-test dependencies
Identify economic dependencies on the PRC, particularly in infrastructure, technology, and energy. Evaluate risks of overreliance on Chinese investments (e.g., BRI projects) and supply chains through mapping exercises and stress tests.

1.3 Implement mechanisms to monitor and evaluate Chinese economic leverage
Implement mechanisms to track the PRC's economic leverage, especially regarding trade relations and financial influence. These include scrutiny of investment agreements, tracking capital flows, and gathering and analysing investment data.

1.4 Create institutional oversight
Establish economic oversight committees to integrate intelligence on economic dependencies and disinformation campaigns that support the PRC's interests in the SMP.

1.5 Maintain calibrated public messaging
Maintain ambiguity in domestic messaging to avoid signalling negatively towards the PRC but also to avoid negative public perceptions of alignment with the PRC.

1.6 Align domestic policy with strategic messaging
Ensure that domestic policies regarding infrastructure development and foreign investment align with the SMP's economic bandwagoning stance without overtly signalling subordination to the PRC. This entails signalling autonomy and sovereign capacity (i.e. maintaining a clearly defined international policy agenda).

2. Hedging

2.1 Reassess national interests and areas for calibrated engagement
Review key national interests and identify where SMPs have leeway to engage with the PRC without becoming overly reliant. Focus on cybersecurity, information resilience, and economic diversification.

2.2 Identify tools needed for more effective preparedness
Identify the tools that need to be developed in order to be more effective in potential responses, such as assessing whether threats are sufficiently high and persistent to justify the creation of dedicated units to counter Chinese disinformation, and

determining where economic dependence is excessive and could be offset by strengthening or expanding other sectors when full decoupling or de-risking is not feasible.

2.3 Build integrated, cross-domain early-warning systems
Create integrated cross-domain early warning systems that can detect hybrid threats in real-time, especially cyberattacks or disinformation campaigns. This should involve government coordination with the private sector and existing public services (e.g., police, cyber units, etc).

2.4 Establish a national strategic coordination task force
Create a national strategic coordination task force, bringing together key stakeholders from foreign policy, defence, and cybersecurity to ensure that hybrid activity is managed through a multi-tiered response The task force should routinely meet and consistently re-evaluate whether a given approach is suitable and how it could be adjusted.

2.5 Maintain balanced external and domestic messaging
Balance public messaging to reflect the dual strategy of economic engagement with the PRC while maintaining ties with other partners.

2.6 Align domestic economic and technological policies with hedging
Ensure domestic policies, especially in technology and trade diversification, are aligned with the external stance of hedging. For example, when engaging with the PRC on infrastructure projects, simultaneously pursue trade diversification agreements with other powers.

3. Balancing

3.1 Conduct detailed hybrid-threat risk assessments
Assess PRC military and non-military hybrid threats (cyberattacks, disinformation, economic coercion). Identify potential escalatory pathways in response to Chinese hybrid activity and develop concrete red lines with corresponding responses in an anticipatory way.

3.2 Strengthen domestic institutions for counter-hybrid resilience
Develop strong domestic institutions in place for countering hybrid threats, including cybersecurity and dedicated intelligence gathering units that are also able to evaluate how certain indirect dependencies on the PRC (e.g., social media) could be introducing less overt vulnerabilities.

3.3 Reinforce detection and intelligence capabilities
Develop robust detection capabilities, particularly for disinformation and cyberattacks through the development of public-private partnerships to bolster capabilities (as done in the Ukrainian context). Strengthen counter-hybrid intelligence to identify emerging hybrid threats from the PRC.

3.4 Build robust coordination mechanisms
Build coordination mechanisms that enable prompt, cross-sector responses to hybrid threats by ensuring consistent information sharing, strengthening inter-institutional cooperation across cybersecurity, diplomacy, and military sectors, and conducting regular scenario, crisis-simulation exercises, and stress tests.

3.5 Communicate strategic positioning clearly
Clearly communicate the SMP's position towards the PRC's hybrid threats, using both public statements and national strategies as well as strategic alliances (e.g., through NATO, EU, or the Quad) as a concrete signal to the PRC.

3.6 Ensure strategic coherence with a balancing stance
Ensure that national security strategies, especially in cybersecurity, intelligence, and military resilience, align with a countering stance against China's hybrid tactics. Adjust policies regularly to maintain consistency as hybrid threats evolve.

4. Countering

4.1 Conduct a comprehensive vulnerability and confrontation assessment
Assess the risks of direct confrontation with the PRC and its hybrid tactics. Focus on national interests that are most at risk, including national security, critical infrastructure, and political sovereignty.

4.2 Strengthen institutional resilience
Review the resilience of institutions in critical areas such as intelligence and cybersecurity to ensure readiness for high-intensity hybrid threats.

4.3 Build rapid, high-level attribution and monitoring capabilities
Develop high-level attribution capabilities to ensure rapid identification of hybrid attacks, especially cyberattacks and disinformation. Establish dedicated teams across departments to ensure that hybrid threats are tracked in real-time.

4.4 Establish a centralised national security response centre
Establish a centralised national security response centre for counteracting hybrid threats, integrating all relevant sectors to enable a unified and fast response.

4.5 Publicly signal deterrence
Deploy diplomatic measures to signal deterrence against PRC hybrid tactics. Develop cyber defence and deterrence frameworks for swift, credible responses.

4.6 Ensure cohesive domestic and foreign messaging
Ensure that all domestic communication strategies reinforce the countering stance. Coordinate foreign policy with public domestic measures (e.g., stricter controls on Chinese investments in sensitive sectors).

Taken together, these insights and recommendations provide SMPs with the tools to move beyond reactive, ad-hoc measures and foster more coherent, strategic responses to hybrid threats in the era of the PRC's rise.

Figure 4: Summary of recommendations

Response	Review capabilities, stakes, and position	Build sustained cross-domain awareness	Ensure coherence between internal messaging and external positioning
Bandwagoning	1.1 Identify and strengthen key points of interconnection with the PRC	1.3 Implement mechanisms to monitor and evaluate Chinese economic leverage	1.5 Maintain calibrated public messaging
	1.2 Map and stress-test dependencies	1.4 Create institutional oversight	1.6 Align domestic policy with strategic messaging
Hedging	2.1 Reassess national interests and areas for calibrated engagement	2.3 Build integrated, cross-domain early-warning systems	2.5 Maintain balanced external and domestic messaging
	2.2 Identify tools needed for more effective preparedness	2.4 Establish a national strategic coordination task force	2.6 Align domestic economic and technological policies with hedging
Balancing	3.1 Conduct detailed hybrid-threat risk assessments	3.3 Reinforce detection and intelligence capabilities	3.5 Communicate strategic positioning clearly
	3.2 Strengthen domestic institutions for counter-hybrid resilience	3.4 Build robust coordination mechanisms	3.6 Ensure strategic coherence with a balancing stance
Countering	4.1 Conduct a comprehensive vulnerability and confrontation assessment	4.3 Build rapid, high-level attribution and monitoring capabilities	4.5 Publicly signal deterrence
	4.2 Strengthen institutional resilience	4.4 Establish a centralised national security response centre	4.6 Ensure cohesive domestic and foreign messaging

Introduction

Hybrid threats have become a central feature of the contemporary security environment. Rather than relying solely on conventional military force, state and non-state actors increasingly deploy a combination of overt and covert instruments, spanning digital, economic, political, legal, and paramilitary domains, to pursue strategic objectives below the threshold of formal armed conflict.[2] These activities often exploit attribution challenges, legal grey zones, and societal vulnerabilities, blurring the boundaries between peace and conflict. While the concept of hybrid threats remains contested in the academic and policy debate, it has gained traction in key strategic documents and institutions, including NATO and the European Union (EU), as a way of capturing the multidimensional nature of modern coercion and influence.[3]

In this context, the People's Republic of China (PRC) has emerged as a central actor. Building on long-standing doctrinal traditions and contemporary concepts such as the "unrestricted warfare" and the "Three Warfares", the PRC has developed a broad hybrid toolkit. This includes cyber and information operations, economic statecraft, malign finance, paramilitary activities, lawfare, and political influence.[4] These tactics are typically employed in a synchronised and locally enabled way: cyber operations are combined with disinformation, maritime pressure with legal claims, and economic inducements with elite capture or political undermining. Such integrated hybrid activity enables the PRC to shape the strategic environment, affect facts on the ground, and influence the decisions of target states into favourable directions without resorting to open conflict.[5]

Small and middle powers (SMPs) are particularly exposed to these forms of pressure from states like the PRC. As Beijing works to extend its influence abroad, SMPs' limited economic and military capabilities, structural dependencies, and often heightened geographic or political vulnerability create favourable conditions for hybrid tactics. At the same time, SMPs responses to hybrid threats have frequently been fragmented and ad-hoc. Governments tend to focus on individual incidents once they occur rather than situating them within a longer-term pattern. As a result, measures taken in response to Chinese hybrid threats are often reactive, uncoordinated across sectors, and insufficiently anchored in an overarching strategic framework.[6]

Ad-hoc responses to specific episodes of hybrid threats are not efficient in the long term, particularly when dealing with the PRC. SMPs face a structural asymmetry in capabilities, and the PRC's extensive hybrid toolbox allows it to test, probe, and exploit weaknesses over

---

2 Frank Hoffman et al., "The Future of Hybrid Warfare," Center for Strategic and International Studies, July 8, 2024, https://www.csis.org/analysis/future-hybrid-warfare.

3 Dirk Zandee et al., *Countering Hybrid Threats: Steps for Improving EU-NATO Cooperation* (Clingendael - Netherlands Institute of International Relations, 2021), 2, https://www.clingendael.org/sites/default/files/2021-10/countering-hybrid-threats.pdf.

4 Amrita Jash, "Fight and Win Without Waging a War: How China Fights Hybrid Warfare," *CLAWS Journal* 12, no. 2 (2019): 101, https://www.neliti.com/publications/327319/.

5 Elsa Kania, *The PLA's Latest Strategic Thinking on the Three Warfares* (The Jamestown Foundation, 2016), https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/.

6 Mattia Bertolini et al., *Ten Guidelines for Dealing with Hybrid Threats: A Policy Response Framework* (The Hague Centre for Strategic Studies, 2023), 8, https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf; Gregory F. Treverton et al., *Addressing Hybrid Threats* (Försvarshögskolan (FHS), 2018), 83, https://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-7574.

time. Responding to individual incidents risks resource exhaustion, policy inconsistency, and cumulative vulnerability. Conversely, a coherent strategic posture can help SMPs prioritise where to invest limited resources, determine what levels of risk are acceptable, and decide how far they wish to accommodate, hedge against, balance, or counter Chinese influence.

This research is concerned precisely with this gap. It seeks to assist SMPs in moving from ad-hoc responses to coherent strategic posturing against hybrid threats, with a particular focus on the PRC. The central premise is that while understanding the nature of hybrid threats is necessary, it is not sufficient. Effective responses depend not only on how hybrid tools are used but also on who is targeted and in what strategic context. The relationship between the PRC and a given SMP, including its economic exposure, alliance commitments, political priorities, and societal resilience, crucially shapes how hybrid threats are deployed and how they can be tackled.

As is characteristic of hybrid threats, the PRC has many tools at its disposal and uses them in a synchronised, locally enabled way. However, this study argues that responses cannot be designed purely on an understanding of the threat actor's toolkit. Instead, responses must be understood as part of a broader strategic posture of SMPs. This study takes a deep dive into this: it contextualises the responses to hybrid threats within larger strategic positioning, rather than treating responses as isolated, technical countermeasures.[7]

To support this shift from reaction to strategy, the research proposes a framework that categorises SMPs responses' options along four broad types: (1) bandwagoning, (2) hedging, (3) balancing, and (4) countering. These categories reflect different forms of positioning towards the PRC and the wider use of hybrid threats in the current climate of great power competition. The framework helps SMPs identify their prevailing strategy, understand how it shapes their exposure and responses to hybrid threats, and consider the implications for their overall posturing. In other words, it provides an analytical lens through which SMPs can assess not only how they respond, but what those responses reveal about their broader strategic orientation.

Importantly, the research does not tell SMPs how they should respond to Chinese hybrid threats. It does not offer a prescriptive menu of policy measures or a one-size-fits-all template. Instead, it shows SMPs how to prepare themselves to respond: by understanding their position, defining their priorities, and reflecting on the trade-offs inherent in different strategic approaches. Preparation in this sense is not a technical exercise but a strategic one. It involves recognising that hybrid threats are a structural expression of the PRC and that SMPs must position themselves consciously vis-à-vis Beijing.

The report first clarifies the boundaries and playbook of hybrid threats in Section 1 and zooms in on the specificities of the Chinese hybrid toolkit in Section 2. Then, through an analysis of available response strategies (Section 3) and detailed case studies (Section 4), the research demonstrates how SMPs are not only targets but can be actively posturing towards hybrid threats. By linking Chinese patterns of activity to the strategic postures adopted by SMPs in Section 5, the study aims to contribute to more coherent, deliberate counter-hybrid strategies in an increasingly contested international order. Recommendations are articulated through a 3-point agenda for SMPs posturing in the conclusion. The empirical basis for the study is a comprehensive database of confirmed Chinese hybrid threat incidents across 50 SMPs in Europe and the Asia-Pacific compiled in-house through open-source research, the Chinese Latent Activity and Related Interference Scanner (CLARIS).

---

7 Tinatin Khidasheli, *Hybrid Threats and Resilience: Safeguading Democratic Values in a Connected World* (Friedrich-Naumann-Foundation for Freedom South Caucasus, 2024), 12.

1. The rise of hybrid tactics in an era of geopolitical competition

1.1. What constitutes hybrid threats?

Throughout history, a variety of actors have attempted to achieve strategic objectives through means beyond warfare, blending deception and manipulation.[8] Rome turned local chieftains and kings into loyal puppet rulers by promising protection and wealth, blurring the lines between diplomacy and military action to consolidate power.[9] In ancient China, the Han dynasty embedded soldier-farmers in frontier territories, combining economic production and military readiness to create a self-sustaining territorial presence.[10] Perhaps the most iconic example from antiquity is the Trojan Horse, which enabled Greek forces to infiltrate Troy by hiding soldiers within a seemingly benign wooden gift. While such acts of deception are more akin to myth, modern societies still have to contend with their fair share of Trojan Horses: digital and intangible, yet equally deceptive, computer viruses that install malware on the recipient's device under the guise of legitimate software.[11] Yet, what differentiates these modern threats is the scale of their objectives; from disrupting supplies of gas in underwater pipelines to influencing political processes by deliberately spreading false information.[12] These historical and contemporary examples illustrate a foundational characteristic of what is referred to as 'hybrid threats': the blending of overt (visible, tangible) and covert (hidden, secretive) actions to achieve strategic aims which blur the lines between peace and conflict.

While the discreet terminology of 'hybrid threats' is relatively new, the practices that fall under this umbrella are not a new phenomenon.[13] Still, the modern hybrid toolbox has expanded dramatically. With the emergence of digital technologies, a novel arena for the contestation

8 Martin Solik and Jan Graf, "Hybrid Threats to Democracy in Europe: Russian and Chinese Influence in the EU Neighbourhood" (European Network of Political Foundations, 2023), 11, https://www.enop.eu/wp-content/uploads/2023/06/ENoP_Hybrid-Threats-to-Democracy-in-Europe.pdf.

9 Douglas C. Sanders, "Julius Caesar and the Gallic Campaign: A Roadmap to the Use of the Instruments of Power" (Marine Corps University, 2010), 21.

10 Arsinoe Temple Library, "The Tuntian System: Cao Cao's Secret Weapon," Arsinoe Temple Library, February 4, 2020, https://www.arsinoelibrary.org/EPS/articles/the-tuntian-system-cao-caos-secret-weapon/.

11 Fortinet, "What Is a Trojan Horse? Trojan Virus and Malware Explained," Fortinet, n.d., https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus.

12 Andrew Buzzell, "Expert Insight: What Is Election Interference?," Western News, April 6, 2025, https://news.westernu.ca/2025/04/election-interference/.

13 Nicu Popescu, *Hybrid Tactics: Neither New Nor Only Russian*, Issue Alert (European Union Institute for Security Studies, 2015), 1, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_hybrid_warfare.pdf.

of power has manifested, augmenting the effect of traditional influence activities in intensity and speed.[14]

Foundational definitions of hybrid threats considered violence as a core feature, emphasising combinations of conventional, irregular, and coercive kinetic means. However, as the character of conflict evolved through the rise of the digital domain and emerging technologies, nonviolent measures have become key in the hybrid threat arsenal.[15] A modern conceptualisation of hybrid threats further expands beyond technological advancements, reflecting a shifting geopolitical context where both state and non-state actors deliberately employ hybrid tactics. In early literature, hybrid threats were primarily linked to non-state actors such as Hezbollah in Lebanon and the Houthis in Yemen, as employing hybrid tactics reduced the costs of engagement.[16] However, the cyber and information operations surrounding Russia's illegal annexation of Crimea in 2014 marked a paradigm shift. Russia's effective use of cyber and information operations revealed that the appeal and utility of hybrid tools is not limited to non-state actors and can be wielded successfully by state actors.[17] The use of the concept subsequently proliferated across different dimensions –including diplomatic, technological, civil, economic, military, unconventional methods, and information and influence operations– bringing with it an expansion of what qualifies as hybrid threats.[18]

While literature on hybrid threats is vast, the term lacks a universally accepted definition.[19] For the purpose of this study, hybrid threats are understood as the deliberate and coordinated use of overt and covert methods by state and non-state actors to destabilise and undermine the sovereignty, decision-making processes, and societal cohesion of a target, most often a state.[20] Such threats exploit difficulties of attribution (linking actions to specific actors) and detection, operate simultaneously across multiple domains, and remain below the threshold of conventional military warfare to achieve strategic objectives.[21]

For the sake of analytic clarity, it is necessary to further differentiate hybrid threats from related concepts such as asymmetric warfare, hybrid warfare, and grey zone activities.

---

14 Tim Sweijs, *Between War and Peace 'Hybrid Threats' and NATO's Strategic Concept* (The Hague Centre for Strategic Studies, 2022), 1, https://hcss.nl/wp-content/uploads/2022/06/Between-War-and-Peace-HCSS-2022-V2.pdf; Anton Dengg and Michael N. Schurian, "On the Concept of Hybrid Threats," in *Networked Insecurity: Hybrid Threats in the 21st Century* (Schriftenreihe der Landesverteidigungsakademie, 2016), 35–36, https://www.bmlv.gv.at/pdf_pool/publikationen/2016_17_sr__networked_security_dengg_schurian.pdf; North Atlantic Treaty Organization, "Countering hybrid threats," NATO, May 7, 2024, https://www.nato.int/cps/fr/natohq/topics_156338.htm.

15 Hoffman et al., "The Future of Hybrid Warfare."

16 Georgios Giannopoulos et al., *The Landscape of Hybrid Threats: A Conceptual Model (Public Version)* (Publications Office of the European Union, 2021), https://doi.org/10.2760/44985.

17 Murat Caliskan and Michel Liégeois, "The Concept of 'Hybrid Warfare' Undermines NATO's Strategic Thinking: Insights from Interviews with NATO Officials," *Small Wars & Insurgencies* 32, no. 2 (2021): 296, https://doi.org/10.1080/09592318.2020.1860374.

18 Mikael Weissmann, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare: The Role of the Military in the Grey Zone," in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations'*, ed. Mikael Weissmann et al. (Bloomsbury Collections, 2021), 65, https://www.researchgate.net/publication/349496635_Conceptualizing_and_countering_hybrid_threats_and_hybrid_warfare_The_role_of_the_military_in_the_grey_zone.

19 Zandee et al., *Countering Hybrid Threats: Steps for Improving EU-NATO Cooperation*, 2.

20 National Coordinator for Security and Counterterrorism, *Chimaera: An Analysis of the "hybrid Threat" Phenomenon* (Ministry of Justice and Security, 2019), 9, https://english.nctv.nl/documents/publications/2019/09/05/analysis-of-the-%E2%80%98hybrid-threat%E2%80%99-phenomenon; Sofia Romansky et al., *New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape* (The Hague Centre for Strategic Studies, 2024), 4, https://hcss.nl/wp-content/uploads/2024/05/New-Technologies-Changing-Strategies-Hybrid-Threats-HCSS-TNO-2024.pdf; Giannopoulos et al., *The Landscape of Hybrid Threats*, 6.

21 Frank Hoffman, "'Hybrid Threats': Neither Omnipotent Nor Unbeatable," *Orbis* 54, no. 3 (2010): 443, https://doi.org/10.1016/j.orbis.2010.04.009; Zandee et al., *Countering Hybrid Threats: Steps for Improving EU-NATO Cooperation*, 2–5.

Asymmetric warfare, as a sub-category of conventional warfare, involves adversaries with unequal resources such as insurgents acting against state military forces. The disparity in military capabilities typically requires the use of violent methods and means, like Guerilla tactics.[22] In comparison, hybrid threats, are differentiated by their multidimensionality, complexity, and convergence at lower levels of society, targeting vulnerabilities across political, economic, and social levels.[23] Such threats specifically aim to remain below the thresholds of what would formally qualify as acts of war under international law.[24]

The conceptual debates surrounding "hybrid threats" versus "hybrid warfare" are particularly significant. While these terms are often treated interchangeably, the term "warfare" is associated with formal armed conflicts which are governed by international legal frameworks like the Geneva Conventions.[25] Hybrid threat activities intentionally blur the boundaries between peace and war, but fall short of legally defined armed conflict due to their subtlety, lower intensity, and the kinds of actors involved.[26] They also contribute to legal ambiguities in terms of detection, attribution, response and deterrence that can be exploited by the perpetrator.[27] Consequently, using the term "hybrid warfare" limits the conceptual scope to hybrid elements of armed conflict, so it is better understood as a "subset of the hybrid threat spectrum".[28] Finally, although hybrid threats affect national security, many military forces have no relevant internal competences to address this category of threats. Rather, hybrid threats fall primarily within the purview of national law enforcement agencies or civilian government departments, rendering the term hybrid warfare less applicable in these cases.[29]

Similarly, distinguishing hybrid threats from "grey zone" activities enhances conceptual clarity by raising awareness about the full spectrum of modern conflict and the place of hybrid threats within it. The grey zone can be understood as the "shadowy space" between the margins of formal peace and declared war.[30] While many hybrid threats are executed within the grey zone, they are not confined to it. They may also be integrated into active conflict to complement and amplify the effects of traditional military measures or manifest as discrete activities outside the grey zone.[31]

---

22 Patrick A. Mello, "Asymmetric Warfare," in *The Wiley-Blackwell Encyclopedia of Sociology*, 2nd ed. (Wiley-Blackwell, 2015), 1, https://patrickmello.com/wp-content/uploads/2021/04/Mello-2016-EOS.pdf.

23 Susana Sanz-Caballero, "The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe," *Humanities and Social Sciences Communications* 10, no. 1 (2023): 2, https://doi.org/10.1057/s41599-023-01864-y; Sean S. Costigan and Michael A. Hennessy, *Hybrid Threats and Hybrid Warfare: Reference Curriculum* (North Atlantic Treaty Organization, 2024), 37, https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf.

24 Caliskan and Liégeois, "The Concept of 'Hybrid Warfare' Undermines NATO's Strategic Thinking," 297; David Carment and Dani Belo, "Gray-Zone Conflict Management: Theory, Evidence, and Challenges," *Journal of European, Middle Eastern & African Affairs* 2 (June 2020): 22.

25 Sean Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?," *Prism* 8, no. 2 (2019): 83, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf; Hoffman, "'Hybrid Threats,'" 443.

26 Susana Sanz-Caballero, "The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe," *Humanities and Social Sciences Communications* 10, no. 1 (June 29, 2023): 2, https://doi.org/10.1057/s41599-023-01864-y; Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?": 85.

27 Hitoshi Nasu, "Hybrid Threats and Grey Zone Conflict Symposium – Challenges in the Twilight of International Law," Lieber Institute West Point, October 30, 2024, https://lieber.westpoint.edu/challenges-twilight-international-law/.

28 Dengg and Schurian, "On the Concept of Hybrid Threats," 36.

29 Jānis Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy" (Riga: National Defence Academy of Latvia - Center for Security and Strategic Research, April 2014): 7, https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf.

30 Donald Stoker and Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking," *Naval War College Review* 73, no. 1 (2020): 16, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8092&context=nwc-review.

31 Giannopoulos et al., *The Landscape of Hybrid Threats*, 36.

Critics argue that the concept of hybrid threats risks providing too many categories for conflict which undermines clarity, suggesting that it should be "eliminated from the strategic lexicon".[32] The novelty and utility of the concept has also been heavily debated, with some arguing that it lacks conceptual clarity and is merely a repackaging of existing concepts.[33] Despite these critiques, many contemporary security challenges exist beyond the traditional military domain. As such, the flexibility of the concept helps capture the creativity and adaptability with which adversaries instrumentalise tactics.[34] Strategic documents from institutions such as NATO and the European Union increasingly adopt "hybrid threats", with the latter even establishing the European Centre of Excellence for Countering Hybrid Threats.[35]

1.2. How are hybrid threats deployed?

While the post-Cold War world was characterised by Western-led unipolarity, the status quo is increasingly being challenged by other powers, such as the PRC and Russia, competing for influence.[36] The PRC's ascent has been marked by rapid economic growth and military modernisation. The country invests significantly in technology and infrastructure, both domestically and through the Belt and Road Initiative (BRI), aimed at expanding its geopolitical influence.[37] Simultaneously, Russia has sought to reassert its regional dominance by, *inter alia*, occupying and invading Ukraine as well as by getting involved in conflicts in the Middle East.[38] Thess actions have led to a more multipolar world order, where traditional and emerging powers vie for strategic positions, often by employing hybrid threats.

1.2.1. Identifying actors and targets: who are the major players and where do they strike?

Great Powers like Russia, the PRC, and the US have adeptly integrated hybrid tactics into their strategic arsenals. During Russia's annexation of Crimea in 2014, unmarked troops (referred to as "little green men") were deployed to obscure official involvement.[39] This was combined with disinformation campaigns, cyber-attacks, and demoralising anonymous messaging to

32 Colin Gray, *Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional* (U.S. Army War College Strategic Studies Institute, 2012), 35, https://press.armywarcollege.edu/monographs/561; Stoker and Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking," 2.

33 Giannopoulos et al., *The Landscape of Hybrid Threats*, 6; Erik Reichborn-Kjennerud and Patrick Cullen, *What Is Hybrid Warfare?* (Norwegian Institute of International Affairs, 2016), 4, https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf.

34 Reichborn-Kjennerud and Cullen, *What Is Hybrid Warfare?*, 4.

35 Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?," 85.

36 Michael Mazarr and Hal Brands, "Navigating Great Power Rivalry in the 21st Century," War on the Rocks, April 5, 2017, https://warontherocks.com/2017/04/navigating-great-power-rivalry-in-the-21st-century/.

37 Alexander Al-Haschimi and Tajda Spital, *The Evolution of China's Growth Model: Challenges and Long-Term Growth Prospects* (European Central Bank, 2024), https://www.ecb.europa.eu/press/economic-bulletin/articles/2024/html/ecb.ebart202405_01~a6318ef569.en.html.

38 Antonio Perra, "From the Arab Spring to the Damascus Winter: The United States, Russia, and the New Cold War," *Contemporary Review of the Middle East* 3, no. 4 (2016): 371–72, https://doi.org/10.1177/2347798916664578.

39 EUvsDisinfo, "Little Green Men: The Annexation of Crimea as an Emblem of pro-Kremlin Disinformation," EUvsDisinfo, March 16, 2018, https://euvsdisinfo.eu/little-green-men-the-annexation-of-crimea-as-an-emblem-of-pro-kremlin-disinformation/.

Ukrainian soldiers, paving the way for strategic gains without triggering full-scale conflict.[40] During Russia's 2022 invasion, similar hybrid operations have been observed: citizens were sent intimidating messages, fake 'official' evacuation instructions, and some civilians were coerced into carrying out terrorist acts.[41]

Turning to the PRC, its hybrid operations predominantly span economic, informational, legal and maritime domains. They combine coercive economic statecraft –investment pressure, trade restrictions and sanctions against states like Australia, Taiwan and Lithuania– and economic inducements to align countries with its interests.[42] For instance, the PRC uses port infrastructure investments in critical locations such as Sri Lanka, Pakistan, Greece, and Djibouti, allowing Beijing to build strategic leverage.[43] Hybrid maritime tactics, such as surrounding disputed islands with layers of coast guard, fishing and naval vessels, are also frequently employed by the PRC to assert regional control without resorting to military conflict.[44]

Yet, hybrid threats are not tactics that are solely deployed by Russian and the PRC as great powers. An infamous hybrid operation which reshaped the cyber security landscape as one of the first Digital Weapons in history is the Stuxnet malware, discovered in 2010 and allegedly attributed to the US. This computer worm infiltrated Iran's nuclear facilities opening the possibility for destruction of critical infrastructures without direct involvement.[45] The US has also been accused of engaging in espionage and political undermining, notably through manipulation of information during its military invasion of Afghanistan and Iraq, as well as (attempts at) covert regime change is several countries.[46]

---

40 Nino Macharashvili, "Hybrid War with Russian Rules and Ukrainian Resistance," Rondeli Foundation, February 3, 2023, https://gfsis.org/en/hybrid-war-with-russian-rules-and-ukrainian-resistance/; Raphael Satter, "'You're Just Meat' - Ukrainian Soldiers Get Chilling Texts," *Associated Press*, May 11, 2017, https://apnews.com/general-news-1096d53b7e5a4a9682d6b434021fb2f8; Stephanie Stamm and Hanna Sender, "Understanding Russia's Various Hybrid War Tactics in Ukraine," *The Wall Street Journal*, February 25, 2022, https://www.wsj.com/livecoverage/russia-ukraine-latest-news/card/understanding-russia-s-various-hybrid-war-tactics-in-ukraine-H1Hnr8iMvRinuh1qNoB4.

41 Euractiv, "Russia vs Ukraine: The Biggest War of the Fake News Era," Euractiv, August 1, 2024, https://www.euractiv.com/section/global-europe/news/russia-vs-ukraine-the-biggest-war-of-the-fake-news-era/; Stamm and Sender, "Understanding Russia's Various Hybrid War Tactics in Ukraine"; Amirs Barkhush, "Russian Intelligence Blackmails Ukrainian Teen With Compromising Photos into Terrorist Attack," UNITED24 Media, March 21, 2025, https://united24media.com/latest-news/russian-intelligence-blackmails-ukrainian-teen-with-compromising-photos-into-terrorist-attack-6941.

42 Gatra Priyandita, *Chinese Economic Coercion in Southeast Asia: Balancing Carrots and Sticks* (European Centre of Excellence for Countering Hybrid Threats, 2023), 15, https://www.hybridcoe.fi/wp-content/uploads/2023/10/20231026-Hybrid-CoE-Working-Paper-25-Chinese-economic-coercion-WEB.pdf; James Laurenceson, "Australia and Lithuania: Limits of Chinese Trade Coercion," *Council on Geostrategy*, June 14, 2022, https://www.geostrategy.org.uk/britains-world/australia-and-lithuania-limits-of-chinese-trade-coercion/.

43 Daniel F. Runde et al., "Responding to China's Growing Influence in Ports of the Global South," Center for Strategic and International Studies, October 30, 2024, https://www.csis.org/analysis/responding-chinas-growing-influence-ports-global-south.

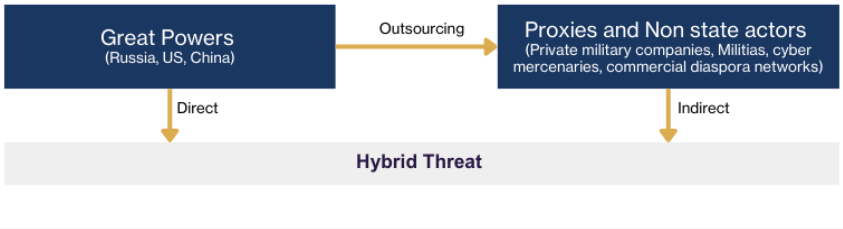
44 Isaac B. Kardon, "Combating the Gray Zone: Examining Chinese Threats to the Maritime Domain," Carnegie Endowment for International Peace, June 4, 2024, https://carnegieendowment.org/posts/2024/06/combating-the-gray-zone-examining-chinese-threats-to-the-maritime-domain?lang=en; Wei-Chung Chen et al., "China's Gray Zone Actions in the East China Sea, Taiwan Strait, and South China Sea: A Comparative Study and Impact on Fisheries," *Marine Policy* 167 (September 2024): 106246, https://doi.org/10.1016/j.marpol.2024.106246.

45 Thomas M. Chen and Saeed Abu-Nimeh, "Lessons from Stuxnet," *Computer* 44, no. 4 (2011): 91, https://doi.org/10.1109/MC.2011.115.

46 Lindsey A. O'Rourke, "The Strategic Logic of Covert Regime Change: US-Backed Regime Change Campaigns during the Cold War," *Security Studies* 29, no. 1 (2020): 92–127, https://doi.org/10.1080/09636412.2020.1693620; Nancy Snow and Philip M. Taylor, "The Revival of the Propaganda State: US Propaganda at Home and Abroad since 9/11," *International Communication Gazette* 68, nos. 5–6 (2006): 392–93, https://doi.org/10.1177/1748048506068718.

Proxies and non-state actors – such as private military companies, militias, cyber mercenaries, commercial diaspora networks, and organised crime groups – are often leveraged by these powers to further their agendas. When it comes to cyberspace, for example, states often outsource disinformation, sabotage, and espionage efforts to hacker collectives, so-called troll farms or criminal entities.[47] This approach provides plausible deniability and extends their reach in a cost-effective way which reduces chances of direct attribution, as visible in Figure 5.[48]

Figure 5: Major Powers' hybrid threats penetration process



Authoritarian powers tend to rely more on such entities due to their centralised political structures and limited transparency and accountability to civil society. While democratic states have also made use of proxies, especially during the Cold War, they face stronger ethical and legal constraints from the media, courts and civil society.[49] Cultural and ideological factors cannot be overlooked in this context and contribute to diverging approaches.[50]

Recurring patterns can be observed both among the actors that employ hybrid threats and in the characteristics of the states they are used against. In particular, the inherent vulnerabilities of SMPs make them attractive targets (Figure 6). SMPs possess limited economic and military capacities, due to their size and resulting capabilities, often rendering them more susceptible to external manipulation.[51] Yet, while SMPs may be overall weaker, they simultaneously often excel in specific areas of industry or exports, making them strategically

47 Emma Schroeder et al., *Hackers, Hoodies, and Helmets: Technology and the Changing Face of Russian Private Military Contractors* (Atlantic Council, 2022), 6–7, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/technology-change-and-the-changing-face-of-russian-private-military-contractors/; Simon Handler, "The 5×5—Non-State Armed Groups in Cyber Conflict," Atlantic Council, October 26, 2022, https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-non-state-armed-groups-in-cyber-conflict/.

48 Sanz-Caballero, "The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe," 3; Janne Jokinen and Magnus Normark, *Hybrid Threats from Non-State Actors: A Taxonomy* (European Centre of Excellence for Countering Hybrid Threats, 2022), 6, https://www.hybridcoe.fi/wp-content/uploads/2022/05/20220609-Hybrid-CoE-Research-Report-6-Non-state-actors-WEB.pdf; European Centre of Excellence for Countering Hybrid Threats, *Frequently Asked Questions on Hybrid Threats* (European Centre of Excellence for Countering Hybrid Threats, n.d.), 1, https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf.

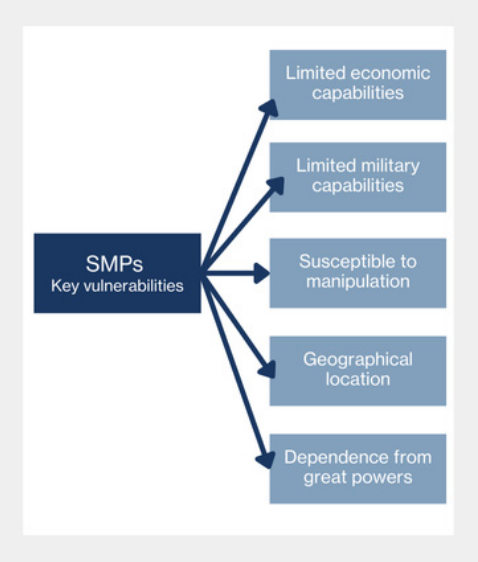
49 Sanz-Caballero, "The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe," 3.

50 Jukka Aukia and Lucjan Kubica, *Russia and China as Hybrid Threat Actors: The Shared Self-Other Dynamics* (European Centre of Excellence for Countering Hybrid Threats, 2023), 5, https://www.hybridcoe.fi/wp-content/uploads/2023/04/NEW_Hybrid_CoE_Research_Report_8_web.pdf.

51 Alexandros Zachariades, "Between a Rock and a Hard Place: Small States, Vulnerabilities and Greek Foreign Policy," *International Politics*, July 2025, 5, https://doi.org/10.1057/s41311-025-00713-w.

valuable to great powers especially when particular SMPs are located in the geographic vicinity of larger powers seeking to expand their influence.[52] The geographical factor also plays into the strategic calculations of great powers when it comes to creating spheres of influence and control, to the extent where SMPs may be considered security buffers as part of a defence strategy. Reinforcing these vulnerabilities and qualities are pre-existing dependencies – economic, financial or technological – on larger powers which are necessary for the SMPs' prosperity, the very which create leverage that can be exploited through coercive hybrid methods.[53] These factors collectively create an environment where hybrid threats can effectively influence and destabilise SMPs without provoking direct military confrontation as responses may prove too costly.

Figure 6: SMP's vulnerabilities



1.2.2. Decoding the hybrid playbook: what are the key tactics?

The primary objective of deploying hybrid threats is to influence and destabilise target states without engaging in direct military confrontation.[54]

Establishing an overview of hybrid threat tactics and tools is challenging due to their highly context-dependent and adaptive nature. However, this study identifies five broad categories along which manifestations of hybrid threats can be organised: (1) Digital and information warfare, (2) Economic and financial coercion, (3) Paramilitary operations, (4) Physical destruction and violence, and (5) Legal and political activities. Each of these five categories have several manifestations, as exemplified in Table 2 below.

---

52 Živilė Marija Vaicekauskaitė, "Security Strategies of Small States in a Changing World," *Journal on Baltic Security* 3, no. 2 (2017): 8, https://doi.org/DOI%252010.1515/jobs-2017-0006.

53 Diplo, "Diplomacy of Small States," Diplo, 2024, https://www.diplomacy.edu/topics/diplomacy-of-small-states/.

54 North Atlantic Treaty Organization, "Countering hybrid threats"; Giannopoulos et al., *The Landscape of Hybrid Threats*, 10.

Table 2: Categorisation of hybrid threats and their ways of manifesting

Category	Subcategory
Digital and information warfare	Cyber operations and attacks
	FIMI
	Digital espionage
Economic statecraft	Economic coercion or dependence
	Malign finance
Paramilitary operations	Military exercise and build up
	Organised violence (riots, protests, terrorism)
Physical destruction and violence	Arson or explosion (excl. infrastructure)
	Assassination (attempt)
	Sabotage of infrastructure
Legal and political activities	Political undermining
	Lawfare
	Espionage

In recent years, **digital and information warfare** have become central to hybrid threats. Between 2000-2023, global internet connectivity rose from 7% of the world's population to 67%, reflecting the growing reliance of modern societies on digital infrastructure and media.[55]

[55] International Telecommunication Union, "World Bank Open Data," World Bank Open Data, n.d., https://data.worldbank.org.

This expansion provided hybrid threat actors with unprecedented opportunities to manipulate information and digital infrastructure. Specifically, societal stability is highly reliant on the functioning of information and technology systems, making digital warfare a highly efficient tool for disruption.[56] Key tactics include espionage, cyber operations, and disinformation. Cyber operations target sensitive political or commercial data through methods like phishing or malware.[57] For instance, in late June 2013 the DarkSeoul malware wiped data on over 48,000 computers across South Korea – crippling ATMs, banking networks and major media outlets – in a state-linked cyber-attack widely attributed to North Korea.[58]

Meanwhile, disinformation and misinformation campaigns blur the line between perception and reality by disseminating misleading information or half-truths through social media, troll farms, and manipulated news outlets. Examples include Chinese operations such as "Spamouflage" or "Dragonbride", where fake accounts propagate pro-the PRC narratives to manipulate public opinion and foster societal polarisation.[59] Russia also notoriously employs disinformation as a tool to bend public opinion when it comes to its 2022 invasion of Ukraine. Since the beginning of the conflict, Russia used more than 100,000 social-media pages and a network of hundreds of Telegram channels to spread false narratives dismissing reports of Ukrainian war-crimes or civilian atrocities.[60] These efforts are often psychological in nature, exploiting societal fears and prejudices to deepen internal divisions within target populations.[61] However, hybrid tactics can also blend the digital and physical domains, turning digital intrusions into tangible disruptions.

Hybrid threats also leverage the globalised nature of trade, investment and finance through **economic statecraft**. Tactics within this category combine conventional tools of economic statecraft (like trade embargoes and investment blockages) with more opaque tactics that are difficult to attribute directly to state actors and to distinguish from nonintentional market dynamics, such as market interference, manipulation of critical supply chains and selective investments.[62] Such measures target industries that are deemed vital to national security or economic well-being – such as energy, telecommunications or key manufacturing sectors.[63]

---

56 Steven Bowcut, "Cyberwarfare: The New Frontlines," *Cybersecurity Guide*, April 28, 2025, https://cybersecurityguide.org/resources/cyberwarfare/.

57 Cyble, "What Is Cyber Espionage?," Cyble, February 17, 2025, https://cyble.com/knowledge-hub/what-is-cyber-espionage/.

58 Puya Pakshad, "An In-Depth Analysis of a Cyber Attack: Case Study and Security Insights," in *Integrating Artificial Intelligence in Cybersecurity and Forensic Practices* (IGI Global Scientific Publishing, 2025), https://doi.org/10.4018/979-8-3373-0588-2.ch013.

59 Peter Suciu, "China's 'Spamouflage' Aims To Confuse Voters Ahead Of Election," Forbes, September 10, 2024, https://www.forbes.com/sites/petersuciu/2024/09/10/chinas-spamouflage-aims-to-confuse-voters-ahead-of-election/; Olivier Giullard, "China-linked 'Spamouflage' network and the US November election," Institut d'Études de Géopolitique Appliquée, September 18, 2024, https://www.institut-ega.org/l/china-linked-spamouflage-network-and-the-us-november-election/.

60 Dr Ewelina U. Ochab, "Russia's Strategic Disinformation Warfare And War Crimes Cover-Up Campaign," Policy, *Forbes*, June 8, 2025, https://www.forbes.com/sites/ewelinaochab/2025/06/08/russias-strategic-disinformation-warfare-and-war-crimes-cover-up-campaign/.

61 Massimo Flore et al., "Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda" (Brussels: European Commission, 2019), 6-7, https://publications.jrc.ec.europa.eu/repository/handle/JRC116009.

62 Khidasheli, *Hybrid Threats and Resilience: Safeguading Democratic Values in a Connected World*, 10; Marcin Szczepański, *China's Economic Coercion: Evolution, Characteristics and Countermeasures* (European Parliamentary Research Service, 2022), 4, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738219/EPRS_BRI(2022)738219_EN.pdf.

63 See for example: Bureau of Industry and Security, "Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications," December 2, 2024, https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced; The Guardian, "China Likely to Target US Agriculture, State Media Reports, as Trump Tariff Deadline Nears," World News, *The Guardian*, March 3, 2025, https://www.theguardian.com/world/2025/mar/03/china-us-relationship-trump-tariff-deadline-agriculture-impact.

Financial coercion, in turn, includes malign financial practices such as money laundering, elite capture, bribery to promote alignment, and orchestrating capital flight to destabilise a target's currency.[64]

Another tool is referred to as "debt-trap diplomacy", wherein the creditor extends loans on terms that make repayment challenging or sometimes even impossible.[65] This creates leverage over strategic assets or political influence over the indebted state.[66] For instance, the PRC's BRI involves infrastructure loans that often create heavy debt burdens, allowing the PRC to seize strategic assets upon default, as illustrated by the Hambantota Port in Sri Lanka.[67] Beyond their material impacts, these tactics can lead to societal destabilisation in the form of democratic dissatisfaction, as economic distress weakens public confidence in political leaders and institutions.[68]

Operating in a legal and operational grey zone, **paramilitary operations** are usually carried out by non-state actors, private security companies, or covert military units on behalf of the state, granting plausible deniability to the aggressor.[69] These forces are often used to undertake intimidation campaigns, orchestrate small-scale sabotage, infiltrate protests to incite violence, and covertly support societal unrest in target states. For example, Pakistan has also long used proxy militant groups such as Lashkar-e-Taiba, Jaish-e-Mohammed, and the Haqqani Network as deniable paramilitary tools to conduct cross-border sabotage, intimidation, and political destabilisation in India and Afghanistan.[70] In many cases, the objective is to weaken governance structures and the public order, ultimately eroding political cohesion and creating an environment conducive to external influence.[71]

Although hybrid threats are designed to operate below the threshold of conventional warfare, **physical destruction and violence** remain key tactics. These span from targeted sabotage – such as affecting pipelines, communication lines, or other critical infrastructure – to vandalism, assassinations, and orchestrated violence. Chinese and Russian vessels have reportedly been involved in incidents affecting deep-sea cables in the Baltic Sea, and Chinese

64 Aleksi Aho et al., *Hybrid Threats in the Financial System* (European Centre of Excellence for Countering Hybrid Threats, 2020), 14–17, https://www.hybridcoe.fi/wp-content/uploads/2020/07/20200630_Working-Paper-8_Web-1.pdf; Dursun Peksen and Byunghwan Son, "Economic Coercion and Currency Crises in Target Countries," *Journal of Peace Research* 52, no. 4 (2015): 448, https://www.jstor.org/stable/24557431.

65 This term was popularised by Indian scholar Brahma Chellaney in 2017 (see Brahma Chellaney, "China's Global Hybrid War," The Strategist, December 10, 2021, https://www.aspistrategist.org.au/chinas-global-hybrid-war/.). Subsequently, the term has predominantly been used in the Chinese context and has been criticised for being a constructed narrative lacking empirical grounding (see Michal Himmer and Zdeněk Rod, "Chinese Debt Trap Diplomacy: Reality or Myth?," *Journal of the Indian Ocean Region* 18, no. 3 (2022): 250–72, https://doi.org/10.1080/19480881.2023.2195280.).

66 Aaron Onyango, "Debt Trap Diplomacy: How Financial Hegemony Hinders Trade and Development," Trade Finance Global, October 4, 2021, https://www.tradefinanceglobal.com/posts/debt-trap-diplomacy-how-financial-hegemony-hinders-trade-and-development/.

67 Jonathan E. Hillman, "Game of Loans: How China Bought Hambantota," Center for Strategic and International Studies, April 2, 2018, https://www.csis.org/analysis/game-loans-how-china-bought-hambantota.

68 Ignacio Jurado and Rosa M. Navarrete, "Economic Crisis and Attitudes Towards Democracy: How Ideology Moderates Reactions to Economic Downturns," *Frontiers in Political Science* 3 (August 2021): 11, https://doi.org/10.3389/fpos.2021.685199; Manuel Funke and Christoph Trebesch, *Financial Crises and the Populist Right* (ifo Institut, 2017), 8, https://www.ifo.de/DocDL/dice-report-2017-4-funke-trebesch-december.pdf.

69 Uğur Ümit Üngör, "Introduction: Old Wine in New Bottles?," in *Paramilitarism: Mass Violence in the Shadow of the State*, ed. Uğur Ümit Üngör (Oxford University Press, 2020), 7, https://doi.org/10.1093/oso/9780198825241.003.0001; National Intelligence Council, "Updated IC Gray Zone Lexicon: Key Terms and Definitions," National Intelligence Council, July 2024, 8, https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf.

70 Kunwar Khuldune Shahid, "Pakistan and the Latest Reincarnation of Lashkar-e-Taiba," *The Diplomat*, May 31, 2025, https://thediplomat.com/2025/05/pakistan-and-the-latest-reincarnation-of-lashkar-e-taiba/.

71 Costigan and Hennessy, *Hybrid Threats and Hybrid Warfare: Reference Curriculum*, 33.

intelligence operations have targeted dissidents abroad through harassment, surveillance, coercion, and even assassination attempts or forced repatriation.[72] While large-scale attacks such as complete disruption of infrastructure, can create widespread instability, smaller-scale disruptions, like arson, the use of low-cost tools, undermining public transportation, or the plotting of deportations, also have potentially destabilising impacts.[73] Moreover, cyber operations against critical infrastructure can spill over into tangible disruptions, blurring the line between digital and physical attacks. In Norway, for instance, Russian-backed hackers breached the software of a dam used for fish farming, releasing 500 litres of water per second for four hours until the attack was noticed and stopped.[74]

Lastly, **legal and political activities**, sometimes referred to as "lawfare", exploit legal mechanisms and international norms to create narratives of legitimacy or to tie a target state down in lengthy legal disputes, effectively slowing down its ability to respond.[75] Lawfare also involves the exploitation of ambiguities in international law to obstruct diplomatic or economic actions against the aggressor.[76] Russia has utilised this tactic effectively, when in December 2022, it passed a domestic law claiming portions of the Northern Sea Route as Russian internal waters – a reinterpretation of the law of the sea that attempts to legitimise control over Arctic shipping lanes and restrict other states' freedom of navigation.[77] On a domestic level, political subversion takes many forms, including covert financial support for political parties, fostering corruption among key officials, orchestrating media campaigns to influence public opinion, and offering investment to favourable political leaders.[78]

By employing these multifaceted tactics, states can destabilise targets, rendering them more susceptible to influence and control, while minimising the risks and costs associated with conventional warfare.[79] As hybrid tactics evolve, they continue to pose a growing challenge to international security, particularly for SMPs that lack the strength and resources to counter threats. Table 3 summarises the five categories of hybrid threats, their main characteristics and principal tactics.

---

72 Jill Goldenziel, "Law Can't Stop Undersea Cable Cutting by Russia and China," Forbes, February 13, 2025, https://www.forbes.com/sites/jillgoldenziel/2025/02/13/law-doesnt-protect-undersea-cables-russia-and-china-know-it/; United States Department of Justice, "40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents," United States Department of Justice, April 17, 2023, https://www.justice.gov/archives/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us; BBC, "China Says Repatriated Dissidents 'Guilty of Crimes,'" *BBC News*, November 23, 2015, sec. the PRC, https://www.bbc.com/news/world-asia-china-34901965.

73 Nick Paton Walsh et al., "From $7 Graffiti to Arson and a Bomb Plot: How Russia's 'Shadow War' on NATO Members Has Evolved," *CNN*, July 10, 2024, https://www.cnn.com/2024/07/10/europe/russia-shadow-war-nato-intl-latam/index.html. For further examples see: Romansky et al., *New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape*, 8; Reuters, "Murder Plot against Rheinmetall CEO Was Part of Sabotage Campaign, NATO Says," Europe, *Reuters*, January 28, 2025, https://www.reuters.com/world/europe/threat-plot-murder-rheinmetall-ceo-was-part-sabotage-campaign-nato-says-2025-01-28/.

74 Miranda Bryant, "Russian Hackers Seized Control of Norwegian Dam, Spy Chief Says," World News, *The Guardian*, August 14, 2025, https://www.theguardian.com/world/2025/aug/14/russian-hackers-control-norwegian-dam-norway.

75 Douglas Guilfoyle, "The Rule of Law and Maritime Security: Understanding Lawfare in the South the PRC Sea," *International Affairs* 95, no. 5 (September 2019): 1015, https://doi.org/10.1093/ia/iiz141.

76 Jordan Foley, "Multi-Domain Legal Warfare: China's Coordinated Attack on International Rule of Law," Lieber Institute West Point, May 28, 2024, https://lieber.westpoint.edu/multi-domain-legal-warfare-chinas-coordinated-attack-international-rule-law/.

77 Omer Duru and Jill Goldenziel, "Countering Russian Lawfare and Gray Zone Operations," *Just Security*, March 3, 2025, https://www.justsecurity.org/108588/countering-russian-lawfare-and-gray-zone-operations/.

78 Khidasheli, *Hybrid Threats and Resilience: Safeguading Democratic Values in a Connected World*, 10.

79 Sanz-Caballero, "The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe," 3; Jokinen and Normark, *Hybrid Threats from Non-State Actors: A Taxonomy*, 6; European Centre of Excellence for Countering Hybrid Threats, *Frequently Asked Questions on Hybrid Threats*, 1.

Table 3: Summary of hybrid threats categorisation

Category	Core Characteristics	Principal tactics
Digital and information warfare	Central pillar of hybrid activity enabled by global digital dependence	Cyber espionage, infrastructure intrusions, disinformation and misinformation
Economic statecraft	Use of economic statecraft and opaque financial tools to create leverage	Trade embargoes, investment restrictions, supply-chain manipulation, money laundering, bribery, capital flight
Paramilitary operations	Activities in the grey zone using non-state proxies or deniable units	Intimidation, sabotage, infiltration of protests, support to unrest
Physical destruction and violence	Targeted attacks below conventional warfare thresholds	Sabotage of infrastructure, vandalism, harassment, coercion, assassinations
Legal and political activities	Manipulation of legal frameworks and political systems to generate strategic advantage	Use of domestic laws for external claims, exploitation of legal ambiguity, political subversion, espionage.

2. The PRC's shadow: tracing Chinese hybrid threats across Europe and the Asia-Pacific

The PRC's hybrid threat strategies present complex challenges to regional stability and broader international security. Through hybrid tactics, Beijing alters the facts on the ground to its advantage, undermining the unity of opposing coalitions, and expanding its global influence in a manner that traditional military power alone could not easily achieve. This gradual accumulation of advantages poses a strategic challenge to other powers, particularly SMPs.[80] In the context of escalating great power competition, SMPs find themselves increasingly vulnerable to hybrid threats exploiting their economic, societal, and institutional weaknesses.[81] Unlike larger powers that can invest heavily in multi-domain defence mechanisms, SMPs have more limited economic and power bases and must adopt alternative strategies to mitigate risks, deter aggressors, and maintain their sovereignty.[82] As the PRC strives to become the dominant power in the Asia-Pacific, SMPs in the region have been particularly targeted by Chinese hybrid threats. Simultaneously, the PRC increasingly targets SMPs on the European continent, focusing on specific industries or favourable regimes to increase its global influence.

Still, while Russia's hybrid tactics have been widely analysed in Europe, the PRC's strategies remain comparatively underexplored. Whereas both Russia and the PRC employ hybrid tactics to achieve strategic objectives and expand their sphere of influence, their approaches and aims differ. Examining the PRC's hybrid approach is therefore essential to grasp the breadth and complexity of the contemporary hybrid threat landscape. This section looks into the PRC's use of hybrid tactics in Europe and the Asia-Pacific. It starts by giving a regional overview of the threat landscape in the two regions. It then proceeds with a comparative analysis of the two theatres through a threat-based approach.

---

80 Aukia et al., "Strings Attached: the PRC's Narrative Influence in Sub-Saharan Africa," 13.

81 Vaicekauskaitė, "Security Strategies of Small States in a Changing World," 8.

82 Constantinos Adamides and Petros Petrikkos, "Small European States in the Hybrid Warfare Era: The Cases of Cyprus, Malta, and Estonia," *Small States & Territories* 6, no. 1 (2023): 25, https://www.um.edu.mt/library/oar/bitstream/123456789/109186/1/SST6%281%29A2.pdf; Tomorr Sinani and Bardhyl Hoxha, "The Security Strategy of Small States in the 21st Century and Beyond," *Academic Journal of Business, Administration, Law and Social Sciences* 11, no. 1 (2025): 47, https://doi.org/10.2478/ajbals-2025-0004.

The analysis is carried out on the basis of a comprehensive database mapping hybrid threats across 50 different SMPs in the Asia-Pacific and Europe. The database, compiled through open-source research, collects confirmed Chinese hybrid threats incidents across the five main domains of hybrid activity described in Section 1 of this report and summarised in Table 3. For each incident, the database offers information on who was targeted, what tactic was used, when it occurred, which sector it struck and what strategic effect it sought. Through the threat-based analysis and in-depth case studies, this section showcases a comprehensive picture of how the PRC adapts its tactics to exploit country-specific vulnerabilities, economic dependencies, or political sensitivities. The database's results are also visualised in a connected dashboard.[83]

2.1. The PRC's hybrid strategy: a comprehensive approach to global influence

To fully understand the PRC's approach to hybrid threats, it is essential to situate them within the country's broader strategic objectives, recognising that these threats are tools for achieving those goals. The PRC, as a long-term thinking strategic actor has grounded its use of hybrid threats into a solid doctrinal foundation, while adapting the implementation of hybrid tactics to local realities of targeted states through synchronised efforts. To accurately understand the effect of such strategy, the analysis needs to be necessarily informed by cultural and political framing.

2.1.1. Doctrinal foundation

When comparing the approaches of the PRC and Russia to hybrid threats, key distinctions can be observed, underpinned by differing national strategies and capabilities alike. Russia's hybrid tactics often involve direct interference, leveraging historical and cultural ties in its neighbourhood.[84]Meanwhile, the PRC's approach to hybrid threats focuses principally on economic enticements, legal instruments, and information manipulation.[85] This tactical patience reflects the PRC's strategic culture and long-term vision of incrementally altering the international order and cementing its position within it.[86]

This is closely tied to the PRC's complex relationship with the post-World War II order. The PRC has benefitted from access to global markets and international institutions that facilitated its economic development. Yet, the Chinese Communist Party (CCP) remains dissatisfied with constraints on its regional dominance and ideological legitimacy.[87] This dual stance, a

83 Chinese Latent Activity and Related Interference Scanner, The Hague Centre for Strategic Studies, https://claris.app.hcss.nl/.

84 Javier Sutil Toledano, "The Use of Hybrid Warfare to Achieve Strategic Objectives: Comparing Russian and Chinese Approaches" (Charles University, 2023), 71–75, https://dspace.cuni.cz/handle/20.500.11956/187366.

85 KCS Group Asia, "Hybrid Warfare – the Coordinated Efforts of Russia and the PRC against the West."

86 Bonnie Glaser and Khairulanwar Zaini, "the PRC as a Selective Revisionist Power in the International Order," Perspective (Singapore: Yusof Ishak Institute, April 5, 2019), 8, https://www.iseas.edu.sg/wp-content/uploads/pdfs/ISEAS_Perspective_2019_21.pdf.

87 Suisheng Zhao, "A Revisionist Stakeholder: the PRC and the Post-World War II World Order," *Journal of Contemporary the PRC* 27, no. 113 (September 3, 2018): 643, https://doi.org/10.1080/10670564.2018.1458029.

mix of integration and revisionism, is manifested in the PRC's hybrid approach. Rather than overtly dismantling the system that enabled its rise, Beijing operates within and around it, using sub-threshold tactics to erode aspects of the world order it deems unfair or harmful to its interests.[88]

Over time, the PRC has greatly enhanced its economic and military capabilities to assert influence on a global scale. Economically, the BRI has extended the PRC's reach into every continent, creating dependencies through infrastructure investments and trade relationships.[89] Between 2013 and 2022, the PRC invested around $679 billion across 150 countries and has an estimated outstanding borrower debt between $1.1 trillion and $1.5 trillion.[90] Militarily, the PRC has also expanded its presence in the South China Sea by constructing artificial islands, also referred to the "Great Wall of Sand", and by establishing overseas military bases.[91]

In addition to tangible assets, the PRC employs hybrid tactics that leverage political and informational tools to influence international norms and perceptions.[92] This strategy is deeply rooted in historical doctrines, such as Sun Tzu's emphasis on "breaking the enemy's resistance without fighting" and the maxim that "all warfare is based on deception".[93] Throughout its history, Imperial China used tactics akin to hybrid threats to advance its interests, notably the "four methods approach." This entailed (1) the division of foreigners ("barbarians"), (2) the dissuasion of foreign leaders from attacking the PRC through bribes and tribute, (3) the establishment of fortifications, and finally, (4) military intervention.[94] The contemporary equivalents of these tactics include diplomatic pressure, support for local insurgencies, the PRC's aid policy, the creation of artificial islands and control over strategic areas.[95] Based on Chinese strategic doctrine, the notion of hybrid threats can be considered as a comprehensive way of indirectly confronting adversaries through different domains.[96]

Modern manifestations of such strategies are rooted in the PRC's adoption of "unrestricted warfare" and the "Three Warfares" doctrine. The concept of "unrestricted warfare" was coined by two People's Liberation Army (PLA) colonels in 1999. In their eponymous book, they pointed to the transformed nature of the battlefield where key actors in conflict are no longer

88 Glaser and Zaini, "the PRC as a Selective Revisionist Power in the International Order," 7.

89 Center for Strategic and International Studies, "How Will the Belt and Road Initiative Advance China's Interests?," the PRC Power Project - Center for Strategic and International Studies, May 8, 2017, https://chinapower.csis.org/china-belt-and-road-initiative/.

90 U.S. Government Accountability Office, "China's Foreign Investments Significantly Outpace the United States. What Does That Mean?," U.S. Government Accountability Office, October 16, 2024, https://www.gao.gov/blog/chinas-foreign-investments-significantly-outpace-united-states.-what-does-mean.

91 Michael Paul, "A 'Great Wall of Sand' in the South China Sea?" (Berlin: German Institute for International Security Affairs, July 2016), 13, https://www.swp-berlin.org/publikation/a-great-wall-of-sand-in-the-south-china-sea; Asia Maritime Transparency Initiative, "China Island Tracker," Asia Maritime Transparency Initiative, n.d., https://amti.csis.org/island-tracker/china/; Aadil Brar, "Map Shows Countries Where China Seeks Overseas Military Base," *Newsweek*, March 12, 2024, sec. World, https://www.newsweek.com/china-overseas-military-bases-us-intelligence-1878183.

92 Jukka Aukia, "China as a Hybrid Influencer: Non-State Actors as State Proxies" (Helsinki: European Centre of Excellence for Countering Hybrid Threats, June 2021), 7, https://www.hybridcoe.fi/publications/hybrid-coe-research-report-1-china-as-a-hybrid-influencer-non-state-actors-as-state-proxies/.

93 Sun Tzu, *The Art of War*, 2nd ed. (Norderstedt: BoD – Books on Demand, 2020), 8, 11.

94 Benjamin D. Baker, "Hybrid Warfare With Chinese Characteristics," *The Diplomat*, September 23, 2015, https://thediplomat.com/2015/09/hybrid-warfare-with-chinese-characteristics/.

95 Amrita Jash, "Fight and Win Without Waging a War: How the PRC Fights Hybrid Warfare," *CLAWS Journal* 12, no. 2 (2019): 98–99, https://www.neliti.com/publications/327319/.

96 Nils Peterson, *The Chinese Communist Party's Theory of Hybrid Warfare* (Institute for the Study of War, 2023), 1, https://www.understandingwar.org/sites/default/files/The%20Chinese%20Communist%20Party%27s%20Theory%20of%20Hybrid%20Warfare_0.pdf.

limited to military engagements. They identified various threats, including financial, smuggling, cultural, media, technological, psychological, environmental, legal and economic aid threats.[97] This concept subsequently laid the foundation for the development of the "Three Warfares" doctrine, as put forward by the CCPs Central Committee and Central Military Commission in the Political Work Regulations. These documents, from 2003 and 2010 respectively, constitute a code of conduct of political warfare for the PLA.

The "Three Warfares" doctrine encompasses: (1) public opinion warfare, (2) psychological warfare, and (3) legal warfare, culminating in seven strategic objectives: (1) controlling public opinion, (2) undermining the determination of the adversary, (3) transformation of emotion, (4) psychological guidance, (5) achieving the collapse of the organisation of the adversary, (6) psychological defence, and (7) legal restrictions.[98] By controlling narratives, influencing perceptions, and exploiting legal frameworks, the CCP seeks to advance its interests globally while minimising the risks associated with overt military engagements.[99]

2.1.2. Synchronised and locally enabled implementation

Chinese doctrinal approaches to hybrid threats translate in practice in the synchronisation of combined tactics through the simultaneous use of several hybrid threats. This gives the PRC larger leverage and allows for a strong push of its interests.[100] In Taiwan for example, sequences of threats involving cyber-warfare, economic sanctions and military buildup aim to create larger destabilisation and make responding to these attacks proportionally difficult for the island. In 2022, the PRC engaged in a large campaign of threat and destabilisation against Taiwan following Pelosi's visit to the island, and her statement reaffirming support for the "vibrant Taiwanese democracy".[101] The PRC responded with military exercises encircling Taiwan, economic threats and cyber-attacks. Similarly, synchronisations of attacks targeted Lithuania in 2021 as retaliation for the opening of a Taiwan Representative Office in Vilnius, combining cyber-attacks with economic sanctions and diplomatic isolation in order to exercise domestic political pressure. These effects were largely felt by large parts of the Lithuanian society and various sectors who openly called for better relations with the PRC.[102]

The combination of threats employed varies greatly depending on the perceived capabilities of the targeted states, their geographic proximity to the PRC, the strategic importance of the target, and overall escalation risks. For instance, Beijing is keener on utilising a combination of digital warfare and economic statecraft in Europe, while Asia-Pacific states are also targeted with paramilitary operations in conjunction with disinformation and cyber efforts to ensure greater societal destabilisation. Beijing's ability to implement several tactics simultaneously hinges on its ability to exploit not only its national capabilities but also local actors in target

97 Jash, "Fight and Win Without Waging a War," 101.

98 Kania, *The PLA's Latest Strategic Thinking on the Three Warfares*.

99 Pieter Zhao, "Chinese Political Warfare: A Strategic Tautology? The Three Warfares and the Centrality of Political Warfare within Chinese Strategy," The Strategy Bridge, August 28, 2023, https://thestrategybridge.org/the-bridge/2023/8/28/chinese-political-warfare-a-strategic-tautology.

100 Sikander Naseeb, "Hybrid Warfare: Blurring the Lines Between Conventional and Non-Conventional Tactics," *International Journal for Conventional and Non-Conventional Warfare* 1, no. 1 (2024): 46.

101 Paul Mozur et al., "Nancy Pelosi Arrives in Taiwan, Drawing a Sharp Response From Beijing," U.S., *The New York Times*, August 2, 2022, https://www.nytimes.com/2022/08/02/us/politics/nancy-pelosi-taiwan-beijing.html.

102 Matthew Reynolds and Matthew P. Goodman, "China's Economic Coercion: Lessons from Lithuania," *CSIS*, June 5, 2022, https://www.csis.org/analysis/chinas-economic-coercion-lessons-lithuania.

countries.[103] These are fundamental agents of Chinese influence and contribute to extend the reach of Chinese hybrid threats.

The PRC regularly exploits diaspora communities both as a target audience and as a vehicle of influence, especially through state-controlled media and information campaigns. In some cases, the PRC illegally implemented "police stations" to survey the Chinese diaspora and ensure non-spreading of anti-PRC narratives.[104] In addition, the PRC has also implemented information warfare through the promotion of PRC-controlled media, especially in countries with large mandarin-speaking communities.[105]

The bribing of local elites to promote PRC-favourable ideas and narratives is also an example of local actors' exploitation in what is known as "elite capture".[106] Hybrid threats have also been carried out through commercial entities directly or indirectly linked to the PRC. The use of companies, particularly state-owned enterprises, has facilitated the acquisition of strategic positions outside mainland China.[107]

Building on its use of commercial entities to extend its influence, the PRC has also sought to strengthen its reach across various domains, including academia. The PRC has supported the establishment of organisations that promote pro-China narratives, such as the Confucius Institute, which organises cultural and educational events while advocating for Chinese policies.[108] In addition to these efforts, China has been involved in several academic projects and research institutes.[109]

In conclusion, the PRC's approach to hybrid threats is rooted in a long-term doctrinal view that facilitates the strategic synchronisation of multiple tactics to destabilise its target states. By combining these methods, China not only maximises its leverage but also makes it more difficult for target countries to respond effectively, a characteristic aspect of the hybrid threat toolkit. A central component of this approach is the use of local actors, such as commercial entities, elites, and diaspora communities, which help extend the PRC's influence and amplify the impact of its hybrid strategies. This ability to coordinate various forms of pressure, while leveraging local actors to further its aims, is reflective of Beijing's broader strategy of exerting influence and reshaping regional and global dynamics in a gradual, indirect manner.

---

103 Andrew Mumford, "Proxy Warfare and the Future of Conflict," *The RUSI Journal* 158, no. 2 (2013): 44, https://doi.org/10.1080/03071847.2013.787733.

104 Euronews and AFP, "Netherlands Orders Closure of 'illegal Chinese Police Stations' in Amsterdam and Rotterdam," Euronews, November 2, 2022, https://www.euronews.com/2022/11/02/netherlands-orders-closure-of-illegal-chinese-police-stations-in-amsterdam-and-rotterdam.

105 "Malaysia: Beijing's Global Media Influence 2022 Country Report," Freedom House, 2022, https://freedomhouse.org/country/malaysia/beijings-global-media-influence/2022.

106 Jenni Marsh, "The Rise and Fall of a Belt and Road Billionaire," CNN, accessed September 19, 2025, https://edition.cnn.com/interactive/2018/12/asia/patrick-ho-ye-jianming-cefc-trial-intl/.

107 "A Tale of Two Reams: Questions Remain at Cambodia's Growing Naval Base," *Asia Maritime Transparency Initiative*, n.d., accessed September 19, 2025, https://amti.csis.org/a-tale-of-two-reams-questions-remain-at-cambodias-growing-naval-base/.

108 Ágota Révész, "The Pandora's Box of Fudan Hungary," *Daedalus* 153, no. 2 (2024): 207–16, https://doi.org/10.1162/daed_a_02084.

109 Robert Chesal, "Mensenrechtencentrum VU Amsterdam wordt opgedoekt na kritisch rapport," *NOS*, July 11, 2022, https://nos.nl/artikel/2436278-mensenrechtencentrum-vu-amsterdam-wordt-opgedoekt-na-kritisch-rapport.

2.2. A shifting landscape: Chinese hybrid tactics across Europe and the Asia-Pacific

The implementation of a synchronised, locally enabled approach to hybrid threats allows China to extend its influence globally by targeting multiple regions simultaneously[110] The employment of hybrid tactics in the Asia-Pacific and Europe represent particularly interesting analytical and comparative cases.

The former is the theatre closest to the PRC and the one Beijing needs to control if it wishes to cement its status as the regional superpower. This is not an easy feat, considering the proximity to the US, who has allies and military bases in the region, and the corresponding high risks of escalation. Employing hybrid tactics here allows Beijing to assert influence while avoiding direct confrontations that might escalate into a regional conflict. The PRC's hybrid campaigns are thus most intense in the Asia-Pacific, where its core national interests – territorial sovereignty claims, regional hegemony, and unification with Taiwan – are at stake. Here, the PRC's approach blends economic and informational tools but with an overt paramilitary presence, creating a spectrum of pressure on neighbouring SMPs.[111]

The PRC's hybrid activities have also made inroads into Europe, primarily driven by economic interests and the strategic objective of countering US influence. Europe's central role in global trade and its intricate alliances make it a critical arena for the PRC to project power, cultivate dependencies, and neutralise potential challenges to its influence.[112] For Beijing, exercising influence in Europe is hence not only a matter of economic gains, but also of weakening historic ties to the US. Geographic distance has made the PRC's approach more subtle, and largely based on economic statecraft, cyber espionage, and information manipulation carried out by local actors including governments, companies, and diaspora communities.[113]

While Chinese strategic objectives differ in targeting Europe and the Asia-Pacific, both regions are home to several SMPs with varying degrees of ties to the PRC as well as economic and political vulnerabilities. These states are the perfect testing grounds for Beijing's efforts to exert foreign policy influence through hybrid threats. By examining cross-regional trends, one can better understand how China adapts its hybrid warfare tactics to local contexts while pursuing its overarching global ambitions. The HCSS database allows to compare trends across regions through a threat-based approach to Chinese use of hybrid threats in Europe and the Asia-Pacific.[114] From the analysis of the data collected, a series of observations emerge.

---

110 See U.S. Government Accountability Office, "the PRC's Foreign Investments Significantly Outpace the United States. What Does That Mean?"

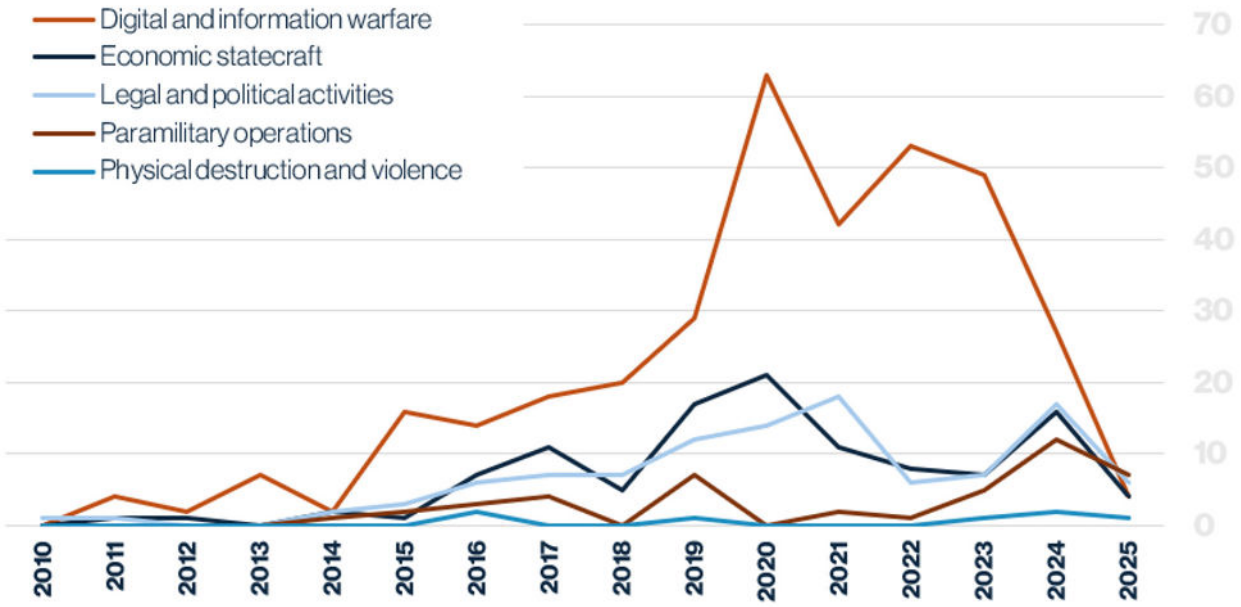
111 Nathan Attrill, "To Counter China's Coercion of Taiwan, We Must Track It Better," The Strategist, March 28, 2025, https://www.aspistrategist.org.au/to-counter-chinas-coercion-of-taiwan-we-must-track-it-better/.

112 William Lt. Col. (Ret.) Hagestad II, "Countering China in Europe," per Concordiam, September 12, 2024, https://perconcordiam.com/countering-china-in-europe/.

113 KCS Group Asia, "Hybrid Warfare – the Coordinated Efforts of Russia and China against the West."

114 Chinese Latent Activity and Related Interference Scanner, The Hague Centre for Strategic Studies, https://claris.app.hcss.nl/.

Figure 7: Number of events per threat type across Europe and Asia-Pacific (2010-2025)[115]



Source: China Latent Activity and Related Interference Scanner

Across both Europe and the Asia-Pacific, Beijing makes heavy use of **digital and information warfare** tactics. In Europe this is enabled by the high European dependence on digital infrastructure which the PRC has highly exploited over the years. Through proxy actors, it has led various cyber operations, specifically in Western Europe, aiming to steal sensitive data of government, private companies and the general public to compromise and disturb activity. It has also made use of this overreliance on digital system to conduct digital espionage and ransomware, such as in the Netherlands where it has employed proxies to collect intelligence on opposing parties' arguments in the Arbitration Court of the Hague, or on NXP, exfiltrating chip designs.[116]

In the Asia-Pacific, the PRC has made use of the weak media literacy combined with high smartphone and social media penetration rates.[117] The Chinese government's actions particularly targeted electoral processes and disrupted the political and economic life of citizens, especially in key targets. In Taiwan, FIMI was used to manipulate public opinion in a campaign targeting over 40 major temples, accused of coordination with the Chinese Religious Affairs Administration.[118] In Cambodia, the PRC influenced the 2023 presidential election results to maintain the pro-PRC candidate in the government.

115 Digital incidents are the most frequently recorded in this dataset, in part because they are easier to detect and attribute than other forms of hybrid activity. This may introduce reporting bias, but the figures remain indicative of relative patterns and frequency.

116 "Chinese State-Affiliated Hackers Attack Permanent Court of Arbitration," Alliance For Securing Democracy, July 2015, https://securingdemocracy.gmfus.org/incident/chinese-state-affiliated-hackers-attack-permanent-court-of-arbitration/; "Chinese Hacker Group Chimera Accessed IT System of Dutch Semiconductor Manufacturer NXP during 2017-2020," EuRepoC: European Repository of Cyber Incidents, November 28, 2023, https://eurepoc.eu/table-view/.

117 Azaz Zaman, "How Digitalization Is Making South and Southeast Asia Engines of Growth," World Economic Forum, February 10, 2022, https://www.weforum.org/stories/2022/02/digitalization-south-southeast-asia/.

118 James Pomfret and Yimou Lee, "China Wields Mazu 'peace Goddess' Religion as Weapon in Taiwan Election," *Reuters*, December 21, 2023, https://www.reuters.com/world/asia-pacific/china-wields-peace-goddess-religion-weapon-taiwan-election-2023-12-21/; European Repository of Cyber Incidents, "Leviathan Aka TEMP. Periscope Aka APT 40 Influences on the Election in Cambodia," August 2022, https://eurepoc.eu/table-view/.

These regional patterns reveal broader trends in the PRC's hybrid approach. Cyber operations are generally easier to detect and attribute than disinformation, which makes Beijing's activities highly visible. Since 2015, cyberattacks have accelerated sharply for both Europe and the Asia-Pacific, peaking around 2020 with over 60 recorded incidents, a surge coinciding with heightened geopolitical tensions and the onset of the COVID-19 pandemic. [119] Small and mid-sized powers in the Asia-Pacific remain more frequent and aggressive targets than European states, reflecting their geographic proximity, the potential for synchronised tactics, and lower investment in cyber-resilient infrastructure. [120]

Economic statecraft also reflects one of the most prominent hybrid tactics used by the PRC across Europe and the Asia-Pacific. In the last ten years, the PRC used economic statecraft in a cyclical manner, with incidents spiking during trade disputes. This trend highlights the PRC's ability to exploit its economic links in moment of needs to bend international governance in its favour. This is especially the case with SMPs for which the PRC represents one of, if not *the* most important trading partner.[121] States in both the Asia-Pacific and Europe depend heavily on Chinese imports/exports, and Beijing knows how to exploit these dependencies tiptoeing the line between economic coercion and business. Since 2020, following a diplomatic disagreement regarding Gui Minhai, a Hong Kong-Swedish book publisher and writer, the PRC has imposed an unofficial ban on graphite exports to Sweden. This decision is now suspected to be motivated by additional economic purposes, in relation to a surge of Chinese battery investments in Europe.[122]

While vulnerability is high across the board, in Western Europe these tactics are mostly detrimental to diplomatic relations and can cause supply chain delays; certain countries in Asia-Pacific and Eastern Europe are however at risk of a debt trap, with the impossibility of ensuring repayment leading to Chinese control over key industries and areas.[123] This is the strategy employed by the PRC in Sri Lanka, where it has invested over 3.9B in 4 port infrastructure development projects as part of the BRI.[124] Sri Lanka's inability to repay its debts resulted in the government giving to the PRC in 2017 a controlling equity stake for Hambantota port with a 99-year lease.[125] This is a clear strategy for the PRC to obtain control over strategic locations, resources and infrastructures as a repayment for being involved in the economic development of SMPs.

Many of the PRC's economic statecraft strategies go hand in hand with **legal and political activity**. While both Europe and the Asia-Pacific are subjects to Chinese attempts at bending legal frameworks, influencing local politics, and gathering sensitive information, differences between the two regions exist. In Europe, the PRC focuses mainly on political undermining,

119 "Coronavirus Malware: Cyber Threats Rising," Okta, November 3, 2024, https://www.okta.com/identity-101/coronavirus-malware/.

120 "World Bank Country Classifications by Income Level for 2024-2025," World Bank Blogs, accessed September 9, 2025, https://blogs.worldbank.org/en/opendata/world-bank-country-classifications-by-income-level-for-2024-2025.

121 Brunello Rosa, 'Why China Is Poised for Macroeconomic Dominance – and What That Might Mean for the Rest of the World. | LSE Executive Education', geraadpleegd 18 september 2025, https://www.lse.ac.uk/study-at-lse/executive-education/insights/articles/why-china-is-poised-for-macroeconomic-dominance-and-what-that-might-mean-for-the-rest-of-the-world.

122 "Why Is China Blocking Graphite Exports to Sweden?," *The Economist*, June 22, 2023, https://www.economist.com/business/2023/06/22/why-is-china-blocking-graphite-exports-to-sweden.

123 Keith Barney e.a., 'Trapped in debt: China's role in Laos' economic crisis | Lowy Institute', *Lowy institute*, 13 april 2025, https://www.lowyinstitute.org/publications/trapped-debt-china-s-role-laos-economic-crisis.

124 Zongyuan Zoe Liu, "Tracking China's Control of Overseas Ports," *Council on Foreign Relations*, n.d., accessed December 3, 2025, https://www.cfr.org/tracker/china-overseas-ports.

125 Jonathan E. Hillman, *Game of Loans: How China Bought Hambantota*, February 4, 2018, https://www.csis.org/analysis/game-loans-how-china-bought-hambantota.

as exemplified by several instances of bribes in Belgium, with the involvement of Huawei in espionage cases or direct engagement with political figures such as Filip Dewinter, leading member of the Vlaams Belang party.[126] In 2023, a member of the same party was evicted for allegedly spying for the PRC, resulting in large tensions in the Belgian parliament regarding the safeguarding of autonomy and sovereignty from corruption by the PRC.[127]

Lawfare is a key strategy for the PRC and its use is more prominent is the Asia-Pacific, with frequent Chinese attempts to manipulate weak legal frameworks by shaping decisions and laws which favour its economic, military, and political interests. In recent years, the PRC has exploited and distorted international and domestic law to justify its expansive maritime claims – including its "nine-dash line" in the South China Sea – presenting legally baseless claims as legitimate under international norms.[128]

Further differences between Chinese hybrid operations in the Asia-Pacific and Europe emerge when looking at the extension of hybrid tactics to the physical realm. These PRC-associated **paramilitary operations** principally target SMPs in the Asia-Pacific. A prominent example is the deployment of paramilitary groups in the South China Sea in areas of contested sovereignty.[129] These operations primarily involve military exercises and buildups, which have been gradually increasing since 2016, following the Permanent Court of Arbitration's rejection of the PRC's claims over the nine-dashed line and historic rights over the South China Sea in a case against the Philippines.[130] Since then, the PRC carried out several incursions through paramilitary groups in the territorial waters of Taiwan, Vietnam, Malaysia, and the Philippines as well as around contested areas such as the Scarborough Shoal, Paracel Islands, Spratly Islands, and Senkaku Islands.[131] The PRC's reach and ability to organised paramilitary operations on the European content is limited by geographic distance.[132]

Lastly, **physical destruction and violence** is rarely used by the PRC and mainly manifests in the damaging of underwater infrastructure. Attributing the cutting of undersea cables and pipelines is complicated due to lack of judicial clarity, but some instances clearly framed the PRC as the perpetrator of such actions. In 2024 for example, Chinese vessel Yi Peng 3 was suspected of having deliberately dragged an anchor along the seabed to destroy a fibre optic cable linking Lithuania Germany, Sweden and Finland. While the PRC permitted observation

---

126 Redactie, "Documenten bewijzen: Filip Dewinter werkte in opdracht van Chinese Communistische Partij," Humo: The Wild Site, March 25, 2024, https://www.humo.be/nieuws/documenten-bewijzen-filip-dewinter-werkte-in-opdracht-van-chinese-communistische-partij-b92fcada/; Atalayar, "Huawei, the Trojan Horse of Chinese Espionage," Atalayar, July 21, 2025, https://www.atalayar.com/en/articulo/gustavo-aristegui/huawei-the-trojan-horse-of-chinese-espionage/20250721092801216916.html.

127 *Belgische politicus was jarenlang informant Chinese geheime dienst*, December 15, 2023, https://nos.nl/artikel/2501666-belgische-politicus-was-jarenlang-informant-chinese-geheime-dienst.

128 Jordan Foley, "Multi-Domain Legal Warfare: China's Coordinated Attack on International Rule of Law," *Lieber Institute West Point*, May 28, 2024, https://lieber.westpoint.edu/multi-domain-legal-warfare-chinas-coordinated-attack-international-rule-law/.

129 Richard A. Bitzinger, 'China's Militarisation of the South the PRC Sea: Creating a Strategic Strait?', *Nanyang Technological University* 221 (2016): 1.

130 News Agencies, 'Chinese, Philippine Ships Collide near Disputed Shoal in South China Sea', Al Jazeera, geraadpleegd 18 september 2025, https://www.aljazeera.com/news/2025/9/16/chinese-philippine-ships-collide-near-disputed-shoal-in-south-china-sea.

131 Esther E. Song and Sung Eun Kim, "China's Dual Signalling in Maritime Disputes," *Australian Journal of International Affairs* 78, no. 5 (2024): 660–82, https://doi.org/10.1080/10357718.2024.2394179; "Timeline: China's Maritime Disputes," Council on Foreign Relations, 2023, https://www.cfr.org/timeline/chinas-maritime-disputes; Nong Hong, "China's Maritime Law Enforcement Reform and Its Implication on the Regional Maritime Disputes," *Asia Maritime Transparency Initiative*, April 1, 2015, https://amti.csis.org/chinas-maritime-law-enforcement-reform-and-its-implication-on-the-regional-maritime-disputes/.

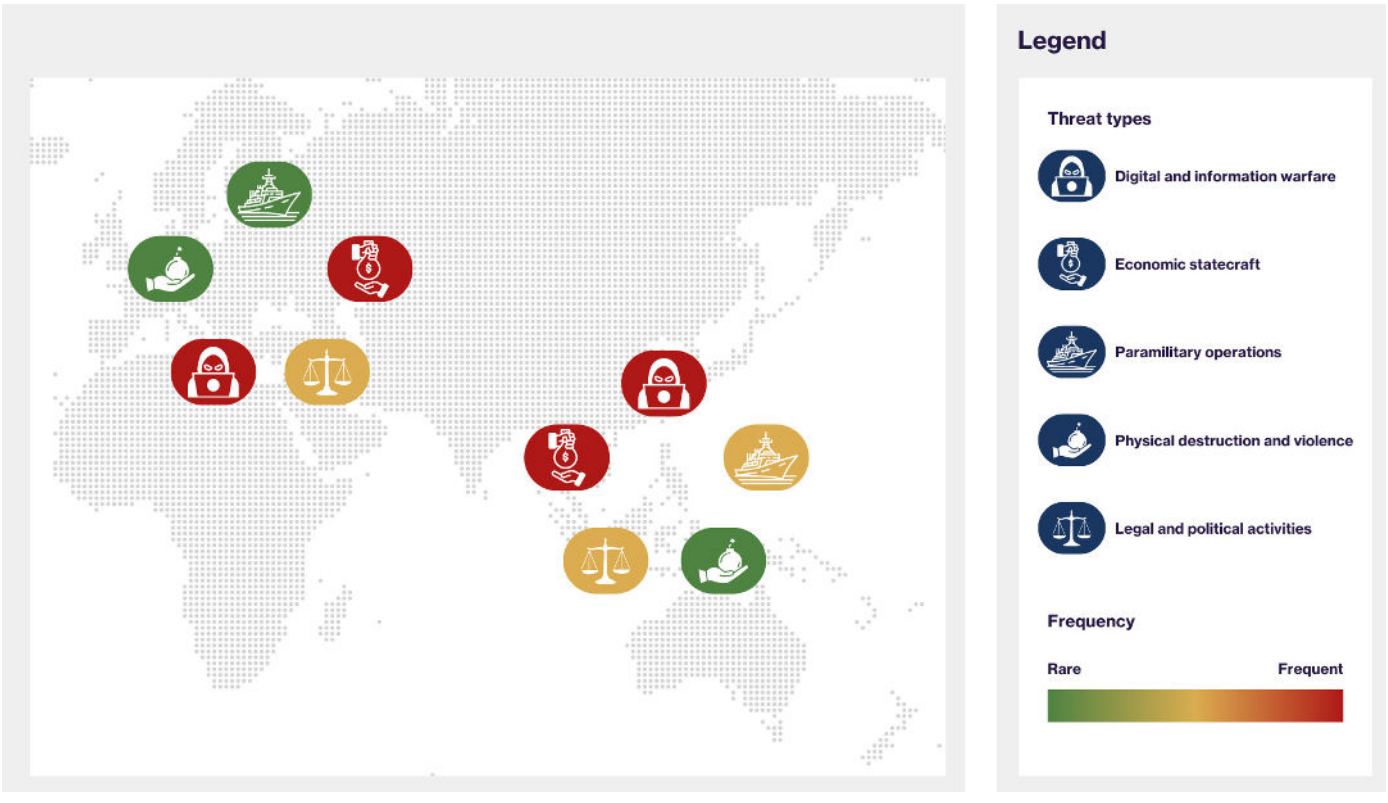
132 Mark Scott et al., "European Commission Accuses China of Peddling Disinformation," *POLITICO*, June 10, 2020, https://www.politico.eu/article/european-commission-disinformation-china-coronavirus/.

over their own inquiry, the government denied the ability for countries to conduct their own investigation on Yi Peng 3.[133]

Taken together, the PRC's hybrid tactics reveal a highly adaptive, context-sensitive, and regionally differentiated approach to exerting influence and reshaping the international order. Across Europe and the Asia-Pacific, Beijing leverages a combination of tactics tailored to the vulnerabilities and strategic significance of each target, as visible in Figure 8. In Europe, the emphasis on digital exploitation, political interference, economic coercion, and elite capture reflects both geographic distance and the relative robustness of European security infrastructures, whereas in the Asia-Pacific, hybrid tactics are intensified through paramilitary presence, lawfare, and economic coercion, underscoring the PRC's prioritisation of its immediate regional sphere. Across both theatres, the integration of local actors, diaspora networks, and commercial entities amplifies the reach and impact of these campaigns, blurring the lines between state and non-state instruments of power.

This underscores that the PRC's hybrid approach is less a series of isolated threats, but rather a deliberate, long-term orchestration of multi-domain pressures designed to exploit systemic weaknesses, advance strategic objectives, and incrementally alter regional and global power balances –all while remaining largely below thresholds that would provoke conventional military confrontation.

Figure 8: Frequency of Hybrid Threats used by PRC in Europe and Asia-Pacific



133 Miranda Bryant and Miranda Bryant Nordic correspondent, "Sweden Seeks Clarity from China about Suspected Sabotage of Undersea Cables," World News, *The Guardian*, November 28, 2024, https://www.theguardian.com/world/2024/nov/28/sweden-seeks-clarity-from-china-about-suspected-sabotage-of-undersea-cables.

3. Hybrid pressure, strategic responses: how SMPs react to Chinese hybrid threats

To navigate the complex threat environment described above, SMPs rely on a combination of methods, including the creation of dedicated counter-hybrid units, the drafting of strategies and the establishment of relevant legal frameworks to enhance detection and response coordination. This has enabled them to undertake measures to deter future violations and minimise the effectiveness of hybrid tactics.[134] Still, in both Europe and the Asia-Pacific most of the measures against hybrid threats occur in an ad-hoc manner, only after an incident has taken place, rather than as part of consistent defence and mitigation strategy against such threats in ways that increase a state's resilience against future threats.

Resilience serves as a critical tool for SMPs in managing and mitigating hybrid threats.[135] At its core, resilience refers to the ability of states to withstand, adapt to, and recover from hybrid attacks.[136] This extends beyond traditional military defence and encompasses a whole-of-society approach, including the psychological, institutional, and infrastructural strengths that allow society to function amidst and after disruptive activities.[137] For resilience to be achieved, however, there must be constant attention to a variety of potential threats, rather than merely reactive actions. In fact, purely reactive measures risk amplifying the damage incurred from a hybrid threat – whether direct, by allowing excessive time to elapse, or reputational, in terms of public perceptions – potentially undermining the resilience of a state more than the hybrid disruptions themselves. By strengthening their internal structures, SMPs can reduce their susceptibility to hybrid operations while maintaining stability in the face of external pressure.[138]

134 Bertolini et al., *Ten Guidelines for Dealing with Hybrid Threats*, 8; Treverton et al., *Addressing Hybrid Threats*, 83.

135 European Commission, "Hybrid Threats," European Commission, n.d., https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en.

136 Björn Fägersten, "Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence," in *Forward Resilience: Protecting Society in an Interconnected World* (Washington, DC: Center for Transatlantic Relations, 2016), 115, https://archive.transatlanticrelations.org/wp-content/uploads/2017/02/resilience-forward-book-fagersten-final-version.pdf.

137 Mikael Wigell et al., *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats* (European Parliament, 2021), 21, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf.

138 Khidasheli, *Hybrid Threats and Resilience: Safeguading Democratic Values in a Connected World*, 12.

Figure 9: Strategic responses to hybrid threats

While resilience provides SMPs with a defensive shield, strategic alignments determine their positioning in the broader picture of great power competition. Given their limited individual capabilities, SMPs often navigate the international landscape by aligning with stronger actors in ways that best serve their security and economic interests. The need to build resilience, together with alignment dictated by economic and security interests, translates in different responses to Chinese hybrid threats. These approaches can be classified along four broad categories, each reflecting different levels of risk tolerance and geopolitical considerations: **(1) Bandwagoning, (2) Hedging, (3) Balancing, and (4) Countering** (Figure 9)**.** Every approach involves trade-offs in autonomy and risk, and each state's unique geopolitical context, threat perceptions, and domestic considerations play a role in the manifestation of these strategies, categorised in Table 4.

Bandwagoning can be considered as unambiguously aligning with or acquiescing to the source of a threat, either to protect against external risks or to gain economic or security benefits in exchange for political concessions.[139] This strategy is particularly attractive when the aggressor is geographically near and wields overwhelming power, rendering resistance costly.[140] At the same time, bandwagoning can be characterised by the opportunities of self-extension and gain rather than explained simply by the existence of external threat.[141] Bandwagoning is therefore not solely a strategy of appeasement and product of a security dilemma, but rather a practice which aims to secure gains through positive-sum game associations.[142] Yet, this strategy is sometimes pursued "by stealth", principally when public opinion on the great power is predominantly negative or when it is perceived as a major threat to the SMP's sovereignty.[143] Certain SMPs also engage in "indirect bandwagoning" where they align with the great power's interests by discreetly combating the influence of another great power without openly confronting it.[144]

With the rise of the PRC to great power status, bandwagoning behaviour has spiked especially among SMPs in the Asia-Pacific.[145] The perceived economic prospects associated

139 Stephen M. Walt, "Alliance Formation and the Balance of World Power," *International Security* 9, no. 4 (1985): 4.

140 Stephen M. Walt, *The Origins of Alliances* (Cornell University Press, 1990), 33, https://web.stanford.edu/class/ips198/docs/Walt.pdf.

141 Randall L. Schweller, "Bandwagoning for Profit: Bringing the Revisionist State Back In," *International Security* 19, no. 1 (1994): 74, https://doi.org/10.2307/2539149.

142 Schweller, "Bandwagoning for Profit," 106–7.

143 Bidzina Lebanidze and Kornely Kakachia, "Bandwagoning by Stealth? Explaining Georgia's Appeasement Policy on Russia," *European Security* 32, no. 4 (2023): 677, https://doi.org/10.1080/09662839.2023.2166404.

144 Dana Abu-Haltam, "How to Politely Say No: Jordan's Indirect Bandwagoning Behavior toward US–China Competition," *Foreign Policy Analysis* 21, no. 4 (2025): 2, https://doi.org/10.1093/fpa/oraf032.

145 Evelyn Goh, "Great Powers and Hierarchical Order in Southeast Asia: Analyzing Regional Security Strategies," *International Security* 32, no. 3 (2007): 118.

with a certain degree of cooperation are a leading factor of SMPs bandwagoning with the PRC.[146] The latter is the most common trend between both Europe and Asia, with SMPs eyeing Chinese large investments in technology ecosystems and development of infrastructures.[147] While this strategy can preserve or increase economic capacity and security, it often comes at the expense of strategic autonomy as bandwagoning may require SMPs to accept a degree subordination, or in some cases loss of sovereignty.[148] Obligations of political concessions and alignment with the PRC in international relations matters are also part of the risks associated with bandwagoning.[149]

Hedging represents a more flexible approach, allowing SMPs to maintain beneficial relations with a hybrid threat actor while cultivating partnerships with other powers as a fallback option.[150] This allows for the maximisation of profits while avoiding overdependence. Hedging entails a careful and pragmatic balancing act, simultaneously preserving leverage and security.[151] The concept of hedging has often been compared to a "risk management strategy" which aims to ensure protection of vital interests (sovereignty, political and economic independence) while extracting opportunities from cooperation with the great powers. [152]

Many Southeast Asian nations have a long legacy of hedging; engaging economically with China while maintaining security ties with the United States and regional allies.[153] This dual approach is not as "politically provocative" as bandwagoning or balancing, and mitigates risks while preserving strategic options in a polarised international system.[154] As such, SMPs tend to hedge either when they judge that joining one side is too risky or when the perceived threat is not yet acute.[155] This strategy allows government to maintain strong political independence and avoid concessions, while ensuring a greater legitimacy of the regime due to socio-economic developments permitted by the economic cooperation with the PRC.[156]

---

146 Denny Roy, "Southeast Asia and China: Balancing or Bandwagoning?," *Contemporary Southeast Asia* 27, no. 2 (2005): 307.

147 Domingo I-Kwei Yang, "Resisting China's ICT Influence in Sub-Saharan Africa: A Bandwagoning-for-Profit Perspective," *Issues & Studies* 59, no. 01 (2023): 2350004, https://doi.org/10.1142/S1013251123500042.

148 Máté Szalai, *Between Hedging and Bandwagoning: Interpreting the Reactions of Middle Eastern and North African States to the Russian-Ukrainian War* (European Institute of the Mediterranean, 2023), 2, https://www.euromesco.net/wp-content/uploads/2023/02/Policy-Brief-N%C2%BA123.pdf.

149 Veasna Var, "Cambodia's South China Sea Policy: From ASEAN Aligned to Echoing Chinese Clientism," in *Security, Strategy, and Military Dynamics in the South China Sea: Cross-National Perspectives*, ed. Gordon Houlden et al. (Bristol University Press, 2021), 203, https://doi.org/10.46692/9781529213478.012.

150 Evan S. Medeiros, "Strategic Hedging and the Future of Asia pacific Stability," *The Washington Quarterly* 29, no. 1 (2005): 145, https://doi.org/10.1162/016366005774859724; Sovinda Po and Christopher B. Primiano, "An 'Ironclad Friend': Explaining Cambodia's Bandwagoning Policy towards China," *Journal of Current Southeast Asian Affairs* 39, no. 3 (2020): 447, https://doi.org/10.1177/1868103420901879.

151 Ann Marie Murphy, "Great Power Rivalries, Domestic Politics and Southeast Asian Foreign Policy: Exploring the Linkages," *Asian Security* 13, no. 3 (2017): 169, https://www.tandfonline.com/doi/full/10.1080/14799855.2017.1354566; Szalai, *Between Hedging and Bandwagoning: Interpreting the Reactions of Middle Eastern and North African States to the Russian-Ukrainian War*, 2–3.

152 Jürgen Haacke, "The Concept of Hedging and Its Application to Southeast Asia: A Critique and a Proposal for a Modified Conceptual and Methodological Framework," *International Relations of the Asia-Pacific* 19, no. 3 (2019): 377, https://doi.org/10.1093/irap/lcz010.

153 Lee Hsien Loong, "The Endangered Asian Century," *Foreign Affairs*, June 2020, https://www.foreignaffairs.com/articles/asia/2020-06-04/lee-hsien-loong-endangered-asian-century; Sergio Grassi, *The Belt and Road Inititative in Malaysia: China's Geopolitics and Geoeconomics Challenged by Democratic Transformation* (Friedrich Ebert Stiftung Asia, 2020), 6, https://library.fes.de/pdf-files/iez/16766.pdf; Ajeng Rizqi Rahmanillah et al., "Indonesia's South China Sea Policy: The Limits of Hedging," *Social and Educational Studies Journal* 2, no. 11 (2024): 1279–91, https://doi.org/10.57096/edunity.v2i11.177.

154 Vaicekauskaitė, "Security Strategies of Small States in a Changing World," 12.

155 Alexander Korolev, "Shrinking Room for Hedging: System-Unit Dynamics and Behaviour of Smaller Powers," *International Relations of the Asia-Pacific* 19 (June 2019): 422, https://doi.org/10.1093/irap.

156 Alfred Gerstl, "Malaysia's Hedging Strategy Towards China Under Mahathir Mohamad (2018–2020): Direct Engagement, Limited Balancing, and Limited Bandwagoning," *Journal of Current Chinese Affairs* 49, no. 1 (2020): 111, https://doi.org/10.1177/1868102620964219.

Recently, SMPs have engaged in "omnidirectional hedging" as a product of the Sino-American competition exerted as part of the BRI and the US' Free and Open Indo-Pacific strategy. This implies the extension of strategic space of actions for SMPs to manoeuvre great power pressure and avoid entrapment between GP rivalry by including diplomatic security and economic diversification to prevent possible losses.[157] This is observable particularly in the Asia-Pacific with SMPs tending to maximise economic advantages generated by cooperation with the PRC while at the same time seeking security guarantees from the United States.[158] Hedging is also present in Europe, especially for states who see significant economic benefit in aligning with the PRC. Italy has engaged in this behaviour, maintaining deep economic ties while reinforcing its commitments within NATO and building up resilience against Chinese hybrid threats.

While often depicted only under a positive light, hedging is also a question of legitimacy and as such it comes at a cost. Hedging states can suffer from a perceived lack of loyalty by both the PRC and the competing powers, risking long-term balancing pressures that they might not be able to withstand.[159]

Balancing involves actively counter aligning against the source of a hybrid threat. This entails openly identifying the hybrid threat actor as an adversary and "balancing" the threat, typically through the formation of alliances and coalitions to deter the aggressor. SMPs that perceive a proximate or immediate threat, such as Eastern European states facing Russian hybrid activities, are more likely to pursue this strategy.[160] For states with limited means, balancing often takes the shape of participation in a larger alliance system like NATO or the EU.[161] Outside of large formal alliances, minilateral initiatives have also become more popular. This approach is particularly evident in the Asia-Pacific, where countries have formed non-treaty security partnerships with allies to balance against Chinese hybrid threats.[162]

Engaging in balancing strategy against the hegemonic power brings opportunities for the SMPs to protect their sovereignty while establishing their interests against the great power posing the biggest threat.[163] The main drawbacks of the balancing strategy are the high costs involved in the joint action. These can entail retaliation on the PRC side across multiple domains, among which most commonly the use of economic coercion and diplomatic pressure, as well as a potential long-term increase in the intensity of hybrid tactics' targeting.[164] The SMP's might end up needing to change its strategy towards a more neutral one to avoid these risks, or in contrary reinforce its position by engaging in countering.

---

157 Maheera Munir and Aiysha Safdar, "Sino-U.S. Strategic Competition in the Asia-Pacific: Omnidirectional Hedging of Traditional Middle Powers," *Strategic Studies* 43, no. 2 (2023): 21.

158 Charles Chong Han Wu, "Why Do States Hedge in East Asia? An Empirical Study on Hedging," *Asian Perspectives* 43, no. 3 (2019): 557.

159 Kuik Cheng-Chwee, "The Essence of Hedging: Malaysia and Singapore's Response to a Rising China," *Contemporary Southeast Asia* 30, no. 2 (2008): 159.

160 Vaicekauskaitė, "Security Strategies of Small States in a Changing World," 10.

161 Marina Stănescu, "A Small State's Security Strategy in a Changing World – Republic of Moldova Case Study," *Scientific Bulletin* 29, no. 2 (2024): 308, https://doi.org/10.2478/bsaft-2024-0031.

162 Sung Chul Jung and Er-Win Tan, "Middle Powers and Minilateralism against Hybrid Threats in the Indo-Pacific: South Korea, Singapore, and Taiwan," *Australian Journal of International Affairs* 78, no. 6 (2024): 890, https://doi.org/10.1080/10357718.2024.2399339.

163 Tongfi Kim, *Sino-Philippine Disputes and the US-Philippines Alliance*, US Alliance Obligations in the Disputes in the East and South China Seas (Peace Research Institute Frankfurt, 2016), 19, https://www.jstor.org/stable/resrep14540.5.

164 Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (1978): 169, https://doi.org/10.2307/2009958.

Finally, **countering** can be used to directly deal with hybrid threats by focusing on internal resilience and proactive measures to disrupt and mitigate hybrid operations. This strategy entails a more open and obvious opposition to the great power on almost all fronts.[165] Countering therefore involves an element of deterrence, which can be done by denial (building resilience and offensive capabilities to prevent the enemy access to the SMP) or by punishment (the ability to impose costs on the enemy attacking).[166] States employ countering for a variety of reasons, but mainly for strategic, identity and coalition motives. Countering cultivates legitimacy and sustains a confrontational stance, poses the bases for collaboration with a rival greater power and bolsters a SMP leverage in the international system.[167]

However, it also entails putting at risk both the SMP's direct relation with the great power as well as its own sovereignty. Countering is thus not a common strategy utilised by SMPs due to these risks, the potential for escalation, and the very low space for manoeuvring left to solve a potential confrontation.[168] In the case of the PRC, its economic weight makes the impact of engaging in countering particularly heavy, as retaliatory measures can severely affect the SMP involved.[169] Given the risks associated, when a SMP chooses a strategy of countering, a whole-of-government coordination is essential, requiring the breakdown of silos between military intelligence, law enforcement, and civilian agencies. A coordinated countering response is hence particularly complex to implement.[170]

165 Cheng-Chwee Kuik, "Getting Hedging Right: A Small-State Perspective," *China International Strategy Review* 3, no. 2 (2021): 306, https://doi.org/10.1007/s42533-021-00089-5.

166 Sean Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?," *PRISM* 8, no. 2 (2019): 90.

167 Tom Long, "Small States, Great Power? Gaining Influence Through Intrinsic, Derivative, and Collective Power," *International Studies Review* 19, no. 2 (2017): 185–205.

168 Ciwan M. Can, "Small Power Strategies under Great Power Competition," *International Politics* 61, no. 2 (2024): 296, https://doi.org/10.1057/s41311-023-00552-7.

169 Matthew Reynolds and Matthew P. Goodman, *China's Economic Coercion: Lessons from Lithuania*, June 5, 2022, https://www.csis.org/analysis/chinas-economic-coercion-lessons-lithuania.

170 Monaghan, "Countering Hybrid Warfare," 91.

Table 4: Categorisation of response strategies

Response	Definition	Focus of response	Approach to China	Mechanism	Risks
Bandwagoning	Aligning with the PRC's policies and goals to gain economic or political benefits.	Preservation	Cooperative: ignores or downplays hybrid tactics to maintain favourable relations	Actively supporting Chinese-led initiatives Adopting pro-PRC foreign policy stances Granting PRC's access to strategic resources or infrastructure	Erosion of sovereignty Over reliance on the PRC
Hedging	Pursuing a dual strategy of engaging with the PRC while diversifying partnerships.	Adaptability	Pragmatic: limits damage from hybrid tactics without provoking direct retaliation.	Actively supporting Participation in Chinese-led initiatives (e.g., BRI) while forging non-PRC partnerships (e.g., CPTPP)Chinese-led initiatives Avoiding overt confrontation or alignment Diversifying economic and security partners	Perceived lack of loyalty by both the PRC and competing powers Long-term balancing pressures
Balancing	Counterbalancing the PRC's influence by aligning with other powers to strengthen national capabilities without direct provocation.	Deterrence	Cautious: builds resilience through alliances but without direct confrontation.	Joining frameworks and partnerships that limit/counter the PRC's influence Diplomatic and economic signalling Hosting joint military exercises, bolstering joint ventures for defence capabilities	Retaliation across multiple domain (economic, diplomatic) Long-term increase in tensions
Countering	Openly and directly opposing China's tactics, often through confrontational measures.	Confrontation	Confrontational: calls out and actively combats China's hybrid tactics on multiple fronts	Imposing tariffs/sanctions/bans Rejecting Chinese investments Public condemnation of Chinese actions (e.g., violation of human rights)	Strained bilateral relations Escalation

4. Case studies

Investigating the application of response strategies by SMPs to the PRCs hybrid tactics is vital to understanding their implications on counter-hybrid posturing. The section below presents eight in-depth case studies that highlight how a state's relations to the PRC shapes its strategic objectives, in turn defining their response to hybrid threats.

While the eight cases below encapsulate the essence of the four strategies highlighted above, it must be noted that the lines between a type of response and another are often blurred. A state's overall tendency might be, for instance, to favour bandwagoning, but this does not mean that it never engages in, say, hedging. Variations in behaviour depend on the (geo)political, economic, and security conditions under which Chinese hybrid threats are perpetrated, as well as the countries' capabilities, resolve, and stakes. Most often, these variations are driven by the ad-hoc nature of hybrid threats responses. In fact, SMPs have the tendency to respond to hybrid threats on a case-by-case basis, without an overarching harmonised strategy.

Nonetheless, the case studies below show that it is possible to distinguish overall patterns that help situate a SMP's response to Chinese hybrid threats in a broader strategic context, as seen in Figure 10.

Figure 10: Strategic responses to hybrid threats: case studies results

4.1. Bandwagoning

Bandwagoning states align themselves with China's policies to secure economic or political gains, prioritising the preservation of favourable relations and therefore downplaying or overlooking Beijing's hybrid tactics. They have a cooperative approach to the PRC, that often includes actively supporting Chinese-led initiatives, adopting pro-China foreign policy stances, and granting China's access to strategic resources or infrastructure to appease Beijing and contain its use of hybrid threats. Often, bandwagoning states do not possess the resources necessary to actively counter the PRC and hence choose preservation over autonomy. Almost always, this has to do with the economic benefit they can reap from their partnerships with China. Still, bandwagoners want to ensure that they can detect and prepare

for Chinese hybrid threats, as they have an interest in reducing the impact of hybrid threats that Beijing uses on them despite their closer alignment to the PRC. Hungary is a good case of this on the European side, while Cambodia's security and economic dependence make it the perfect example in the Indo-Pacific.

4.1.1. Hungary

Hungary's response to Chinese hybrid threats has been marked less by resistance than by deliberate strategic accommodation, opting for deep engagement with the PRC's expanding influence and thereby positioning itself as a key gateway for Beijing's economic and political ambitions in Europe. [171] The two countries established cooperative and aligned relations several decades ago and upgraded their 2017 "comprehensive strategic partnership" to an "all-weather comprehensive strategic partnership for the new era" in 2024.[172] Hungary has been an active advocate for Chinese interests in the EU, making it the biggest destination for Chinese investment in Europe amounting to €2.9B (44% of total European FDI of 6.8B), as well as the recipient of some of the biggest loans.[173] Beyond economic involvement, the PRC has even offered to support the government on strategic public security issues.[174] This all points to dual goal of the PRC in Hungary, namely the establishment and exploitation of both an economic and a political bastion.

This relationship granted the PRC access to strategic sectors in Hungary, which have downplayed hybrid tactics to maintain close relations. In 2019, a consortium including a company linked to Hungarian Prime Minister Viktor Orbán's ally Lőrinc Mészáros and two Chinese state backed construction companies secured a €2.1 billion contract for Hungary's section of the Budapest-Belgrade railway, a key part of the China's BRI.[175] Then in 2020, Hungary announced a €2 billion loan from the China Development Bank to finance 85% of its share in the Budapest–Belgrade rail project. Since 2024, Hungary has taken another €1 billion loan from the China Development Bank, further compromising Hungarian economic independence from the PRC.

Hungary has not only welcomed growing Chinese involvement in its society and academic sector but actively facilitated it, exemplified by the planned €1.5 billion loan for a Fudan University campus, thereby exposing itself to a broader range of Chinese hybrid threats that extend beyond economics to include societal, informational, and political influence.[176] These academic connections serve as a direct pathway and tool for the spread of pro-Chinese narratives which can be used to promote certain political agendas.

---

171 Tian Shenyoujia, "Interview: Hungary Looks Forward to Further Cooperation with China, Official Says," *Belt and Road Portal*, May 5, 2024, https://eng.yidaiyilu.gov.cn/p/0DG0579C.html.

172 Eva Seiwert and Claus Soong, "What's in a Name? A Rough Guide to China's Elaborate Labeling of Bilateral Relations in Europe," *Merics*, October 15, 2024, https://merics.org/en/comment/whats-name-rough-guide-chinas-elaborate-labeling-bilateral-relations-europe.

173 Agatha Kratz et al., "Dwindling Investments Become More Concentrated - Chinese FDI in Europe: 2023 Update | Merics," Merics, June 6, 2024, https://merics.org/en/report/dwindling-investments-become-more-concentrated-chinese-fdi-europe-2023-update.

174 "In Unusual Move, China Offers to Back Hungary in Security Matters," *Euractiv*, February 19, 2024, https://www.euractiv.com/news/in-unusual-move-china-offers-to-back-hungary-in-security-matters/.

175 "Chinese Money Flows to Friend of Hungarian PM Orban in Contract for Budapest-Belgrade Railway," Alliance For Securing Democracy, accessed September 1, 2025, https://securingdemocracy.gmfus.org/incident/chinese-money-flows-to-friend-of-hungarian-pm-orban-in-contract-for-budapest-belgrade-railway/.

176 Akos Keller-Alant and Reid Standish, "What's Next For China's Fudan University Campus In Hungary?," China In Eurasia, *Radio Free Europe/Radio Liberty*, 09:45:57Z, https://www.rferl.org/a/hungary-orban-china-fudan-budapest/31888800.html.

Despite its close ties with China, Hungary remains as exposed to general PRC cyber operations – like the Nevada Ransomware and APT Group Earth Krahang attacks– as its neighbours.[177] Chinese companies also enjoy direct access to public officials, not seldomly facilitated through these academic connections. For instance, Huawei executives used the donation of COVID-19 medical supplies to secure a meeting with Hungarian Foreign Minister Péter Szijjártó.[178] Later in 2024, Hungary's 4iG signed a memorandum of understanding with Huawei which promises collaboration on projects in 5G, data centres, and IT infrastructure during President Xi's visit to Budapest.[179]

Hungary has therefore engaged in a bandwagoning strategy, aligning with Chinese policies in a variety of domains. Rather than engaging in confrontational stance, Hungary prefers to attract investments in key sectors such as energy and technology, overlooking the risk of economic dependence. The Hungarian government has also blocked the EU from issuing condemnations of Beijing's clampdown on Hong Kong and other human right's issues, avoided criticising aggressive action in the South China sea, and opposed the EUs economic de-risking from the PRC.[180]

This bandwagoning strategy is even more notable considering Hungary's participation in other regional frameworks, such as the EU and NATO, where Chinese influence is viewed in a cautious way. Despite Hungary's presence in NATO and participation in resilience programs against hybrid threats, the government has granted China access to strategic resources and infrastructures including technology leadership and telecommunication networks and infrastructures.[181]

Hungary's response thus focuses on avoiding the destructive effects of hybrid tactics while benefitting from investments to the cost of its autonomy.

4.1.2. **Cambodia**

Cambodia's close alignment with the PRC has fostered deep political, economic and military dependence, leaving the country comparatively insulated from overt Chinese hybrid threats but increasingly vulnerable to structural influence exercised through investment, cyber operations and sustained leverage over strategic governance and infrastructure. Cambodia is one of the states with the closest ties to the PRC. It has largely supported the PRC within international institutions and has issued several statements in support of the PRC's policy regarding

177 "European Repository of Cyber Incidents," EuRepoC, accessed September 1, 2025, https://eurepoc.eu/table-view/.

178 "Huawei Uses Medical Donation to Secure Meeting with Hungarian Officials," Alliance For Securing Democracy, accessed September 1, 2025, https://securingdemocracy.gmfus.org/incident/huawei-uses-medical-donation-to-secure-meeting-with-hungarian-officials/.

179 "Xi's Visit Sparks Future Huawei, 4iG Collabs," Central European Times, May 12, 2024, https://centraleuropeantimes.com/xis-visit-sparks-future-huawei-4ig-collaboration/.

180 Thomas Grove and Drew Hinshaw, "Hungary Extends Warm Welcome to Top Chinese Diplomat," World, *Wall Street Journal*, February 20, 2023, https://www.wsj.com/articles/hungary-extends-warm-welcome-to-top-chinese-diplomat-e79b9d8; Ian Williams, "Hungary Has Become China's Useful Idiot," *The Spectator*, February 22, 2024, https://www.spectator.co.uk/article/hungary-has-become-chinas-useful-idiot/; Thomas Moller-Nielsen, "Hungary Looks to 'de-Escalate' EU-China Trade Tensions While Commission Distances Itself from Orbán's Beijing Trip," Defence, *Euractiv*, July 8, 2024, https://www.euractiv.com/section/defence/news/hungary-looks-to-de-escalate-eu-china-trade-tensions-while-commission-distances-itself-from-orbans-beijing-trip/; Tamás Matura, "Chinese Influence in Hungary," *CEPA*, August 18, 2022, https://cepa.org/comprehensive-reports/chinese-influence-in-hungary/.

181 The Government of Hungary, "Government Resolution on Hungary's National Security Strategy," June 21, 2021, https://www.surrey.ac.uk/sites/default/files/2024-09/2020_Hungary.pdf.

its treatment of the Uyghur population.[182] Cambodia has also vetoed the implementation of the South China Sea ruling against the PRC into ASEAN legal frameworks, advocating against several of its neighbours' interests in favour of the PRC.[183]

The PRC is also the largest investor in Cambodia's economy, participating largely in the development of digital technologies and infrastructure.[184] The two countries maintain diplomatic and economic relations and participate in bilateral military exercises. The PRC also contributes largely to the development of Cambodian forces (infrastructure, arms trade and training).[185] In Cambodia, Chinese presence and influence is generally positively interpreted, especially due to the positive economic prospects brought by the BRI and its large investments in national infrastructures which promote development and improved public access to social services.[186]

The Sino-Cambodian relationship has allowed the PRC to gain a political and military presence in key strategic areas such as the Gulf of Thailand through the Ream Naval Base.[187] Yet, this came at the price of cultural and political autonomy in Cambodia, sacrificed in pursuit of economic prospects and foreign investment. For these reasons, Cambodia has been relatively shaded from Chinese hybrid threats contrarily to its neighbours. Still, Cambodia's alignment with the PRC and the support it provides internationally requires Beijing to maintain a pro-Chinese government in Cambodia. To this end, cyber operations linked to Beijing have targeted Cambodian elections through hacking and data theft, while extensive Chinese investment has strengthened the PRC's leverage over economic negotiations and facilitated the diffusion of its political preferences in the region.[188] Overall, the PRC's involvement in Cambodia principally engages in short term operations, espionage, and cyber-attacks to ensure continued alignment and long-term economic dependence.

Unsurprisingly, Cambodia has adopted a bandwagoning strategy with the PRC, primarily by actively supporting Chinese-led initiatives like the BRI as well as granting the PRC access to strategic resources or infrastructures, therefore giving away parts of its own sovereignty to benefit from Chinese investments. Regarding political undermining, Cambodia has rejected accusations of political interference, mostly because the elected government was the one supported by the PRC.[189] While Cambodia has been a victim of cyber-attacks and intrusion in governmental agencies from Chinese linked APTs, the Cambodian government has avoided

182 Tamara Qiblawi, "Muslim Nations Are Defending China as It Cracks down on Muslims, Shattering Any Myths of Islamic Solidarity," *CNN*, July 17, 2019, https://edition.cnn.com/2019/07/17/asia/uyghurs-muslim-countries-china-intl/index.html.

183 Manuel Mogato Martina Michael and Ben Blanchard, "ASEAN Deadlocked on South China Sea, Cambodia Blocks Statement," World, *Reuters*, July 26, 2016, https://www.reuters.com/article/world/asean-deadlocked-on-south-china-sea-cambodia-blocks-statement-idUSKCN1050F6/.

184 Neak Chandarith, "China-Proposed Belt and Road Initiative Promotes Cambodia's Development, Regional Connectivity," *The State Council Information Office The People's Republic of China*, May 19, 2025, http://english.scio.gov.cn/beltandroad/2025-05/19/content_117882124.html.

185 "China-Cambodia 'Golden Dragon 2025' Joint Exercise Kicks Off," Ministry of National Defense, accessed October 21, 2025, http://eng.mod.gov.cn/xb/News_213114/TopStories/16387004.html.

186 "About AIIB," Asian Infrastructure Investment Bank, accessed September 2, 2025, https://www.aiib.org/en/about-aiib/index.html.

187 "A Tale of Two Reams: Questions Remain at Cambodia's Growing Naval Base," *Asia Maritime Transparency Initiative*, n.d., accessed September 2, 2025, https://amti.csis.org/a-tale-of-two-reams-questions-remain-at-cambodias-growing-naval-base/.

188 EuRepoC, "European Repository of Cyber Incidents"; Heng Pheakdey, "Cambodia-China Relations: A Positive-Sum Game?," *Journal of Current Southeast Asian Affairs* 31, no. 2 (2012): 68, https://doi.org/10.1177/186810341203100203.

189 European Repository of Cyber Incidents, "Leviathan Aka TEMP.Periscope Aka APT 40 Influences on the Election in Cambodia."

commenting on the attacks, sometimes refuting the allegations.[190] As part of the BRI the PRC has involved in water management systems, roads infrastructure, agriculture improvements, energy infrastructures as well as financial systems and technologies.[191] The country therefore openly welcomes China's BRI as a strategy for development making it difficult to engage fully in other partnerships.[192]

This dependence severely restricts possibilities of countermeasures against Chinese hybrid threats, including cyber-attacks. First because the country's economy largely depends on Chinese investments and, therefore, cannot officially condemn Chinese interference for risks of retaliation. Second, by the lack of physical means, as most development infrastructures are funded by the PRC, and thus subject to Chinese oversight.[193]

Overall, Cambodia remains among the countries most exposed and vulnerable to Chinese influence, through a combination of economic and political hybrid threats. It is therefore not a surprise for Cambodia to employ bandwagoning as its main response to Chinese hybrid threats.

4.2. **Hedging**

Hedging states pursue a dual approach of engaging China while broadening external partnerships, adopting a pragmatic posture that mitigates the impact of hybrid tactics without inviting direct retaliation. Adaptability is key for hedging states, that often join, especially economic, Chinese-led initiatives while diversifying their options. While states in this category still respond to China's hybrid measures, their action are more nuanced and will not overstep the threshold of what might be considered from Beijing as an act of confrontation. The cases of Italy and Malaysia show how responses to Chinese threat can encompass both engagement and diversification at the same time.

4.2.1. **Italy**

Italy is one of the closest partners of the PRC in the EU, and more importantly, the first G7 member to participate in the BRI. While Italy refused to renew the BRI agreements in 2023 citing unfavourable results, it has replaced it with a strategic partnership on Science and Technology research and innovation.[194] Contrary to Hungary, the Italian government has been a large critic of Chinese FIMI during Covid-19 as well as the PRC's human rights abuses on the Uyghur population.[195] Additionally, the war in Ukraine has required NATO members

190 Chansambath Bong, "Cambodia's Disastrous Dependence on China: A History Lesson," *The Diplomat*, December 4, 2019, https://thediplomat.com/2019/12/cambodias-disastrous-dependence-on-china-a-history-lesson/.

191 Thy Try, *China Index Spotlight: Cambodia and the PRC: Mutual Beneficence and Sovereignty* (Doublethinklab, 2025), https://medium.com/doublethinklab/china-index-spotlight-cambodia-and-the-prc-mutual-beneficence-and-sovereignty-119645b8327b.

192 Bong, "Cambodia's Disastrous Dependence on China."

193 "China: Southeast Asia Visit Raises Alarm over Digital Repression," *ARTICLE 19*, April 14, 2025, https://www.article19.org/resources/china-southeast-asia-visit-raises-alarm-over-digital-repression/.

194 Ilaria Mazzocco and Andrea Leonard Palazzi, *Italy Withdraws from China's Belt and Road Initiative* (Center for Strategic and International Studies, 2023), https://www.csis.org/analysis/italy-withdraws-chinas-belt-and-road-initiative.

195 "Italy Follows France, Germany in Sanctioning China over Treatment of Uyghurs," sec. International, *RFI*, March 24, 2021, https://www.rfi.fr/en/international/20210324-italy-follows-france-germany-in-sanctioning-china-over-treatment-of-uyghurs.

to strengthen their alliance and prepare against security threats in Eastern Europe. These priorities, coupled with the rising US-PRC rivalry, have reshaped the economic agenda of Italy, which has limited the extent of its PRC partnership.[196]

Still Italy, along with Germany, remains the principal actor linking the PRC with the rest of Western Europe, a connection which Beijing cannot afford to compromise.[197] It is thus no surprise that, in this context, the PRC has made use of hybrid tactics to further its interests in Italy. Rome's previous participation in the BRI increased its exposure to Chinese influence, making it one of the most targeted European countries after Belgium. Cyber operations and attacks consisting in a variety of malicious actions aiming to disrupt or destroy information systems, peaked throughout 2020-2021, during Covid-19, but continued afterwards too.[198] The private sector was particularly targeted, suggesting either that Italy counters Chinese hybrid threats against its government more effectively than other states, or that the PRC pursues a different strategy than in the Asia-Pacific (where it targets government agencies) to reengage Italy in the BRI. For instance, in June and July 2024, the PRC-linked APT17 group targeted Italian companies and government entities by spear-phishing emails installing a malware designed for surveillance, file management and network discovery. [199] These attacks came a few months following Italy's withdrawal from the BRI, but also Italy's recent involvement as a strategic and military presence in the Indo-Pacific.[200] Chinese FIMI is also diffused in Italy. In 2020 to the PRC organised a campaign for the promotion of "PRC aid packages" delivered to Italy making use of hashtags and information bubbles on twitter.[201] This campaign targeting the public, creating instability in the already delicate situation of Covid-19, where the PRC was also accused of engaging in FIMI with regards to its 'mask diplomacy'. [202]

Given its multifaceted relation to the PRC, Italy has engaged in a more complex and subtle hedging strategy. Rome actively countered Chinese attempts at information manipulation, blocking several Chinese investments in the country due to concerns over the PRC's aggressive information tactics.[203] Launched in 2021 as part of a broader European network, the Italian Digital Media Observatory was created to detect fake news and track its disseminators in response to ongoing disinformation campaigns.[204] Italy also signed in 2024 a memorandum of understanding (MoU) with the US on Countering FIMI, reestablishing its strong stance against the spread of deepfakes and manipulation campaigns among the population and influential institutions such as universities.[205]

196 Giorgio Prodi, "Italy's Soft Reset with China after Dropping the Belt and Road," China, *East Asia Forum*, September 28, 2024, https://eastasiaforum.org/2024/09/28/italys-soft-reset-with-china-after-dropping-the-belt-and-road/.

197 Prodi, "Italy's Soft Reset with China after Dropping the Belt and Road."

198 Ravie Lakshmanan, "China-Linked APT17 Targets Italian Companies with 9002 RAT Malware," The Hacker News, July 17, 2024, https://thehackernews.com/2024/07/china-linked-apt17-targets-italian.html.

199 Julian Ryall, "Italy Latest in Europe to Step up Military Ties with Japan," *DW* (Tokyo), June 29, 2024, https://www.dw.com/en/italy-latest-in-europe-to-step-up-military-ties-with-japan/a-69502769.

200 Ryall, "Italy Latest in Europe to Step up Military Ties with Japan."

201 Brian Hart, "Is China Succeeding at Shaping Global Narratives about Covid-19?," *ChinaPower Project*, October 22, 2021, https://chinapower.csis.org/china-covid-disinformation-global-narratives/.

202 Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (2018): 90–113.

203 Noah Barkin et al., "GMF Expert Analysis: Shifting Italy-China Relations," German Marshall Fund of the United States, August 2, 2023, https://www.gmfus.org/news/gmf-expert-analysis-shifting-italy-china-relations.

204 *IDMO – Italian Digital Media Observatory*, n.d., accessed November 18, 2025, https://www.idmo.it/en/.

205 "The United States of America and Italy Sign Memorandum of Understanding to Expand Collaboration on Countering Foreign State Information Manipulation," *United States Department of State*, n.d., accessed November 18, 2025, https://2021-2025.state.gov/the-united-states-of-america-and-italy-sign-memorandum-of-understanding-to-expand-collaboration-on-countering-foreign-state-information-manipulation/.

Similarly, Italy has also engaged in the Cybersecurity Advisory which clearly focuses on sharing intelligence with other partners to counter Advanced Persistent Threats (APT) linked to the PRC.[206] Following legal developments in the EU, the country also established a clear, all-encompassing legal framework regarding the tackling of ransomware attacks, in addition to new laws preventing non-NATO/EU suppliers and technologies in sensitive sectors. [207] These actions are implemented along a wider strategy of establishing a cybersecurity training and culture among the population, increasing awareness.

Overall, Italy has clearly positioned itself against Chinese espionage, cyberattacks and FIMI attempts by engaging in realignment while avoiding complete rupture. Italy has nevertheless maintained cordial relationships with the PRC on the economic side by engaging in partnership and investments. Italy's cautious re-alignment with European and transatlantic positions on the PRC, while simultaneously maintaining its role as the PRC's closest partner in Western Europe, exemplifies a hedging strategy that balances engagement with China and diversification of partnerships.[208]

4.2.2. **Malaysia**

Malaysia's response to Chinese hybrid threats reflects a hedging strategy that balances deep economic dependence and expanding cooperation with selective protective measures in cyber security, information governance and maritime defence, while avoiding direct confrontation with Beijing. This is especially true after bilateral relations have greatly improved over the past two years.[209] Malaysia's language towards Taiwan has gradually moved from a nuanced, non-aligning position towards a pro-PRC one.[210] This shift occurs in a context of high dependence from trade with the PRC, which made up 17.1% of all Malaysian trade in 2024.[211] This is greatly facilitated by the signing of several MoUs and Malaysia's involvement in the BRI which enhance trade partnerships and collaborations on research and development.[212] The two countries also engage militarily as part of regional security exercises, involving arms trade, naval training, and strategic operation.[213] However despite the improved relations, Malaysia has maintained its overlapping sovereignty claims with the PRC in the South China Sea, and quietly facilitates US presence in the Indo-Pacific region

206 "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System | CISA," September 3, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.

207 Decode39, "Italy Locks down Its Digital, 5G Security," Politics, *Decode39*, October 21, 2025, https://decode39.com/12124/italy-locks-down-its-digital-security/.

208 swong, "Italy's Policy on China: The Belt and Road Gamble and Its Aftermath," *Atlantic Council*, November 10, 2025, https://www.atlanticcouncil.org/in-depth-research-reports/report/italys-policy-on-china-the-belt-and-road-gamble-and-its-aftermath/.

209 Thomas Daniel, "Malaysia's Relations with China and the United States in 2025," ISIS, March 19, 2025, https://www.isis.org.my/2025/03/20/malaysias-relations-with-china-and-the-united-states-in-2025/.

210 Nithin Coca, "Are Indonesia and Malaysia Ready to Stand up for China's Muslims ?," Centre tricontinental, October 21, 2025, https://www.cetri.be/Are-Indonesia-and-Malaysia-Ready.

211 *Trade Performance 2024* (Malaysian Ministry of Investment, Trade and Industry, n.d.), accessed August 20, 2025, https://www.matrade.gov.my/en/export-to-the-world/216-malaysian-exporters/trade-performance-2024.

212 "Joint Statement Between the People's Republic of China and Malaysia on Building a High-Level Strategic Malaysia-China Community with a Shared Future," Ministry of Foreign Affairs Malaysia, April 17, 2025, https://www.kln.gov.my/web/guest/-/joint-statement-between-the-people-s-republic-of-china-and-malaysia-on-building-a-high-level-strategic-malaysia-china-community-with-a-shared-future-1.

213 "Aman Youyi-2023 Joint Exercise Kicks off in China," Ministry of National Defense, November 14, 2023, http://eng.mod.gov.cn/xb/News_213114/TopStories/16266698.html.

by conducting joint military exercise annually and gradually intensifying economic and diplomatics partnerships.[214]

The PRC has used a combination of political undermining and strategic investment offers to secure influence in Malaysia, most notably by allegedly offering to bail out 1Malaysia Development Berhad (1MDB) in 2016 in exchange for lucrative infrastructure contracts such as the East Coast Rail Link (ECRL) and gas-pipeline deals. Through inflated contracts awarded to Chinese state-owned firms, Beijing effectively exchanged financial and political assistance for long-term control over Malaysian infrastructure and economic dependence[215] Despite improving relations, Malaysia is also subject to cyberattacks. The PRC has also been actively engaged in FIMI, in particular amongst Chinese language media, of which around 90% is owned by a single Chinese-Malaysian media tycoon with strong business links to the PRC.[216] For example, Chinese language media is much more pro-PRC in its coverage of the Uyghur situation, a high priority for the PRC.[217] As a result, the Malaysian government is more subdued in its vocal support of Uyghurs compared to its support of Palestinians or Rohingya despite vocally recognising the persecution.[218] The government has however refused to comply with Chinese requests of Uyghur extraditions arguing that, due to valid security concerns, they were considered refugees.[219]

The effectiveness of PRC media influence on the public is therefore limited. Whilst the older Chinese population is generally pro-PRC, younger and more educated Malaysians seem more sceptical.[220] Besides digital operations, the PRC also been active in military exercises and buildup in the South China Sea, resulting in the infringement of Malaysia's EEZ.[221] The near-permanent presence of Chinese coast guard vessels in Malaysia's EEZ since 2013 prompted diplomatic protests and attempts from the Royal Malaysian Navy to turn the Chinese ships away without escalation .[222]

Malaysia has focused its countermeasures on reinforcing national systems and infrastructure and deepen cooperation with other partners without confronting Beijing directly.[223] To combat Chinese interference, the government supports media literacy programs and has establish guidelines for the governance and ethics of AI and the spread of Fake News, both

214 "U.S. Navy and Marine Corps, Malaysian Armed Forces Commence CARAT 2025," United States Navy, accessed December 5, 2025, https://www.navy.mil/Press-Office/News-Stories/display-news/Article/4348193/us-navy-and-marine-corps-malaysian-armed-forces-commence-carat-2025/; Ian Storey, *Malaysia's Hedging Strategy with China*, no. 7, China Brief (Jamestown Foundation, 2007), https://jamestown.org/malaysias-hedging-strategy-with-china/.

215 Prashanth Parameswaran, "A China Bailout in Malaysia's 1MDB Scandal?," accessed August 21, 2025, https://thediplomat.com/2019/01/a-china-bailout-for-malaysias-1mdb-scandal/.

216 "Malaysia: Beijing's Global Media Influence 2022 Country Report," Freedom House, accessed August 20, 2025, https://freedomhouse.org/country/malaysia/beijings-global-media-influence/2022.

217 Asia Fact Check Lab, "A Look at How Beijing Influences Chinese Media, Diaspora in Malaysia," Radio Free Asia, July 19, 2023, https://www.rfa.org/english/news/afcl/malaysia-chinese-press-07192023095502.html.

218 "Malaysian Minister Slammed for Comments about Visit to Uyghur Camp," Radio Free Asia, July 2, 2019, https://www.rfa.org/english/news/uyghur/malaysia-uyghurs-07022019141108.html.

219 "Malaysia Won't Extradite Uighurs to China - Minister," *Reuters*, September 4, 2020, https://www.reuters.com/world/asia-pacific/malaysia-wont-extradite-uighurs-china-minister-2020-09-04/.

220 Lab, "A Look at How Beijing Influences Chinese Media, Diaspora in Malaysia."

221 "South China Sea Dispute: Malaysia Accuses China of Breaching Airspace," *BBC*, June 2, 2021, https://www.bbc.com/news/world-asia-57328868.

222 "Malaysia's Claims in the South China Sea: A Strategy of Quiet Diplomacy and Legal Assertion," *Catalyst International*, August 10, 2025, https://catalyst-international.org/2025/08/09/malaysias-claims-in-the-south-china-sea-a-strategy-of-quiet-diplomacy-and-legal-assertion/.

223 "Malaysia and the United States Elevate Bilateral Relations to Comprehensive Strategic Partnership," Official Portal: Ministry of Foreign Affairs Malaysia, October 26, 2025, https://www.kln.gov.my/web/guest/-/malaysia-and-the-united-states-elevates-bilateral-relations-to-comprehensive-strategic-partnership.

at the National level and at the regional one, within ASEAN.[224] The government also publicly acknowledged actions from Chinese linked groups and has taken action to counter it by implementing the Cyber Security Act 2024.[225] These actions aim at countering Chinese hybrid threats while avoiding direct confrontation and escalation.

At the same time, Malaysia has sought to diversify its international partnerships away from the PRC to reduce economic coercion opportunities. In October 2025, Malaysia and the US elevated their bilateral relationship to a Comprehensive Strategic Partnership, signalling deeper cooperation. In the same month, the two states signed a new Agreement on Reciprocal Trade, which gives US exporters increased access to Malaysian markets while requiring Kuala Lumpur to align with certain US export-control and investment-security measures.[226] Malaysia also turned to the US and Japan for assistance in acquiring maritime surveillance capabilities.[227]

The growing ties with the US, coupled with continuous engagement with the PRC exemplify Malaysia's hedging strategy to face hybrid pressures, especially in the economic domain.

4.3. **Balancing**

Balancing states counter China's influence by strengthening national capabilities through alignment with other powers, adopting a cautious deterrence posture that enhances resilience without engaging in direct confrontation. For balancing states, the emphasis is on joining frameworks and partnerships that limit/counter the PRC's influence, hosting joint military exercises and bolstering joint ventures for defence capabilities, as well as signalling autonomy from the PRC through diplomatic and economic means, as exemplified by the Philippines' and the Netherlands' cases.

4.3.1. **Netherlands**

The Netherlands has navigated its relationship with China through a careful balancing strategy, maintaining strong economic ties while addressing security risks. Recognising the growing threat of Chinese hybrid tactics, the Dutch government has implemented measures to protect critical industries, research institutions, and strategic infrastructure, while reinforcing cooperation with EU and NATO partners to enhance resilience and safeguard national autonomy. At the same time, the Netherlands is the PRC's 2nd largest trading partner in all of Europe, explained by its position as one of the PRC's primary investment destinations

224 "Malaysia: Beijing's Global Media Influence 2022 Country Report," Freedom House, accessed November 24, 2025, https://freedomhouse.org/country/malaysia/beijings-global-media-influence/2022; "The National Guidelines on Governance and Ethics," Malaysian Science and Technology Information Centre, September 24, 2024, https://mastic.mosti.gov.my.

225 "Protecting Malaysian Cyberspace," Official Portal Ministry of Communications, accessed November 24, 2025, https://www.komunikasi.gov.my/en/public/news/22458-protecting-malaysian-cyberspace; "Malaysian Legislation: Official Secrets Act 1972," CommonLII, January 2006, https://www.commonlii.org/my/legis/consol_act/osa1972156/.

226 Netty Idayu Ismail et al., "Anwar Turns Malaysia Into Stage for Dealmaking With Trump's Help," *Bloomberg.Com*, October 27, 2025, https://www.bloomberg.com/news/articles/2025-10-27/how-anwar-ibrahim-is-making-malaysia-a-global-diplomatic-powerhouse; "Agreement Between the United States of America and Malaysia on Reciprocal Trade," The White House, October 26, 2025, https://www.whitehouse.gov/briefings-statements/2025/10/agreement-between-the-united-states-of-america-and-malaysia-on-reciprocal-trade/.

227 "Malaysia's Claims in the South China Sea."

in the EU.[228]. The Netherlands and the PRC also cooperate heavily on infrastructure, technology and science research with a continuous renewal of their MoU.[229]

Still, the Netherlands has been openly vocal about the PRC's treatment of the Uyghur population, being the first EU country to qualify it as genocide.[230] Several instances of espionage have also been recorded over the Netherlands' advancements in the semiconductor industry undermining cooperation efforts.[231] Most recently, the Nexperia case has cooled off the relations with Beijing. Suspecting knowledge leaks by Nexperia's Chinese director, the Dutch Ministry of Economic Affairs took control of the firm prompting its Chinese branch to halt exports towards the Netherlands.[232] The Dutch government's move demonstrated the Netherlands' active efforts to prevent economic coercion and counter Chinese influence, as well as its strive for strategic autonomy and diversification away from the PRC.

This two-faced relationship has turned the Netherlands into a key target of hybrid threats for the PRC. The Dutch maritime sector, anchored by the port of Rotterdam, which handles a significant share of the EU's imports, represents a key point of influence for the PRC.[233] Meanwhile, the Dutch semiconductor industry, bolstered by key firms like ASML and NXP, plays a critical role in the production of advanced components, making it a strategic hub in global supply chains.[234] While the PRC dominates the production of essential raw materials such as gallium (93%) and germanium (83%)—which Dutch companies rely on—economic coercion is limited by the mutual dependence between the Netherlands and the PRC in semiconductor technology.[235] This interdependence constrains direct economic leverage, prompting the PRC to focus on cyber operations and digital espionage to advance its interests. Targeting companies like ASML and NXP, these efforts aim to acquire intellectual property and bolster Chinese research and development, exemplified by the Chimera hacking campaign against NXP between 2017 and 2020.[236]

The private sector is not the only valuable Dutch target for the PRC. In 2023, the Dutch Ministry of Defence research network was hacked, marking the first time that the Netherlands

---

228 Lucia Brancaccio, "China-Netherlands Relations: Bilateral Trade and Investments Overview," *China Briefing News*, April 9, 2024, https://www.china-briefing.com/news/china-netherlands-relations-bilateral-trade-and-investments-overview/.

229 Fons Klein Tuente, "The Netherlands Signs Memorandum of Understanding with Chinese Ministry of Science and Technology," *Netherlands Innovation Network*, October 11, 2023, https://netherlandsinnovation.nl/life-sciences-health/the-netherlands-signs-memorandum-of-understanding-with-chinese-ministry-of-science-and-technology/.

230 "Dutch Parliament: China's Treatment of Uighurs Is Genocide," World, *Reuters*, February 26, 2021, https://www.reuters.com/article/world/dutch-parliament-chinas-treatment-of-uighurs-is-genocide-idUSKBN2AP2CH/.

231 Toby Sterling, "Dutch Government Says China Seeks Military Advantage from ASML Tools," Technology, *Reuters*, February 19, 2024, https://www.reuters.com/technology/dutch-government-says-china-seeks-military-advantage-asml-tools-2024-02-19/.

232 Meaghan Tobin and Xinyun Wu, "The Small Company in Europe Caught in the Big Trade War Between the U.S. and China," Business, *The New York Times*, October 16, 2025, https://www.nytimes.com/2025/10/16/business/nexperia-netherlands-us-china.html. 2025. https://www.nytimes.com/2025/10/16/business/nexperia-netherlands-us-china.html

233 'Port of Rotterdam Position Paper 2024', 2024, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.portofrotterdam.com/sites/default/files/2024-04/Port%20of%20Rotterdam%20-%20Gateway%20to%20Europe.pdf.

234 Kan Ji Powell Lize Nauta, Jeffrey, 'Mapping Global Supply Chains – The Case of Semiconductors', Rabobank, accessed 1 September 2025, https://www.rabobank.com/knowledge/d011371771-mapping-global-supply-chains-the-case-of-semiconductors.

235 Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (European Commission) et al., *Study on the Critical Raw Materials for the EU 2023: Final Report* (Publications Office of the European Union, 2023), https://data.europa.eu/doi/10.2873/725585.

236 'Targeting of Dutch Chipmaker NXP | CFR Interactives', accessed 1 September 2025, https://www.cfr.org/cyber-operations/targeting-dutch-chipmaker-nxp.

accused the PRC of a state-sponsored cyber-attack.[237] Beijing also actively influences discourse in the Netherlands, both in the academic and political domain. Between 2018 and 2020, The Free University of Amsterdam's centre for human rights received €300,000 from PRC state-funded universities.[238] The centre worked on sensitive topics including the Uyghur prosecution in Xinjiang, and as a result of the funding adopted more pro-CCP talking points.[239] On the political side, investigations revealed in 2022 that the PRC had covertly established 'overseas police stations' with the goal of suppressing dissent from Chinese nationals living in the Netherlands.[240]

The Netherlands, while maintaining strong economic ties with the PRC, actively seeks to reduce dependency and strengthen domestic capabilities through a careful balancing strategy. This approach was formalised in 2019 with the Ministry of Foreign Affairs' report, 'The Netherlands-China: A New Balance,' which marked a shift toward cautious engagement, emphasising security concerns and a reserved outlook on joint economic activity. The Dutch balancing strategy thus focuses on EU and NATO cooperation, enhanced intelligence sharing, updated legal frameworks on hybrid threats, and public reporting on cyberattacks, while supporting domestic companies with training and threat alerts to bolster resilience against espionage.

Proposals to counter FIMI include forensic readiness information training in collaboration with Dutch intelligence for Dutch domestic companies that issues alerts and shares threat indicators.[241] The Netherlands also participates with the US and other European states in the CSA.[242] Furthermore, the government has also increased protection of critical target hubs including high-tech manufacturing and universities against Chinese influence. At the same time, the Netherlands cannot afford economic decoupling from the PRC and, while not heavily subject to economic coercion, it needs to maintain good trade relations with one of its major trading partners. This is exemplified in the de-escalation of the Nexperia case, that saw outgoing Economic Minister Karremans suspend the intervention at Nexperia after the PRC signalled it would resume chip exports to European companies.[243]

The Netherlands' balancing response to Chinese hybrid tactics hence speaks of a SMP that cautiously builds its national resilience through closer alignment with other powers and diversification away from the PRC, while avoiding and de-escalating direct confrontation with the PRC.

---

237 Ministerie van Defensie, 'Public annual report Netherlands Defence Intelligence and Security Service 2024 - Jaarverslag - Defensie.nl', jaarverslag, Ministerie van Defensie, 22 April 2025, 19, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/public-annual-report-2024-netherlands-defence-intelligence-and-security-service.

238 'China Financiert Onderzoek Naar Mensenrechten Aan VU', 19 January 2022, https://nos.nl/artikel/2413702-china-financiert-onderzoek-naar-mensenrechten-aan-vu.

239 'China Financiert Onderzoek Naar Mensenrechten Aan VU'.

240 'China heeft illegale politiebureaus in Nederland: aanwijzingen voor intimidatie', RTL.nl, 25 October 2022, https://www.rtl.nl/nieuws/onderzoek/artikel/5342214/china-illegale-politiebureaus-nederland-dissident-en-onderzoek.

241 Nationaal Cyber Security Centrum, "Bent u al klaar voor 'forensic readiness'? - Expertblogs - Nationaal Cyber Security Centrum," webpagina, Nationaal Cyber Security Centrum, May 12, 2021, https://www.ncsc.nl/actueel/weblog/weblog/2021/bent-u-al-klaar-voor-forensic-readiness.

242 "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System | CISA."

243 "Kritiek op minister Karremans na Nexperia-rel: 'Ingreep zonder enig overleg,'" *NOS.nl*, November 20, 2025, https://nos.nl/nieuwsuur/artikel/2591228-kritiek-op-minister-karremans-na-nexperia-rel-ingreep-zonder-enig-overleg.

4.3.2. **Philippines**

The Philippine's relation with the PRC has continuously fluctuated over the years, largely dependent on the ruling power's perceptions of Sino-American rivalry. Under Duterte (2016-2022) the Philippines avoided criticism against the PRC, including its treatment of Uyghur population, and issued a statement along with Cambodia supporting PRC policies.[244] With the election of Marcos to presidency (2022), the country shifted trajectory, pulling out of the BRI due to rising tensions in the South China Sea and the Philippines reconciliation with the US.[245] Currently, Manila has adopted a dual-track strategy towards the PRC: publicly documenting and condemning Chinese harassment under a "transparency initiative," while simultaneously broadening its security partnerships, notably with the United States Department of Defense and various foreign navies, to deter further Chinese aggression. Still, the Philippines refrains from provoking the PRC directly, as Beijing is still Manila's largest trading partner.[246]

To combat the rising influence of the US over the Philippines, the PRC has mostly focused on actions targeting the government or multiple sectors simultaneously in the aim to advance its strategic objectives.[247] To this end, the PRC's hybrid strategy in the Philippines has escalated over the years, increasing in frequency since 2014-2015 but also in diversity, combining more specifically digital warfare, paramilitary operations, and legal and political action making traceability and accountability difficult. Paramilitary operations have been undertaken mostly since 2017, following the decision by the Permanent Court of Arbitration which ruled that there was no legal basis for the PRC to claim historic right to resource within the nine-dash line in the South China Sea.[248] However, the PRC has persisted in their use of organised violence and military exercises with, for example, coast guards firing water cannons at vessels in August 2023, which the Philippines condemned as illegal and dangerous.[249] Beyond hybrid tactics at sea, China has pursued lawfare by challenging the legitimacy of Philippine maritime laws governing its exclusive economic zone and attempting to re-frame Manila's legitimate acts as provocative.[250] Marcos has strongly reassured the sovereignty of the Philippines over Scarborough Shoal by signing into law the 2016 arbitration.[251]

As a response, from 2016 and more intensely since 2020, the PRC has been involved in a series of sponsored cyber operations with the aim to destabilise and discredit the Filipino government, increase public and social tensions and collect information. In 2023, the Chinese government launched a cyberespionage campaign through the Chinese-linked

244 Agence France-Presse, "Philippines, 36 Other Countries Defend China over Xinjiang in UN Letter," ABS-CBN, July 12, 2019, https://www.abs-cbn.com/overseas/07/13/19/philippines-36-other-countries-defend-china-over-xinjiang-in-un-letter.

245 Tommy Walker, "Philippines Drops China's Belt and Road as Tensions Flare," *DW*, August 11, 2023, https://www.dw.com/en/philippines-drops-chinas-belt-and-road-as-tensions-flare/a-67344929.

246 Center for Preventive Action, "Territorial Disputes in the South China Sea," *Global Conflict Tracker*, September 17, 2024, https://cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea.

247 Richard Javad Heydarian, "A South China Sea Collision Brings US-Philippines Alliance to the Fore," *Lowy Institute* (Manila), August 14, 2025, https://www.lowyinstitute.org/the-interpreter/south-china-sea-collision-brings-us-philippines-alliance-fore.

248 "The 2016 South China Sea Arbitration: A Philippine Perspective and Lessons for Europe[:]," Leiden Asia Centre, June 13, 2019, https://leidenasiacentre.nl/english-the-2016-south-china-sea-arbitration-a-philippine-perspective-and-lessons-for-europe/.

249 "Philippines Accuses China of Water Cannon Attack in Spratly Islands," World News, *The Guardian* (Manila), August 6, 2023, https://www.theguardian.com/world/2023/aug/06/philippines-accuses-china-of-water-cannon-attack-in-spratly-islands.

250 Monica Sato, *Rhetoric vs. Reality: The Philippines, ASEAN, and the South China Sea*, July 11, 2025, https://www.csis.org/analysis/rhetoric-vs-reality-philippines-asean-and-south-china-sea.

251 Harrison Prétat and Gregory B. Poling, "Manila and Beijing Clarify Select South China Sea Claims," *Center for Strategic and International Studies*, November 21, 2024, https://www.csis.org/analysis/manila-and-beijing-clarify-select-south-china-sea-claims.

APT group Stately Taurus across Southeast Asia following the August water canon incidents in the Philippines.[252] This attack leveraged legitimate software to sideload malicious files to collect information.[253]

With the country dependent on the PRC for trade, the Filipino government mostly seeks to counter Chinese influence by finding other partners and investors, substituting the previous role of the PRC in the BRI.[254] For example, investments amounting 180 million USD from Japan, free trade agreements with South Korea and 6.2 billion USD of foreign investments in 2023 aim to counter the Philippine's dependence on Chinese investments and infrastructure.[255] These partnership also aim to reduce involvement of the PRC in internal affairs to avoid digital espionage. The government has set up intelligence networks and revised legal frameworks, allowing it to seize and arrets suspects of espionage.[256]

Governmental offices have also been dedicated to the monitoring of Cyber and Emerging Threats to provide direction in policy making against digital espionage, within the Directorates for Cyber intelligence and Weapons of mass Destruction.[257] Concurrently, the government has increasingly partnered with other countries which also consider the PRC as a threat to protect itself through mutual defence agreements such as the 2023 Bilateral Defence Guidelines between the US and the Philippines which reaffirms a shared vision of a free and open Indo-Pacific region.[258] Joint naval patrols with the US and Australia also strengthen the Philippines' resilience to Chinese hybrid threats.[259]

The emerging pattern indicates that the Philippines is balancing Chinese hybrid by aligning with other powers to strengthen national capabilities without direct provocation.

---

252 Unit 42, "Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific," *Unit 42*, November 17, 2023, https://unit42.paloaltonetworks.com/stately-taurus-targets-philippines-government-cyberespionage/.

253 Unit 42, "Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific."

254 "Philippines to Exit from China's Belt and Road Initiative - Times of India," *The Times of India*, November 4, 2023, https://timesofindia.indiatimes.com/world/south-asia/philippines-to-exit-from-chinas-belt-and-road-initiative/articleshow/104951862.cms.

255 Kris Crismundo, "4 Japanese Firms Investing P10.8-B in PEZA," *Philippines News Agency*, September 11, 2023, https://www.pna.gov.ph/articles/1209655; Briefing, "Philippines and South Korea Sign Free Trade Agreement," ASEAN Business News, September 25, 2023, https://www.aseanbriefing.com/news/philippines-and-south-korea-sign-free-trade-agreement/; "PH-US Trade Relations," Embassy of the Republic of the Philippines, accessed September 2, 2025, https://philippineembassy-dc.org/ph-us-trade-relations/.

256 Gabriel Dominguez, "Philippines Says Chinese 'Malign Influence Activities' Continue at High Pace," The Japan Times, September 13, 2025, https://www.japantimes.co.jp/news/2025/09/13/asia-pacific/philippines-espionage-china/.

257 "Brief History of the NICA," Republic of the Philippines: National Intelligence Coordinating Agency, accessed November 25, 2025, https://www.nica.gov.ph/about-us.html.

258 "FACT SHEET: U.S.-Philippines Bilateral Defense Guidelines," U.S. Department of Defense, accessed September 2, 2025, https://www.defense.gov/News/Releases/Release/Article/3383607/fact-sheet-us-philippines-bilateral-defense-guidelines/.

259 Aaron-Matthew Lariosa, "U.S., Philippines Begin Three Days of Joint Patrols in the South China Sea," *USNI News*, November 21, 2023, https://news.usni.org/2023/11/21/u-s-philippines-begin-three-days-of-joint-patrols-in-the-south-china-sea; Australian Associated Press, "Australia and Philippines Begin Joint Patrols in South China Sea as Regional Tensions Rise," World News, *The Guardian*, November 25, 2023, https://www.theguardian.com/world/2023/nov/25/australia-and-philippines-begin-joint-patrols-in-south-china-sea-as-regional-tensions-rise.

4.4. **Countering**

Countering states openly oppose China's tactics, employing confrontational measures that call out and actively counter hybrid activities across multiple domains. This more openly confrontational approach involves calling out the PRC's use of hybrid tactics and actively resisting to it. The level of resistance often depends on a state's capability to back up its diplomatic signalling with actions. For this reason, even countering states, while calling out the PRC and bolstering their defence, frequently struggle to actively confront the great power. Taiwan and Lithuania offer different perspectives on countering. For Taiwan, Chinese hybrid threats are part of an existential dilemma, while Lithuania maintains minimal bilateral engagement with the PRC. At the same time, they both confront the PRC's use of hybrid tactics, despite the associated escalation risks.

4.4.1. **Lithuania**

Lithuania has responded to escalating Chinese hybrid threats with a strategy of principled resistance, intensified EU and NATO alignment, and strengthened domestic resilience across political, economic, cyber and critical infrastructure domains. Relations between the PRC and Lithuania have been tense since 2021, when the Republic of China was allowed to open a representatives office under the name of 'Taiwan' rather than 'Taipei'.[260] The PRC perceived this as a violation of their sovereignty and the One-China principle and retaliated by recalling its ambassador, expelling Lithuania's envoy from Beijing, and downgrading its diplomatic relations with Lithuania to the level of charge d'affaires.[261] The PRC also implemented severe trade restrictions against Lithuania in 2022, including halting export permits for Lithuanian goods in sectors such as agriculture and timber.[262]

Additionally, they ceased certification processes, removed exporters from approved supply lists, pressured companies that have Lithuanian components in their supply chains, and delisted Lithuania as a country of origin for imports.[263] Beijing's pressure continued, with a notable incident in April 2023 when the PRC's ambassador to France questioned the Baltic states' sovereignty, stating that they lacked "effective status" under international law.[264] While Lithuania is part of the BRI since 2017, it has recorded very few investments from the PRC compared to other countries and more specifically since the embassy incident in August 2021. The country also trades in majority with other partners, with trade with the PRC amounting to a limited percentage of its total trade. In 2022, the newly elected prime minister

260 Joshua Askew, "The Story of How Little Lithuania Took on Global Superpower China," Euronews, October 24, 2023, https://www.euronews.com/2023/10/24/the-story-of-how-a-small-eu-state-like-lithuania-took-on-world-superpower-china.

261 Augustas Stankevičius Jakučionis,BNS,LRT.lt Jūratė Skėrytė,Saulius, "No Chinese Diplomats Remain in Lithuania," *Lrt.Lt*, June 16, 2025, https://www.lrt.lt/en/news-in-english/19/2591238/no-chinese-diplomats-remain-in-lithuania.

262 Mindaugas Laukagalis, "EU to Continue WTO Case against China's Restrictions on Lithuania," *Lrt.Lt*, January 24, 2025, https://www.lrt.lt/en/news-in-english/19/2469316/eu-to-continue-wto-case-against-china-s-restrictions-on-lithuania.

263 Laukagalis, "EU to Continue WTO Case against China's Restrictions on Lithuania."

264 Chris King, "Political Storm Brewing as Baltic States Summon Chinese Representatives over Remarks Made by China's Ambassador in Paris," *Euro Weekly News*, April 23, 2023, https://euroweeklynews.com/2023/04/23/political-storm-brewing-as-baltic-states-summon-chinese-representatives-over-remarks-made-by-chinas-ambassador-in-paris/.

took action to repair diplomatic relations with the PRC.[265] Despite the efforts, Sino-Lithuanian cooperation has remained low on all fronts.[266]

Recorded incidents of Chinese hybrid threat activity in Lithuania span a wide range of sectors targeting government and critical infrastructure, even before the 2021 incident. In 2019, Lithuanian intelligence raised concerns about Chinese companies such as Huawei offering gifts, paid trips, and training to influence public officials in Lithuania.[267] At the time Huawei was actively seeking to operate Lithuania's 5G infrastructure, sending its Vice President for cybersecurity to meet with unnamed government officials in the region. In November 2024, Chinese vessel Yi Peng 3 dragged its anchor along the seabed in the Baltic Sea for 100 miles, severing the connections of two undersea fibre-optic cables between Sweden and Lithuania, and Finland and Germany.[268] The PRC denied affected states the ability to conduct an investigation aboard but analysts have suggested that Beijing may have been involved in the sabotage. [269] The PRC has severely targeted Lithuania, principally as an example of consequences for the non-respect of the One China policy but also because of the government's early concern over Chinese influence.

As such, Lithuania illustrates how a country's willingness to openly challenge PRC narratives can make it more vulnerable to becoming a target of external pressure, while at the same time equipping it with the necessary tools to respond to threats openly and directly. Despite harsh economic retaliation measures from the PRC, Lithuania still took firm stances against Beijing in 2024 by blocking remote access control of Chinese companies in energy infrastructure.[270] This one followed Lithuania's public condemnation of the PRC for its attempt at undermining the sovereignty of the country, but also the opening of a case at the WTO from the European Union.[271] While several of Lithuania's allies were concerned the stance and actions taken by the Baltic state, principally due to fear of retaliation, the government was supported by the EU.[272]

Lithuania also took advantage of the complex situation to enhance cooperation with the EU and NATO, especially for building up its strategic protection domestically from foreign dependence. The country has pushed for enhanced cyber security requirements within both organisation with a particular focus on critical infrastructure and state institution coordination

---

265 Juris Sokolovskis, "Lithuanian PM Seeks to Restore Diplomatic Relations with China," *Euractiv*, April 16, 2025, https://www.euractiv.com/news/lithuanian-pm-seeks-to-restore-diplomatic-relations-with-china/.

266 Stuart Lau, "How Little Lithuania Dragged the EU into Its Showdown with China," POLITICO, October 6, 2021, https://www.politico.eu/article/lithuania-china-showdown-eu-impact/.

267 Konstantinas Andrijauskas, "A Diplomatic Incident in Lithuania Troubles Its Relationship with China," Articles, *Chinaobservers*, September 17, 2019, https://chinaobservers.eu/a-diplomatic-incident-in-lithuania-troubles-its-relationship-with-china/.

268 Miranda Bryant and Miranda Bryant Nordic correspondent, "Sweden Seeks Clarity from China about Suspected Sabotage of Undersea Cables," World News, *The Guardian*, November 28, 2024, https://www.theguardian.com/world/2024/nov/28/sweden-seeks-clarity-from-china-about-suspected-sabotage-of-undersea-cables.

269 Patrick Andersson et al., "What the Yi Peng 3 Cable-Cutting Incident Reveals about China-Russia Relations," *Swedish National China Centre*, March 5, 2025, https://kinacentrum.se/en/publications/what-the-yi-peng-3-cable-cutting-incident-reveals-about-china-russia-relations/.

270 BNS, "Lithuania Passes Law to Block Chinese Access to Solar and Wind Farm Systems," *Lrt.Lt*, November 12, 2024, https://www.lrt.lt/en/news-in-english/19/2411602/lithuania-passes-law-to-block-chinese-access-to-solar-and-wind-farm-systems.

271 Euractiv, "EU Launches WTO Case against China over Lithuania Row," *Euractiv*, January 28, 2022, https://www.euractiv.com/news/eu-launches-wto-case-against-china-over-lithuania-row/.

272 Sebastian Plociennik, "Germany and the Trade Conflict between Lithuania & China," *OSW Centre for Eastern Studies*, February 4, 2022, https://www.osw.waw.pl/en/publikacje/osw-commentary/2022-02-04/germany-and-trade-conflict-between-lithuania-china.

between public private, non-governmental and academic sectors.[273] Additionally, the Lithuanian government declared three staff members of the Chinese embassy persona non grata for violating the Vienna Convention and Lithuanian law.[274] Lithuania has therefore engaged in a countering strategy, refusing to tolerate the framing of the "violation" of the One China policy and, with EU's support, that the PRC's hybrid operations are unjustified.[275]

Lithuania's willingness to frame the PRC as a strategic threat was reaffirmed in July 2025, when it signed a memorandum of understanding with the Philippines addressing growing aggression from states such as the PRC.[276]

4.4.2. **Taiwan**

Taiwan has adopted a comprehensive and increasingly assertive posture to counter sustained Chinese hybrid threats, treating them as a central national security challenge that demands coordinated political, legal, cyber and societal resilience. It cannot be otherwise, considering that the PRC has long vowed to reunify with the self-governing island of Taiwan. Political tensions have escalated in recent years under the pro-sovereignty Democratic Progressive Party (DPP) which Beijing views as hostile to reunification. The government in Taipei in response has been pushing for strengthening their defence and taking a firm stance against Beijing. Taiwan is an essential target for Chinese hybrid operations due to its strategic geopolitical location, advanced technology sector (particularly in semiconductors) and symbolic role in CCP narratives about national reunification.[277]

The strategic objectives of these hybrid threats serve the PRC to undermine Taiwan's *de facto* sovereignty. In other words, the PRC hopes to influence political outcomes in Taiwan to favour pro-PRC candidates and deter foreign alliances, for example with the US and Japan, while furthering its unification agenda.[278] Given Taiwan's strategic capabilities and fundamental role in the world's information technology supply chain, the PRC also hopes to gain technological and strategic intelligence from Taiwanese systems.[279] The use of hybrid tactics serve the interest just mentioned, as cyber-attacks, like APT41's infiltration of government and research institutions, enables Beijing to steal sensitive data and monitor internal affairs.[280] Between 2008 and 2025, cyber operations have been the predominant mode of activity. In 2024 alone, Taiwan experienced an average of 2.4 million cyber-attacks per day, of which many were

273 "National Security Strategy," Ministry of National Defence of the Republic of Lithuania, March 2, 2016, https://www.newstrategycenter.ro/wp-content/uploads/2019/07/2017-nacsaugstrategijaen.pdf.

274 BNS, "Lithuania Expels Three Staff Members of Chinese Mission," *Lrt.Lt*, November 29, 2024, https://www.lrt.lt/en/news-in-english/19/2427422/lithuania-expels-three-staff-members-of-chinese-mission.

275 Paul Antonopoulos, "EU Urges China to Lift 'unjustified' Sanctions on Lithuania's Urbo and Mano Banks Greek City Times," *Greek City Times*, August 17, 2025, https://greekcitytimes.com/2025/08/17/eu-urges-china-to-lift-unjustified/.

276 Jim Gomez, "Lithuania and Philippines Sign a Pact to Build an Alliance against Aggression," AP News, June 30, 2025, https://apnews.com/article/philippines-lithuania-defense-cooperation-c7a2d3827ada567e2e6bab9efad93637.

277 Davis Ellison e.a., *From the Steppes of Ukraine to the Shores of Formosa: Lessons Learned from Contemporary War for Taiwan* (z.d.), https://hcss.nl/report/from-ukraine-to-formosa-lessons-learned-from-contemporary-war-for-taiwan/.

278 Robert D. Blackwill and Philip Zelikow, *The United States, China, and Taiwan: A Strategy to Prevent War*, no. 90, Council Special Report (Council on Foreign Relations, 2021), 26, https://cdn.cfr.org/sites/default/files/report_pdf/the-united-states-china-and-taiwan-a-strategy-to-prevent-war.pdf.

279 Robert D. Blackwill and Philip Zelikow, *The United States, China, and Taiwan: A Strategy to Prevent War*, 18.

280 *BlackTech* (Council on Foreign Relations, 2020), https://www.cfr.org/cyber-operations/blacktech; *Targeting of Taiwanese Government Agencies and Officials' Email Accounts* (Council on Foreign Relations, 2020), https://www.cfr.org/cyber-operations/targeting-taiwanese-government-agencies-and-officials-email-accounts.

linked to the PRC.[281] Meanwhile, election interference and disinformation campaigns seek to erode public trust in democratic institutions and promote pro-PRC sentiment.[282]

Additionally, China's use of lawfare against Taiwan seeks simultaneously to intimidate and pressure Taiwanese society, erode Taipei's territorial claims and de facto sovereignty, isolate it diplomatically, and construct legal narratives intended to justify potential future action.[283] Finally, economic coercion, like the banning of Taiwanese agricultural and petrochemical exports, pressures Taiwan's industries while signalling consequences for political noncompliance.[284] Specific examples include the 2022 Chinese import ban on Taiwanese goods and the 2023 targeted cyber espionage attack. The 2022 example was described by the Taiwanese government as a politically motivated ban and part of a larger economic pressure campaign. The fish industry was severely impacted with 91% of exports previously going to the PRC.[285] The 2023 cyber-attack was attributed to Earth Longzhi, a subgroup of APT41, which used customised Cobalt Strike loaders and tools like Mimikatz to target Taiwan's defence and finance sectors.[286]

In terms of local vulnerabilities at play, Taiwan's limited international recognition complicates comprehensive defensive responses. The elected government is however largely vocal in denouncing the PRC's actions and often engages in diplomatic signalling, strengthening its position towards its population as a legitimate provider of security.[287] Additionally, the wide

281 Yimou Lee and Yimou Lee, "Chinese Cyberattacks on Taiwan Government Averaged 2.4 Mln a Day in 2024, Report Says," Cybersecurity, *Reuters*, January 6, 2025, https://www.reuters.com/technology/cybersecurity/chinese-cyberattacks-taiwan-government-averaged-24-mln-day-2024-report-says-2025-01-06/.

282 Helen Davidson, "China Unveils Taiwan Economic 'Integration' Plan as Warships Conduct Manoeuvres off Coast," World News, *The Guardian*, September 13, 2023, https://www.theguardian.com/world/2023/sep/13/china-unveils-taiwan-economic-integration-plan-as-warships-conduct-manoeuvres-off-coast; James Pomfret et al., "China Wields Mazu 'peace Goddess' Religion as Weapon in Taiwan Election," Asia-Pacific, *Reuters*, December 21, 2023, https://www.reuters.com/world/asia-pacific/china-wields-peace-goddess-religion-weapon-taiwan-election-2023-12-21/; Yuan Lin, "China Hopes Mazu, a Sea Goddess, Can Help It Win over Taiwan," *The Economist*, June 15, 2023, https://www.economist.com/china/2023/06/15/china-hopes-mazu-a-sea-goddess-can-help-it-win-over-taiwan?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gad_source=1&gclid=EAIaIQobChMI096Xs_LyjAMV9KGDBx2Zx-wRQEAAYASAAEgI8LPD_BwE&gclsrc=aw.ds; Chung Li-hua et al., *MAC Rejects Fujian Plan - Taipei Times*, Taiwan News, June 18, 2023, https://www.taipeitimes.com/News/taiwan/archives/2023/06/18/2003801721.

283 "Lawfare: China's Legal Initiatives against Taiwan," IISS, accessed December 2, 2025, https://www.iiss.org/charting-china/2025/01/charting-china-chinas-legal-initiatives-against-taiwan/.

284 Amy Chang Chien, 'First Pineapples, Now Fish: To Pressure Taiwan, China Flexes Economic Muscle', Business, *The New York Times*, 20221-06-22, https://www.nytimes.com/2022/06/22/business/china-taiwan-grouper-ban.html.

285 Chien, "First Pineapples, Now Fish"; "Taiwan Threatens to Take China to WTO in New Spat over Fruit," China, *Reuters*, September 19, 2021, https://www.reuters.com/world/china/china-halts-taiwan-sugar-apple-wax-apple-imports-prevent-disease-2021-09-19/.

286 Hara Hiroaki and Ted Lee, *Hack the Real Box: APT41's New Subgroup Earth Longzhi* (Trend, 2022), https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html; *Incident Details:Chinese State-Sponsored Hacking Group Earth Longzhi Gained Access to Various Targets in Taiwan and the Banking Sector in China Beginning in 2020* (European Repository of Cyber Incidents, 2024), https://eurepoc.eu/table-view/?cyber_incident=1671.

287 "Taiwan Condemns China for 'shooting' Drills off Taiwanese Coast," Reuters, February 26, 2025, https://www.reuters.com/world/china/taiwan-flags-chinas-shooting-drills-off-southwest-coast-2025-02-26/; "Taiwan Condemns China over Harassment of Athletes at Universiade - Focus Taiwan," Focus Taiwan - CNA English News, July 24, 2025, https://focustaiwan.tw/politics/202507240011; "Taiwan Condemns China's Military Drills, Vows to Maintain Regional Peace," website, Taiwan Today, Ministry of Foreign Affairs, Republic of China (Taiwan), April 2, 2025, https://taiwantoday.tw/politics/top-news/267831/taiwan-condemns-china%e2%80%99s-military-drills%2c-vows-to-maintain-regional-peace.

adoption of third-party hardware and software increases vulnerabilities.[288] The Taiwanese government has however focused its battle against Chinese digital espionage through severe countering measures such as the restauration of military court systems to handle espionage and sedition cases, the amendment of laws to punish expressions of loyalty to the PRC and an increased scrutiny of Chinese-issued identity documents in both civilian and military personnel.[289]

To enforce the protection of information and prevent surveillance, Taiwan has also largely invested in adapting legal frameworks such as the Cybersecurity Management act revision in 2025 to address emerging challenges in the safeguarding of national security.[290] It also possesses several Computer Emergency Response Teams (CERTs) across the government and society to counter cyber operations which themselves belong to large networks of CERTs, both within and outside the borders, allowing for an effective prevention, detection and attribution of cyber-attacks.[291] The government has also implemented extensive prevention campaigns against FIMI, especially during elections, to increase societal media literacy.[292] These ones are supported by fact checking groups like Taiwan's Fact Check Centre.[293] The government has also imposed bans on several Chinese owned platforms and communication networks.

Taiwan therefore takes Chinese hybrid threats as a crucial national security threat and acts in consequence despite its limited means.

---

288 Tania Garcia-Millan et al., *Perspectives on Taiwan Insights from the 2018 Taiwan-U.S. Policy Program* (Centre for Strategic and International Studies, 2019), 11, https://www.gmfus.org/sites/default/files/2021-12/2018%20TUPP%20Report.pdf; Lawrence Chung, "Taiwan Leader Tsai Ing-Wen's Office Targeted in Suspected Cyberattack," South China Morning Post, May 18, 2020, https://www.scmp.com/news/china/politics/article/3084931/taiwan-presidents-office-targeted-suspected-cyberattack.

289 "President Lai Holds Press Conference Following High-Level National Security Meeting," Office of the President Republic of China(Taiwan), March 13, 2025, https://english.president.gov.tw/News/6919; Harun Talha Ayanoglu, "A Threat from within: Chinese Espionage in Taiwan," *CEIAS*, May 19, 2025, https://ceias.eu/a-threat-from-within-chinese-espionage-in-taiwan/.

290 "Cyber Security Management Act," Laws & Regulations Database of The Republic of China (Taiwan), June 6, 2018, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297.

291 "TWCERT/CC Taiwan Computer Emergency Response Team/Coordination Center," accessed November 25, 2025, https://www.twcert.org.tw/en/mp-2.html.

292 Huizhong Wu and David Klepper, "How Taiwan Preserved Election Integrity by Fighting Back against Disinformation," World, *PBS News*, January 27, 2024, https://www.pbs.org/newshour/world/how-taiwan-preserved-election-integrity-by-fighting-back-against-disinformation.

293 Huynh Tam Sang et al., "How Taiwan Fights the Disinformation War," *The Interpreter* (Taiwan), June 20, 2024, https://www.lowyinstitute.org/the-interpreter/how-taiwan-fights-disinformation-war.

5. Implications for counter-hybrid posture for SMPs

By concretely identifying both the strategies and the contextual factors which impact the type of responses adopted by SMPs to counter hybrid threats stemming from the PRC, this research helps SMPs moving from approaches primarily reliant on ad-hoc responses to coherent strategic posturing against GP hybrid threats. Such an approach can help mitigate both the direct impact of hybrid threats as well as improve perceptions of an SMPs power, in turn contributing to deterrence. This is approach is particularly important when responding to threats stemming from the PRC, due to the many tactics at its disposal as well as their use in synchronised and locally enabled ways, which is characteristic of the hybrid threat toolbox.

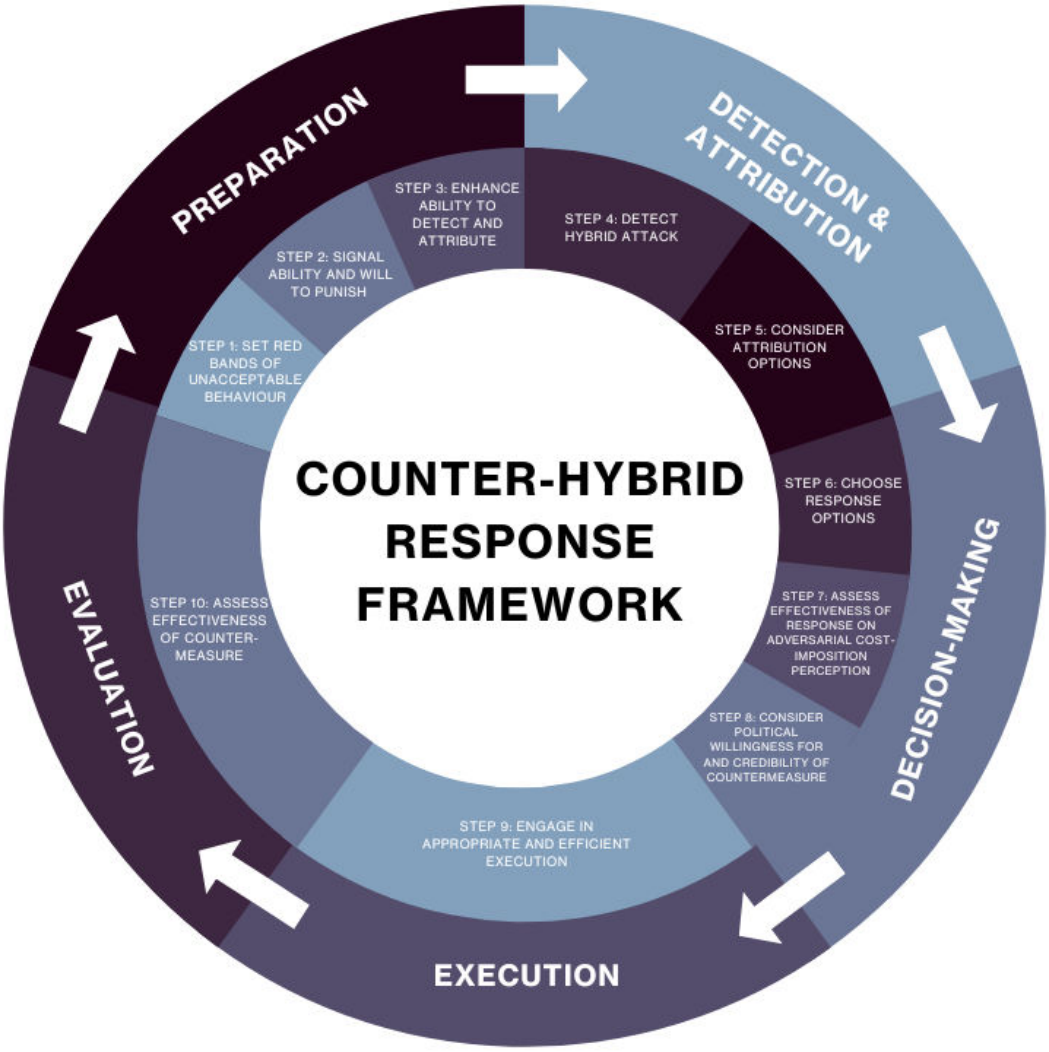
To manage this complexity, an awareness and understanding of an SMP's positioning within the larger geopolitical context is necessary to effectuate appropriate responses. In turn, to build long-term resilience ad-hoc responses are likewise not efficient with the PRC, especially considering the often-limited capabilities of SMPs and the perhaps overwhelming variety of strategies available to counter hybrid threats. Therefore, the starting point should not be an assumption of a disadvantageous position but rather an appreciation of the specific tools at the disposal of SMPs based on a constellation of their specific context and strategic objectives. The expectation should not be that an SMP is prepared to respond to any specific hybrid threat, but rather that when a threat occurs, thinking does not start from zero and instead draws on an existing and known set of available tools, aligned with the overarching state policy. This allows SMPs to maximise their capabilities and preparedness while exploiting their strengths. Depending on the response strategy, policy guidelines for counter-hybrid will vary significantly.

5.1. Stages and steps in developing SMPs posturing

Previous HCSS research suggested a set of non-technical policy guidelines for a counter-hybrid posture for SMPs that explains how core good practices of cross-domain deterrence can be developed, applied and embedded into policies and practice. The framework proposed five stages: of (i) the Preparation Stage, (ii) the Detection & Attribution Stage, (iii) the Decision-Making Stage, (iv) the Execution Stage, and (v) the Evaluation Stage. The research highlighted how for each stage, there are ten consecutive steps to be taken at the policy level for crafting proportional strategies while managing escalation and anticipating ripple effects, as summarised in Figure 11.[294]

[294] Mattia Bertolini et al., *Ten Guidelines for Dealing with Hybrid Threats: A Policy Response Framework* (The Hague Centre for Strategic Studies, 2023), 5–6, https://hcss.nl/report/ten-guidelines-for-dealing-with-hybrid-threats/.

Figure 11: Counter-hybrid response framework



The application of such stages and steps to the four response strategies shows the implications of overarching strategic choices for the counter-hybrid posture of SMPs, as shown below in Table 5.

Table 5: Implications of strategic choices for counter-hybrid posturing

Stage	Step	Bandwagoning	Hedging	Balancing	Countering
Preparation	Step 1: Set red bands of unacceptable behaviour	Limited in scope due to close alignment with the PRC; red bands may be blurred or overlooked.	Red bands are clearly defined but with strategic ambiguity to maintain flexibility.	Red bands set against Chinese influence; clearly defined to counter Chinese hybrid tactics.	Red bands are clearly defined to deter and confront the PRC's hybrid tactics head-on.
	Step 2: Signal ability and will to punish	Minimal signalling; strategic ambiguity is key.	Signals a willingness to work within multiple spheres but without direct confrontation.	Strong signals of deterrence through multilateral alliances and defensive capabilities.	Clear signalling of deterrence through direct actions (e.g., economic sanctions, cyber retaliation).
	Step 3: Enhance ability to detect and attribute	Investment focused on detection, attribution is downplayed to avoid confrontation.	Investment in detection tools is moderate, focused on ensuring resilience without overt alignment.	High investment in detection and attribution to identify Chinese hybrid operations.	Extensive investment in detection and attribution, especially to identify covert operations like cyber threats.
Detection & attribution	Step 4: Detect hybrid attack	Detection mechanisms in place as awareness remains key to assess vulnerability to PRC's hybrid threats.	Detection mechanisms in place but focus remains on mitigating risks through diversified ties.	Strong detection mechanisms to identify hybrid attacks by the PRC across multiple domains.	High-level detection capacity for immediate identification and response to hybrid threats from the PRC.
	Step 5: Consider attribution options	Attribution avoided or downplayed to prevent escalation or direct confrontation.	Attribution handled cautiously; options are open to diplomatic solutions rather than direct confrontation.	Clear attribution when hybrid threats are identified, potentially aligning with international partners.	Immediate attribution to the PRC with a clear public stance to signal accountability and response.
Decision-making	Step 6: Choose response options	Passive response options or limited engagement due to strategic alignment with the PRC.	Response options balanced across different domains; open to both punitive and incentivised measures.	Strong response options focusing on collective action with allies, leveraging military, economic, and political responses.	Aggressive response options, including targeted actions such as sanctions, military deterrence, and cyber retaliation.
	Step 7: Assess effectiveness of response on adversarial cost-imposition perception	Likely low impact on cost-imposition perception due to alignment.	Moderate impact; perception of costs managed by maintaining strategic ambiguity and flexibility.	High impact, as the response is clear and involves multilateral actions that impose considerable costs on the PRC.	High impact; costs for the PRC are significant, including economic and diplomatic fallout.
	Step 8: Consider political willingness for and credibility of countermeasure	Low political willingness for aggressive countermeasures due to reliance on Chinese support.	Moderate willingness, balancing between domestic and international considerations.	High political willingness; strong international backing, especially within alliances and coalitions.	Very high willingness to implement countermeasures, often with international coalitions or public backing.
Execution	Step 9: Execute response option and implement countermeasures	Passive implementation; minimal actions beyond diplomatic engagement.	Balanced execution, focused on strengthening resilience and addressing potential threats.	Strong execution through multilateral coalitions, with coordinated responses to Chinese hybrid tactics.	Strong execution with direct and swift action against hybrid threats (e.g., sanctions, cyber responses).
Evaluation	Step 10: Assess effectiveness of countermeasure	Minimal assessment due to limited engagement and lower stakes in direct confrontation with the PRC.	Moderate assessment, focusing on whether hedging measures are maintaining equilibrium.	High assessment of effectiveness, considering the long-term strategic impact of balancing against the PRC's hybrid tactics.	Rigorous evaluation to determine if deterrence has been successful and if the PRC's actions have been thwarted.

States adopting a **bandwagoning** posture approach hybrid threat with restraint and alignment. During the preparation phase, these states define red lines narrowly, signalling minimally and avoiding overt confrontation with the PRC. Their efforts are focused on detection, as it is still in the interest of the bandwagoner to be aware of its own vulnerabilities and the PRC's leverages. However, attribution efforts are limited, emphasising non-confrontational engagement to mitigate escalation risk. In the decision-making phase, responses are largely passive or restricted, reflecting strategic alignment with the PRC, while political willingness to impose countermeasures is low. Execution remains minimal, focused on

diplomatic engagement, and evaluation of counter-hybrid measures is constrained by limited engagement and low stakes.

Hedging states maintain a calibrated, flexible posture that balances risk and strategic ambiguity. Preparation involves clearly defined but adaptable red lines and cautious signalling, allowing engagement across multiple spheres without direct confrontation. Detection mechanisms target emerging threats while mitigating risks, and attribution is handled carefully, favouring diplomatic solutions. Decision-making blends punitive and incentivised measures, with moderate attention to the perception of cost imposition and political credibility. Execution and evaluation emphasise measured responses that maintain equilibrium and strengthen resilience against hybrid threats from the PRC.

Balancing strategies reflect proactive, coordinated approaches designed to deter hybrid operations through credible collective action. In preparation, red lines are set clearly, deterrence is signalled strongly, and investment in detection and attribution is high. Detection and attribution mechanisms are robust, enabling identification of hybrid attacks by the PRC and alignment with international partners. Decision-making emphasises strong responses leveraging military, economic, and political tools, with high political willingness to act in coordination with allies. Execution is multilateral and coordinated, while evaluation focuses on the effectiveness of these measures in shaping long-term strategic outcomes against the PRC's hybrid tactics.

Countering states adopt an assertive, high-cost posture, signalling immediate readiness to confront hybrid threats from the PRC. Preparation includes clearly defined red lines and direct deterrence through visible actions, supported by extensive investment in detection and attribution. Detection and attribution capabilities enable rapid identification and public attribution of hybrid operations, creating accountability. Decision-making is aggressive, combining sanctions, military options, and cyber responses, with very high political willingness to implement countermeasures. Execution is swift and decisive, and evaluation rigorously assesses the success of deterrence and the neutralisation of hybrid threats from the PRC.

All four postures offer different benefits and drawbacks, highlighting the trade-offs of each response type. Still, all four offer valid policy options for SMPs to position themselves towards the PRC's hybrid threats. By individuating their overarching strategy, policymakers can maximise their country's efforts, resources, and capabilities.

SMPs cannot rely solely on ad-hoc responses to counter Chinese hybrid threats; instead, they must develop a coherent overarching strategy grounded in an understanding of their own capabilities, context, and strategic objectives. By identifying both the threats and the tools available, SMPs can anticipate challenges, make informed decisions, and align responses across multiple domains, thereby enhancing resilience and deterrence. This in turn allows SMPs to operationalise strategic thinking in practice, ensuring that each response draws on pre-established options rather than reactive improvisation. Ultimately, the foundation of an effective posture for SMPs with limited resources and capabilities lies in self-awareness and strategic preparation.

5.2. **Dilemmas in SMPs posturing**

SMPs in both Europe and the Asia-Pacific face complex trade-offs when shaping their posture toward China's hybrid threats. Across regions, SMPs must navigate structural tensions that shape the feasibility and risks of adopting strategies of bandwagoning, hedging, balancing, or countering, all while factoring in the potential for Chinese retaliation.

The **sovereignty-retaliation dilemma** is central to SMP decision-making across both regions. European SMPs, as illustrated by Lithuania's experience after strengthening ties with Taiwan, must weigh principled actions against the risk of Chinese economic coercion.[295] This dynamic can produce hesitation or self-deterrence, pushing some states toward bandwagoning or cautious hedging to avoid retaliation. In the Asia-Pacific, sovereignty assertions are met not only with economic pressure but with synchronised and recurrent physical coercion, including maritime militia swarming, cyber intrusions, and targeted disinformation campaigns.[296] SMPs such as the Philippines and Taiwan must therefore evaluate responses not just in terms of economic cost but in terms of the likelihood and severity of direct retaliation, making balancing and countering particularly high-risk strategies.

The **openness-resilience dilemma** also intersects closely with retaliation risk. European SMPs rely heavily on openness for economic growth, research collaboration, and investment. Still, these same channels create vulnerabilities to foreign interference and technology leakage. The EU's own frameworks on hybrid threats emphasise the growing use of information manipulation, cyber-attacks, and economic coercion as core components of hybrid operations that undermine resilience.[297] In Asia, deep integration into Chinese-led value chains means that restricting access to Chinese vendors or revising infrastructure arrangements can provoke immediate economic or coercive retaliation, especially for export-dependent economies like Malaysia, Thailand, Vietnam, and Indonesia.[298] Measures required for balancing or countering, such as stricter investment screening or tighter vetting of foreign researchers, can trigger Chinese diplomatic or economic pushback, reinforcing the incentive for measured hedging which however limits the degree of openness to actors outside of the PRC.

Lastly, the **collective-national dilemma** diverges sharply between Europe and the Asia-Pacific. European SMPs benefit from EU-level mechanisms such as the Anti-Coercion Instrument, Network and Information Systems Directive 2, and the Hybrid Toolbox, that provide collective leverage, which can reduce exposure to direct Chinese retaliation, offering an extra layer of protection to states choosing a more confrontational strategy. However, EU-driven action may also escalate tensions in ways that individual SMPs cannot control,

---

295 William Piekos, "Investigating China's Economic Coercion: The Reach and Role of Chinese Corporate Entities," *Atlantic Council*, November 6, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/investigating-chinas-economic-coercion/.

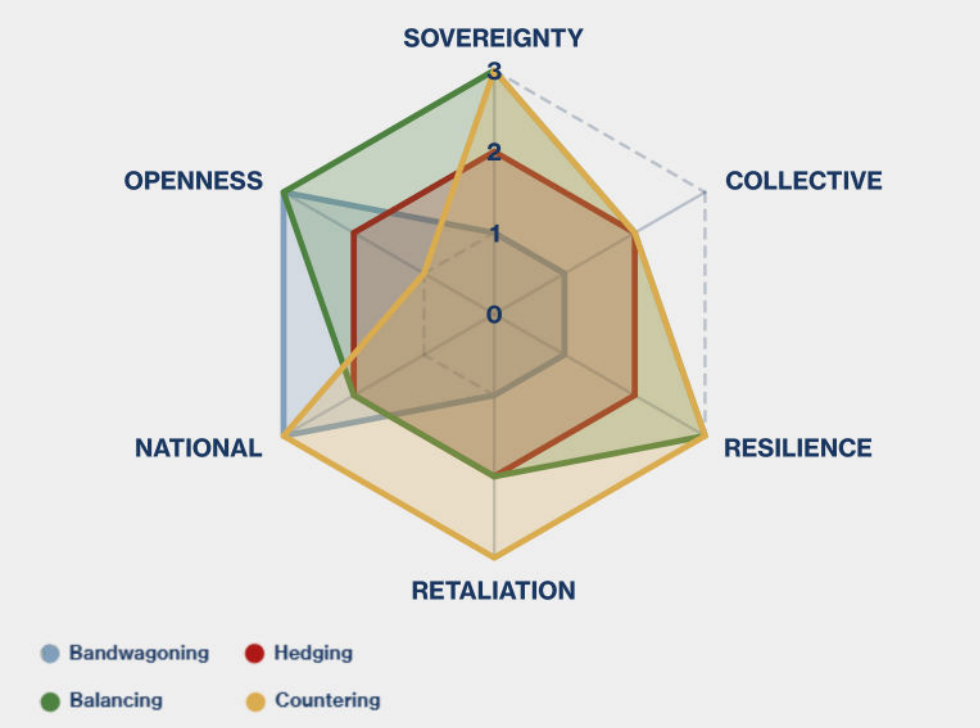
296 Tang Meng Kit, "China's Gray-Zone Hybrid Threats against Taiwan's Pacific Allies," *Asia Times*, July 14, 2025, https://asiatimes.com/2025/07/chinas-gray-zone-hybrid-threats-against-taiwans-pacific-allies/; Logan Wright et al., "Retaliation and Resistance: China's Economic Statecraft in a Taiwan Crisis," *Atlantic Council*, April 2, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/retaliation-and-resilience-chinas-economic-statecraft-in-a-taiwan-crisis/.

297 "Countering Hybrid Threats," European Union External Action, March 18, 2024, https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en.

298 Gatra Priyandita, *Hybrid CoE Working Paper 25: Chinese Economic Coercion in Southeast Asia: Balancing Carrots and Sticks* (Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats, 2023), https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-25-chinese-economic-coercion-in-south-east-asia-balancing-carrots-and-sticks/.

producing internal political pressure to hedge or moderate collective balancing.[299] In Asia, the absence of supranational institutions limits collective action, meaning SMPs face retaliation individually and must manage pressure from China on a bilateral basis. ASEAN's consensus-based decision-making and non-interference norms have limited the bloc's capacity to take unified positions on security issues with China, often resulting in weak or delayed collective responses.[300] Asia-Pacific powers thus have to factor in their national capabilities alone when choosing an overarching strategy. At the same time, this gives states more decisional autonomy at the national level.

Figure 12: Dilemmas in SMPs posturing



Taken together, these dilemmas (summarised in Figure 12)underscore that SMPs' strategic choices are driven not only by capabilities but by also structural exposure, economic interdependence, and regional institutional environments. Bandwagoning eases the sovereignty–retaliation trade-off by minimising confrontation and short-term coercive pressure, but it deepens dependence, constrains national autonomy, and weakens long-term resilience. Hedging seeks to balance sovereignty, openness, and retaliation risks through flexibility and ambiguity, preserving room for manoeuvre while accepting only partial resilience and the risk of strategic incoherence. Balancing prioritises sovereignty and resilience through national or collective deterrence, reducing long-term vulnerability but raising immediate economic and

[299] "Hybrid Threats," European Council; "Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns," European Council, June 21, 2022; "NIS2 Directive: Securing Network and Information Systems | Shaping Europe's Digital Future," European Council, accessed December 12, 2025, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[300] Leticia Simões, "The Role of ASEAN in the South China Sea Disputes," *E-International Relations*, June 23, 2022, https://www.e-ir.info/2022/06/23/the-role-of-asean-in-the-south-china-sea-disputes/.

political costs, particularly where institutional support is limited. Countering most forcefully asserts sovereignty and addresses openness-related vulnerabilities by actively resisting coercion and hybrid threats, yet it amplifies retaliation and escalation risks across all three dilemmas, making it the most demanding posture in terms of capacity and political resolve. For SMPs in both Europe and the Asia-Pacific, coherent posturing requires acknowledging these trade-offs upfront and embedding them into national and regional strategies. Figure 7 below summarises the application of these dilemmas to each strategy.

6. Conclusion: practical recommendations for a coherent counter-hybrid posture for small and middle powers

Hybrid threats have emerged as a persistent and structural feature of the contemporary security landscape. For SMPs, these threats are central challenges that intersect with questions of sovereignty, strategic autonomy, and economic resilience. This report has analysed how the PRC employs hybrid tactics across Europe and the Asia-Pacific and how SMPs in these regions respond to these pressures.

The findings highlight that the PRC has at its disposal a wide array of hybrid tools spanning digital and information warfare, economic and financial coercion, paramilitary operations, physical sabotage, and legal-political activities. Crucially, these tools are not deployed in isolation. As is characteristic of hybrid threat actors, the PRC uses them in a synchronised and locally enabled way. Cyber intrusions may be combined with disinformation, economic inducements with elite capture, and maritime pressure with lawfare. Local actors, such as commercial entities, elites, diaspora networks, and sympathetic political forces, are often instrumental in amplifying these effects. This mode of operation complicates attribution and response, especially for SMPs whose institutional capacities and resources are limited.

In this environment, SMPs face a structural disadvantage vis-à-vis the PRC. They often lack the capabilities and strategic depth to absorb sustained hybrid threats without incurring significant costs. This asymmetry is exacerbated when SMPs responses are predominantly ad-hoc. While reactive measures may address individual incidents, they rarely reduce long-term vulnerability. This means they are not efficient in the long run when dealing with the PRC, particularly given the breadth of its hybrid toolkit and its ability to exploit vulnerabilities and dependencies.

This research has therefore focused on conceptualising how SMPs can move from ad-hoc responses towards coherent strategic posturing against hybrid threats, especially those of the PRC. It has argued that responses to hybrid threats cannot be understood, or designed, solely at the tactical level. Instead, they must be contextualised within the broader strategic position of the SMP, namely its capabilities, stakes, dependencies, and alignments.

To make this strategic dimension visible, the report has proposed a framework that categorises SMP responses into four broad strategies: (1) bandwagoning, (2) hedging, (3) balancing, and (4) countering. These strategies capture different ways in which SMPs can position towards the PRC's hybrid threats. Bandwagoning involves aligning with the PRC to avoid destructive hybrid measures and secure economic or political benefits, often at the expense of autonomy. Hedging reflects efforts to maintain cooperative ties with the PRC while cultivating alternative partnerships to manage risk. Balancing emphasises resilience-building and alignment with other powers or alliances to offset PRC influence. Countering denotes more overt and confrontational efforts to expose, deter, or punish hybrid activities.

While making a choice of strategy, SMPs in Europe and the Asia-Pacific must however navigate three structural dilemmas that shape the risks and feasibility of bandwagoning, hedging, balancing, or countering the PRC's hybrid threats. First, the **sovereignty–retaliation** dilemma forces states to choose between defending sovereign or principled positions and avoiding economic, diplomatic, or coercive retaliation, often encouraging caution or hedging. Second, the **openness–resilience** dilemma arises because economic openness and integration support growth but simultaneously expose states to foreign interference, coercion, and security vulnerabilities. Third, the **collective–national** dilemma concerns whether to rely on collective mechanisms to share risk and deter coercion, which can dilute national control, or to act independently, which preserves autonomy but leaves states more exposed to retaliation.

The eight case studies examined in the report illustrate how these strategies and trade-offs play out in practice and how they shape both exposure to, and responses against, hybrid threats. Hungary and Cambodia, for instance, demonstrate how bandwagoning can secure investment and political support but deepen structural dependencies and reduce scope for independent counter-hybrid action. Italy and Malaysia show how hedging can generate flexibility but also create tensions and ambiguities in policy. The Netherlands and the Philippines highlight how balancing strategies can enhance resilience and deterrence while risking economic or diplomatic costs. The cases of Lithuania and Taiwan show the multifaceted sides of countering, where autonomy meets escalatory risks.

The research does not prescribe which of these strategies SMPs should adopt. It does not tell SMPs how to respond to specific forms of economic coercion, disinformation, or cyber operations. Instead, it shows how SMPs can prepare themselves to respond more coherently and consciously. Preparation in this sense means understanding how their posture shapes the threats they face and the tools available to address them; recognising the trade-offs inherent in different strategic choices; and building internal and external arrangements that align with long-term priorities.

This preparation enables SMPs to move away from fragmented, incident-driven responses towards coherent, concerted efforts. For SMPs, such coherence is indispensable, allowing them to maximise the effect of limited resources and prioritise resilience-building in critical areas. SMPs should hence (a) review their capabilities, stakes, and strategic position; (b) build sustained cross-domain awareness of hybrid threats; and (c) ensure coherence between

internal messaging and external strategic positioning in order to posture themselves effectively vis-à-vis China's hybrid activities. At the same time, SMPs should be mindful of the dilemmas and trade-offs that each strategic posture entails.

States' responses to hybrid threats thus vary by strategic posture, but even the most accommodating strategies retain important defensive elements.

Bandwagoning emphasises restraint and alignment, yet it still prioritises detection and preparation in order to understand vulnerabilities and the PRC's leverage; however, attribution is deliberately muted or avoided, with incidents downplayed or handled privately to minimise escalation and preserve stable relations.

Hedging adopts a flexible and calibrated approach, combining cautious signalling, selective and largely diplomatic attribution, and measured responses that balance risk management with resilience-building.

Balancing involves proactive and coordinated deterrence, characterised by clear red lines, strong detection and attribution capabilities, and robust collective responses designed to impose costs and shape long-term behaviour.

Countering reflects the most assertive posture, with explicit deterrence, rapid public attribution, and decisive use of economic, cyber, and military tools, accepting high costs in order to confront and neutralise hybrid threats directly.

Therefore, the four strategic postures -bandwagoning, hedging, balancing, and countering- provide distinct pathways for managing China's economic, political, and hybrid influence. On the basis of this, it is possible to identify practical recommendations designed to help policymakers in SMPs move towards a more deliberate and coherent counter-hybrid posture and tailored to each of the four archetypical strategies even those whose political leaders feel forced to bandwagon with the PRC:

6.1. Bandwagoning

The focus of bandwagoning SMPs is on preserving relations while benefitting from economic integration with China and minimise and confrontation's risk. To achieve a coherent hybrid threat posture, SMPs should:

6.1.1. Identify and strengthen key points of interconnection with the PRC

Identify key points of interconnection with the PRC and strengthen areas such as trade relations to generate spillover benefits that enhance the state's overall strategic position and reduce disruptive effects of hybrid threats.

6.1.2. Map and stress-test dependencies

Identify economic dependencies on the PRC, particularly in infrastructure, technology, and energy. Evaluate risks of overreliance on Chinese investments (e.g., BRI projects) and supply chains through mapping exercises and stress tests.

6.1.3. Implement mechanisms to monitor and evaluate Chinese economic leverage

Implement mechanisms to track the PRC's economic leverage, especially regarding trade relations and financial influence. These include scrutiny of investment agreements, tracking capital flows, and gathering and analysing investment data.

6.1.4. Create institutional oversight

Establish economic oversight committees to integrate intelligence on economic dependencies and disinformation campaigns that support the PRC's interests in the SMP.

6.1.5. Maintain calibrated public messaging

Maintain ambiguity in domestic messaging to avoid signalling negatively towards the PRC but also to avoid negative public perceptions of alignment with the PRC.

6.1.6. Align domestic policy with strategic messaging

Ensure that domestic policies regarding infrastructure development and foreign investment align with the SMP's economic bandwagoning stance without overtly signalling subordination to the PRC. This entails signalling autonomy and sovereign capacity (i.e. maintaining a clearly defined international policy agenda).

6.2. Hedging

Hedging SMPs privilege flexibility, diversification of alliances, and risk management. As such, they should:

6.2.1. Reassess national interests and areas for calibrated engagement

Review key national interests and identify where SMPs have leeway to engage with the PRC without becoming overly reliant. Focus on cybersecurity, information resilience, and economic diversification.

6.2.2. Identify tools needed for more effective preparedness

Identify the tools that need to be developed in order to be more effective in potential responses, such as assessing whether threats are sufficiently high and persistent to justify the creation of dedicated units to counter Chinese disinformation, and determining where economic dependence is excessive and could be offset by strengthening or expanding other sectors when full decoupling or de-risking is not feasible.

6.2.3. Build integrated, cross-domain early-warning systems

Create integrated cross-domain early warning systems that can detect hybrid threats in real-time, especially cyberattacks or disinformation campaigns. This should involve government coordination with the private sector and existing public services (e.g., police, cyber units, etc).

6.2.4. Establish a national strategic coordination task force

Create a national strategic coordination task force, bringing together key stakeholders from foreign policy, defence, and cybersecurity to ensure that hybrid activity is managed through a multi-tiered response The task force should routinely meet and consistently re-evaluate whether a given approach is suitable and how it could be adjusted.

6.2.5. Maintain balanced external and domestic messaging

Balance public messaging to reflect the dual strategy of economic engagement with the PRC while maintaining ties with other partners.

6.2.6. Align domestic economic and technological policies with hedging

Ensure domestic policies, especially in technology and trade diversification, are aligned with the external stance of hedging. For example, when engaging with the PRC on infrastructure projects, simultaneously pursue trade diversification agreements with other powers.

6.3. Balancing

Balancing SMPs prioritise deterrence, the strengthening of alliances, and managing tensions to avoid escalations. The suggestion for them is hence to:

6.3.1. Conduct detailed hybrid-threat risk assessments

Assess PRC military and non-military hybrid threats (cyberattacks, disinformation, economic coercion). Identify potential escalatory pathways in response to Chinese hybrid activity and develop concrete red lines with corresponding responses in an anticipatory way.

6.3.2. Strengthen domestic institutions for counter-hybrid resilience

Develop strong domestic institutions in place for countering hybrid threats, including cybersecurity and dedicated intelligence gathering units that are also able to evaluate how certain indirect dependencies on the PRC (e.g., social media) could be introducing less overt vulnerabilities.

6.3.3. Reinforce detection and intelligence capabilities

Develop robust detection capabilities, particularly for disinformation and cyberattacks through the development of public-private partnerships to bolster capabilities (as done in the Ukrainian context). Strengthen counter-hybrid intelligence to identify emerging hybrid threats from the PRC.

6.3.4. Build robust coordination mechanisms

Build coordination mechanisms that enable prompt, cross-sector responses to hybrid threats by ensuring consistent information sharing, strengthening inter-institutional cooperation across cybersecurity, diplomacy, and military sectors, and conducting regular scenario, crisis-simulation exercises, and stress tests.

6.3.5. Communicate strategic positioning clearly

Clearly communicate the SMP's position towards the PRC's hybrid threats, using both public statements and national strategies as well as strategic alliances (e.g., through NATO, EU, or the Quad) as a concrete signal to the PRC.

6.3.6. Ensure strategic coherence with a balancing stance

Ensure that national security strategies, especially in cybersecurity, intelligence, and military resilience, align with a countering stance against China's hybrid tactics. Adjust policies regularly to maintain consistency as hybrid threats evolve.

6.4. Countering

SMPs following a countering strategy are inherently more confrontational, while still taking precautions to avoid inadvertent escalation. The recommendations for them are to:

6.4.1. Conduct a comprehensive vulnerability and confrontation assessment

Assess the risks of direct confrontation with the PRC and its hybrid tactics. Focus on national interests that are most at risk, including national security, critical infrastructure, and political sovereignty.

6.4.2. Strengthen institutional resilience

Review the resilience of institutions in critical areas such as intelligence and cybersecurity to ensure readiness for high-intensity hybrid threats.

6.4.3. Build rapid, high-level attribution and monitoring capabilities

Develop high-level attribution capabilities to ensure rapid identification of hybrid attacks, especially cyberattacks and disinformation. Establish dedicated teams across departments to ensure that hybrid threats are tracked in real-time.

6.4.4. Establish a centralised national security response centre

Establish a centralised national security response centre for counteracting hybrid threats, integrating all relevant sectors to enable a unified and fast response.

6.4.5. Publicly signal deterrence

Deploy diplomatic measures to signal deterrence against PRC hybrid tactics. Develop cyber defence and deterrence frameworks for swift, credible responses.

6.4.6. Ensure cohesive domestic and foreign messaging

Ensure that all domestic communication strategies reinforce the countering stance. Coordinate foreign policy with public domestic measures (e.g., stricter controls on Chinese investments in sensitive sectors).

The measures are summarised in Table 6:

Table 6: Summary of recommendations

Response	Review capabilities, stakes, and position	Build sustained cross-domain awareness	Ensure coherence between internal messaging and external positioning
Bandwagoning	1.1 Identify and strengthen key points of interconnection with the PRC	1.3 Implement mechanisms to monitor and evaluate Chinese economic leverage	1.5 Maintain calibrated public messaging
	1.2 Map and stress-test dependencies	1.4 Create institutional oversight	1.6 Align domestic policy with strategic messaging
Hedging	2.1 Reassess national interests and areas for calibrated engagement	2.3 Build integrated, cross-domain early-warning systems	2.5 Maintain balanced external and domestic messaging
	2.2 Identify tools needed for more effective preparedness	2.4 Establish a national strategic coordination task force	2.6 Align domestic economic and technological policies with hedging
Balancing	3.1 Conduct detailed hybrid-threat risk assessments	3.3 Reinforce detection and intelligence capabilities	3.5 Communicate strategic positioning clearly
	3.2 Strengthen domestic institutions for counter-hybrid resilience	3.4 Build robust coordination mechanisms	3.6 Ensure strategic coherence with a balancing stance
Countering	4.1 Conduct a comprehensive vulnerability and confrontation assessment	4.3 Build rapid, high-level attribution and monitoring capabilities	4.5 Publicly signal deterrence
	4.2 Strengthen institutional resilience	4.4 Establish a centralised national security response centre	4.6 Ensure cohesive domestic and foreign messaging

By ensuring coherence between their internal preparations and external positioning, SMPs reduce opportunities for hybrid actors to exploit policy inconsistencies or institutional fragmentation. This does not fix a country in one posture, but it ensures that any posture is supported by stable and predictable foundations.

Still, SMPs should be weary of the trade-offs each posture also entails.

Hybrid threats are likely to remain a defining feature of the international system as great power competition intensifies. The PRC's hybrid activities, deployed in a synchronised and locally enabled way, will continue to test the resilience, autonomy, and strategic clarity of SMPs in Europe, the Asia-Pacific, and beyond. This report has shown that SMPs are not powerless in the face of these pressures. By understanding their own capabilities, stakes, and position; by building a posture that privileges coherence over ad-hoc reaction; and by learning from others

through dialogue and shared practice, SMPs can develop more effective and sustainable counter-hybrid strategies.

Ultimately, this study does not offer a blueprint for how SMPs must respond. Instead, it provides the key steps necessary before the implementation of responses, so that policy-makers can prepare to respond more deliberately, more coherently, and more strategically to great powers' use of hybrid threats.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl