The Hague Centre
for Strategic Studies

CLARIS

Methodological Notes

HCSS Datalab

Jesse Kommandeur, Maria-Antigone Rumpf, Benedetta Girardi

January 2026

Chinese Latent Activity and Related Interference Scanner (CLARIS)
Methodological Notes

Authors: Jesse Kommandeur, Maria-Antigone Rumpf, Bendetta Girardi

Contributors: Noemie Jacq

Created: November 2025

Cover photo: Canva

This methodological note has been constructed by the HCSS Datalab with the financial contribution of the Taipei Representative Office in the Netherlands. The conclusions and recommendations presented in this report are the result of in-house independent research and development. Responsibility for the content rests with the authors and the authors alone.

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

CLARIS in short

The Chinese Latent Activity and Related Interference Scanner (CLARIS) is an interactive dashboard developed by the HCSS Datalab in cooperation with Strategic Analysts to catalogue and analyse verified instances of Chinese hybrid threat activity since 2015. Based on open-source and independently verifiable reporting, it documents how China employs tactics such as cyber operations, disinformation, economic coercion, lawfare, and paramilitary pressure against Small and Middle Powers (SMPs) in Europe and the Asia Pacific.

CLARIS is designed to provide transparency and a structured overview of Chinese hybrid strategies below the threshold of armed conflict. It does not predict future activity but offers a repository of substantiated incidents that highlight trends over time, variation across countries, and shifts in tactics. The tool is publicly accessible, supporting informed debate and data-driven threat monitoring.

The dashboard is organised into three analytical “lenses.” The Global Lens presents a macro-level view of incidents across countries and regions, the National Lens zooms in on individual states, and the Incident Lens provides detailed case-level insights. Together, they allow users to explore Chinese hybrid activities at different scales, from broad patterns to specific operations.

While CLARIS offers a systematic baseline, it faces limitations. Coverage depends on open sources, attribution is often contested, and the scope is restricted to SMPs in Europe and the Asia Pacific. Users should therefore treat the tool as a conservative but reliable starting point for understanding China’s hybrid threat strategies.

1. Introduction

Great power competition has re-emerged, reshaping global politics and security. The increasing interconnectedness and the emergence of the digital world as a new space of contention have expanded hybrid threat possibilities which great powers have increasingly exploited to achieve their foreign policy goals. These threats create large risks for Small and Middle Powers (SMPs) who are likely to be targeted by a combination of covert and overt methods of destabilisation. With rivalry and contention growing in several disputed and conflictual areas, the international community is faced with challenges that do not fit in with traditional frameworks of conventional conflict anymore.

In this context, China has drawn on longstanding and emergent power instruments, adapting and combining economic, political, military, technological, and cultural strategies to expand its influence while staying below the threshold of open conflict. While avoiding escalation of tensions into conflict is crucial for China, Beijing still uses a combination of multifaced measures below the threshold of conventional warfare, part of a strategy of “unrestricted warfare” employed to achieve its foreign policy objectives. China’s whole-of-society approach to hybrid threats covers a variety of domains, from cyberattacks on public infrastructure to coercive economic measures and political interference o exercise its influence, undermine legitimacy and reshape international norms aligning with its model of global governance and ambitions.

The **Chinese Latent Activity and Related Interference Scanner (CLARIS**) is a dashboard designed to catalogue, visualise, and analyse verified instances of Chinese hybrid threat activities targeting SMPs since 2010. Drawing on open-source reporting and independently verifiable information, CLARIS offers a structured record of incidents across multiple threat domains, enabling policymakers, analysts, and researchers to track and contextualise Chinese hybrid engagement patterns. While hybrid threats remain difficult to quantify, forecast or attribute due to their diverse, asymmetric, and often covert nature, the scanner offers a baseline for systematic analysis, highlighting trends over time and variations across countries.

At its core, CLARIS aims to provide transparency and an integrated overview about Chinese hybrid threat activity targeting SMPs in Europe and the Asia Pacific. Demonstrating commitment to transparent and informed dialogue, CLARIS is made available to the public. This accessibility allows a range of stakeholders to benefit from the insights it offers.

The tool is not designed to predict future hybrid activities or to assess their direct strategic impact, but it provides a repository of verified incidents to support national risk assessments and a strategic analysis of China’s hybrid threats patterns. In doing so, it contributes to a broader effort to bridge the gap between security policy and data-driven threat monitoring in an era where the boundaries of peace, conflict, and competition are increasingly blurred. By allowing a better understanding of these hybrid threats patterns, this tool also provides SMPs with the necessary understanding to develop more tailored and effective policy response to the challenges faced.

The methodological note accompanying the dashboard aims to guide the viewer from the conceptual foundations of hybrid threats to the practical application of the tool.

Section 2 lays out the conceptual framework. It introduces the concept of hybrid threats and provides clear distinctions from other related but distinct terms such as *hybrid warfare*, *grey-zone tactics*, and *asymmetric conflict*. It also introduces China's particular approach to hybrid operations, characterised by a *patient, sub-threshold, and multi-domain* strategy that leverages SMPs vulnerabilities with tailored actions.

In section 3, the note presents typology and dimensions of the model. It introduces the five categories of hybrid activity: Digital warfare, economic statecraft, paramilitary operations, physical destruction and violence, and legal and political activities, explaining their defining characteristics and how they are further divided into subcategories. This section also explains the "target type" classification applied to each incident, distinguishing between threats directed at the public sector, private sector, multi sector, government, general public, infrastructure, academia, and the military.

Section 4 introduces the analytical interface of the Scanner, broken down into three main lenses. The Global Lens offers a macro-level perspective of the dataset through interactive maps and ranked tables, enabling comparisons by region, category, and frequency of threat types. The National Lens profiles individual countries and their exposure to specific hybrid tactics over time, offering contextual maps, regional comparisons, and incident timelines. The Incident Lens allows users to explore the granular details of individual threat incidents, including summaries, sources, classification tags, and links to similar cases.

Section 5 reflects on the methodological limitations. It highlights the main caveats users should keep in mind when interpreting the outputs of the dashboard. The section identifies four core challenges: data completeness, which is constrained by reliance on open-source reporting; source availability and bias, which vary across countries, languages, and domains; attribution difficulties, stemming from the deniable and covert nature of hybrid activities; and scope and representativeness, given the tool's focus on SMPs in Europe and the Asia Pacific.

Overall, CLARIS offers both a high-level overview of China's hybrid activity and a detailed, incident-level view of how SMPs are affected. Whether the reader is interested in systemic patterns, country-specific threats, or domain-level tactics, the structure of the report is intended to support both comprehensive exploration and targeted analysis.

2. Conceptual Foundation

This section lays the groundwork for the analytical framework by clarifying what is meant by *hybrid threats* and how the concept is applied in this study. Because the term is often conflated with related notions such as hybrid warfare, asymmetric warfare, or grey zone activity, definitional clarity is crucial for ensuring comparability across cases. Section 2.1 sets out the project's working definition of hybrid threats, drawing on existing scholarly and policy debates. Section 2.2 distinguishes this definition from closely related concepts to prevent conceptual stretching and misinterpretation. Finally, Section 2.3 zooms in on the Chinese approach to hybrid threats, highlighting the unique features of China's long-term, sub-threshold, and multi-domain strategy, which contrasts with other actors' use of hybrid tools.

2.1 Definition of hybrid threats

Hybrid threats can be understood as the deliberate, coordinated, and often simultaneous use of military and non-military instruments by state or non-state actors to undermine the sovereignty, institutional functioning, or societal cohesion of a targeted state or group.[1] These actions are intentionally designed to remain below the threshold of conventional warfare, enabling perpetrators to pursue strategic objectives without provoking direct military retaliation.[2]

Such threats operate across multiple domains – digital, economic, political, informational, and paramilitary – and typically exploit pre-existing vulnerabilities within a target's systems. Their impact arises not from isolated disruptive acts but from the cumulative pressure generated through adaptive and ambiguous tactics. These may include cyberattacks, disinformation campaigns, economic coercion, political interference, or other destabilising methods that erode trust in institutions, polarise societies, or influence state behaviour.[3]

A central characteristic of hybrid threats is their difficulty of attribution, as actors frequently obscure their involvement or operate through proxies. This ambiguity complicates timely responses, reduces the political and legal costs for aggressors, and allows them to operate with a degree of plausible deniability.[4]

This definition forms the conceptual foundation for the analysis that follows. By focusing on observable actions rather than contested labels, it provides a consistent basis for comparative analysis and long-term monitoring of hybrid strategies across regions and time. The next subsection (2.2) sharpens this foundation by differentiating hybrid threats from neighbouring concepts such as hybrid warfare, asymmetric warfare, and grey zone activity.

2.2 Differentiation

Definitional clarity requires distinguishing *hybrid threats* from related concepts such as hybrid warfare, asymmetric warfare, and grey zone activity, which are often used interchangeably in policy debates and academic literature. While these terms share certain features, their scope and meaning diverge in important ways.

[1] G. Giannopoulos et al., *The Landscape of Hybrid Threats: A Conceptual Model : Public Version* (Publications Office of the European Union, 2021), 6, https://data.europa.eu/doi/10.2760/44985.
[2] 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.
[3] Giannopoulos et al., *The Landscape of Hybrid Threats*, 6.
[4] Sanz-Caballero, 'The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe', 3.

Hybrid warfare implies the active presence of kinetic conflict and falls within the legal parameters of armed conflict as defined under international law (e.g., the Geneva Conventions).[5] The term *warfare* suggests formal combat operations, whereas hybrid threats encompass a broader and more ambiguous spectrum of activities including disinformation, cyberattacks, and economic coercion that generally remain below the threshold of physical confrontation.[6] In this sense, hybrid warfare may be viewed as a subset of the wider hybrid threat spectrum, representing the military implementation of hybrid strategies.[7]

Asymmetric warfare refers to confrontation between uneven actors, typically marked by differences in objectives, capacities, and modes of combat.[8] Hybrid threats may also involve non-state actors, but their strategic logic differs rather than focusing on direct military confrontation, they rely on complexity, ambiguity, and cross-domain convergence to erode stability from within.

The **grey zone** describes the ambiguous operational space between war and peace, which frequently provides the setting in which hybrid threats unfold.[9] Yet, it is not conceptually equivalent. Grey zone activity denotes the environment or condition, while hybrid threats capture a structured set of actions with deliberate strategic intent. Hybrid tactics may be deployed within the grey zone, but they also occur during peacetime, escalate in the run-up to conflict, or complement active hostilities by amplifying kinetic operations.[10]

Taken together, hybrid threats stand out for their cross-domain design, their reliance on ambiguity and plausible deniability, and their capacity to destabilise through non-traditional, multi-dimensional means. This conceptual precision is particularly important when analysing distinct national approaches – such as China's – which combine patience, sub-threshold manoeuvring, and coordinated multi-domain tactics, as discussed in the next subsection.

2.3 The Chinese Approach

China's hybrid threat strategy is characterised by a distinctive patience rooted in its strategic culture and long-term vision. Rather than seeking rapid disruption through overt action, Beijing pursues gradual shifts in global power dynamics.[11] Drawing on Sun Tzu's doctrine of coercion and deception, it seeks to revise the international order from within: actively participating in institutions while simultaneously reshaping norms and rules to align with Chinese interests, all while avoiding open confrontation.[12] This approach consistently operates below the threshold of conventional warfare. Inspired by the doctrine of "unrestricted warfare" and the "Three Warfares" (psychological, media, and legal), China employs tools such as legal coercion, cyber operations, and economic pressure to weaken adversaries

[5] Tarik Solmaz, 'Conventional Warfare versus "Hybrid Threats": An Example of the Either-or Fallacy', *Small Wars Journal by Arizona State University*, 27 April 2022, https://smallwarsjournal.com/2022/04/27/conventional-warfare-versus-hybrid-threats-example-either-or-fallacy/.

[6] Sanz-Caballero, 'The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe', 2.

[7] Anton Dengg and Michael Schurian, 'On the Concept of Hybrid Threats', in *Networked Insecurity: Hybrid Threats in the 21st Century* (Schriftenreihe der Landesverteidigungsakademie, 2016), 36.

[8] Patrick A. Mello, 'Asymmetric Warfare', in *The Blackwell Encyclopedia of Sociology*, 1st edn, ed. George Ritzer (Wiley, 2016), 1, https://doi.org/10.1002/9781405165518.wbeos0773.

[9] 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.

[10] Giannopoulos et al., *The Landscape of Hybrid Threats*, 36.

[11] Bonnie Glaser and Khairulanwar Zaini, *China as a Selective Revisionist Power in the International Order* (Yusof Ishak Institute, 2019), 7, https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/201921-china-as-a-selective-revisionist-power-in-the-international-order/.

[12] Elsa Kania, 'The PLA's Latest Strategic Thinking on the Three Warfares', *China Brief* 16, no. 13 (2016), https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/.

without provoking direct military retaliation. Sub-threshold tactics create attributional ambiguity, delay responses by the international community, and allow strategic gains to be achieved at relatively low risk and cost.[13]

At the same time, China's strategy is inherently multi-domain. Hybrid activities extend across political, economic, digital, informational, and military spheres, with instruments of power deployed in a coordinated and adaptive manner.[14] From leveraging the Belt and Road Initiative as a platform for economic influence to shaping public opinion abroad through information operations, China integrates diverse tools within a single strategic framework. This persistent, coordinated, and adaptive application of hybrid methods makes China's approach especially difficult to counter and underscores its divergence from other actors' hybrid threat strategies.

2.4 The Chinese Targeting

Although China's hybrid threat strategy is global in scope, its effects are particularly pronounced in the context of SMPs. In international relations, SMPs are generally defined not by precise material thresholds, but by their relative position in the global order: they lack the comprehensive capabilities of great powers, yet wield greater influence than microstates or weak states. Their significance stems from both their vulnerabilities and their strategic utility in the broader geopolitical competition.

SMPs are attractive targets for hybrid tactics for several reasons. First, their limited economic, military, and institutional resources often constrain their ability to deter or counter hybrid incursions. This makes them more susceptible to external manipulation through economic dependency, disinformation, cyber intrusions, or coercive diplomacy. Second, SMPs frequently occupy strategically pivotal geographic positions – such as maritime chokepoints, border regions, or resource hubs – that magnify their importance in great power rivalry. Third, SMPs often depend on external trade and security guarantees, producing structural dependencies that can be exploited through calibrated incentives or coercive measures.

For China, engaging with SMPs is central to its long-term hybrid strategy. By cultivating influence over smaller states, Beijing not only secures access to resources and markets, but also fragments rival coalitions and reshapes global governance in its favour. The ability to draw SMPs into China's orbit – whether through economic enticements, political alignment, or narrative support – provides cumulative strategic advantages that reinforce its challenge to the Western-led order.

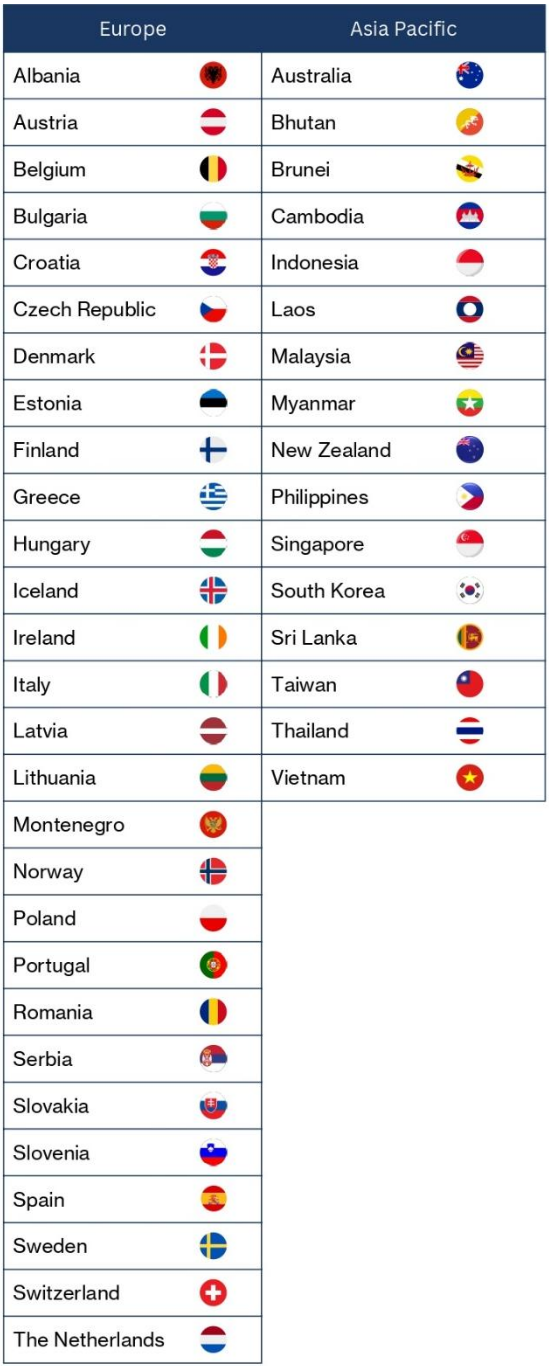
From an analytical perspective, focusing on SMPs highlights both the reach and the limitations of Chinese hybrid threats. On the one hand, SMPs illustrate how hybrid tactics can achieve disproportionate effects against relatively vulnerable targets. On the other, their varied responses – ranging from band wagoning to balancing – reveal the spectrum of agency available to smaller states that do not benefit from extensive capabilities. Studying Chinese targeting of SMPs therefore not only sheds light on Beijing's methods, but also illuminates the broader dynamics of resilience, adaptation, and alignment in an era of intensifying great power competition.

[13] Glaser and Zaini, *China as a Selective Revisionist Power in the International Order*, 7.
[14] Sanz-Caballero, 'The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe', 6.

3. Typology and Dimensions

This section introduces the typology of Chinese hybrid threats and explains the dimensions along which incidents are classified in CLARIS. Building on the literature review, we operationalise hybrid threats into a structured coding framework that allows for systematic comparison across tactics, regions, and targets. The section is organised in three parts. Section one situates the analysis by focusing on SMPs in Europe and the Asia Pacific, section two introduces the typology of threat tactics and their subtypes, and section three focuses on the targets of hybrid threats, comparing across geographies to reveal strategic preferences and vulnerabilities.

3.1 Small and Middle Powers



Europe	Asia Pacific
Albania	Australia
Austria	Bhutan
Belgium	Brunei
Bulgaria	Cambodia
Croatia	Indonesia
Czech Republic	Laos
Denmark	Malaysia
Estonia	Myanmar
Finland	New Zealand
Greece	Philippines
Hungary	Singapore
Iceland	South Korea
Ireland	Sri Lanka
Italy	Taiwan
Latvia	Thailand
Lithuania	Vietnam
Montenegro	
Norway	
Poland	
Portugal	
Romania	
Serbia	
Slovakia	
Slovenia	
Spain	
Sweden	
Switzerland	
The Netherlands	

CLARIS includes a total of 44 SMPs (see Figure 1 - Small and Middle Powers in CLARISFigure 1) across Europe and the Asia Pacific. Countries were selected on the basis of three **inclusion criteria**. First, all included states qualify as SMPs in international relations scholarship, falling below the great power threshold in terms of population, economy, and military capabilities. Second, they hold clear strategic relevance to Chinese hybrid threat strategies, either as documented targets of hybrid activity or as geostrategic actors whose position makes them particularly exposed. Finally, each case offers a sufficient level of data availability, with open-source reporting and expert assessments allowing incidents to be coded in a systematic and longitudinal manner.

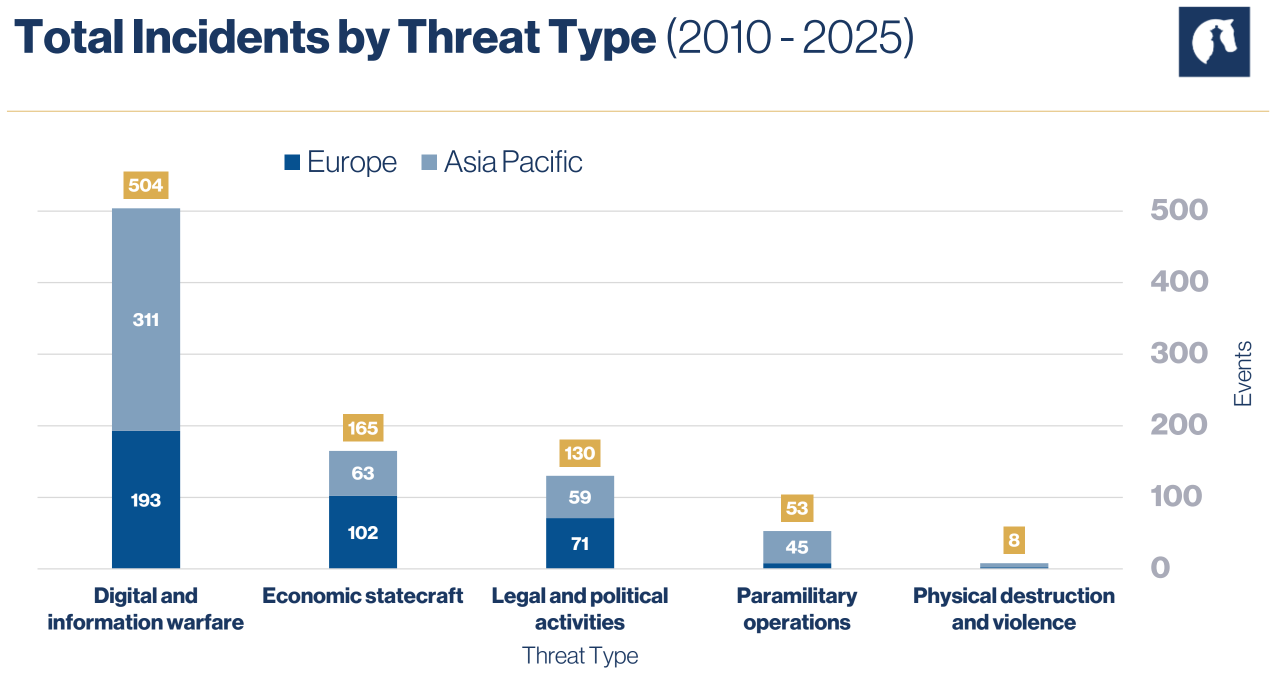
Exclusion criteria consisted of leaving out major or great powers such as the United States, China, Russia, France, Germany, the UK, and India, which fall outside the SMP scope, as well as microstates or countries with negligible Chinese presence and limited exposure to hybrid activity. States for which incident data remain too sparse or unverifiable were also excluded in order to preserve the reliability of outputs.

This approach results in broad regional coverage while reflecting the differential patterns of Chinese hybrid activity. In Europe, 27 states are included. In the Asia Pacific, 17 SMPs are included, reflecting the region's role as the primary focus of China's maritime and territorial strategies as well as its broader competition with the United States. By applying consistent inclusion and exclusion criteria across both regions, the dashboard ensures that the sample captures the states most exposed to Chinese hybrid threats while maintaining methodological rigour and comparability.

3.2 Hybrid Threat Types

Hybrid threats are multidimensional in nature, spanning both conventional and unconventional domains. Drawing directly on the literature review, we adopt a typology that distinguishes between five broad categories of tactics: digital and information warfare, economic and financial coercion, paramilitary operations, physical sabotage and violence, and legal-political manoeuvres.

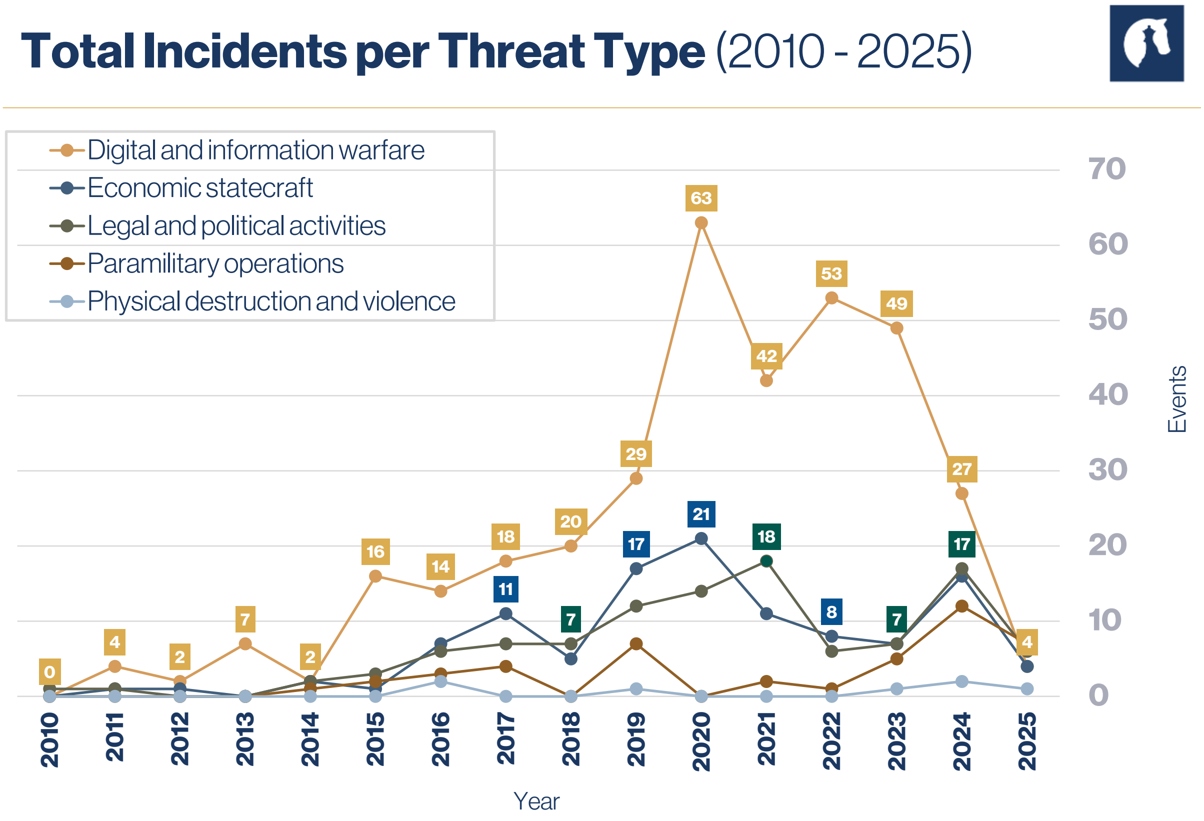
As shown in Figure 2 - Total incidents by Threat type, the dataset confirms the centrality of digital and information warfare to China's hybrid playbook: over 500 incidents fall into this category, making it by far the most prevalent form of activity across both Europe and the Asia Pacific. Economic statecraft and legal-political manoeuvres follow in scale, together accounting for just over 300 incidents, while paramilitary operations and physical sabotage are less frequent but strategically consequential.



Source: China Latent Activity and Related Interference Scanner

Figure 2 - Total incidents by Threat type

The temporal distribution of incidents **Error! Reference source not found.** further illustrates how China's hybrid tactics have evolved since 2010. Digital and information warfare accelerated sharply after 2015, peaking around 2020 with over 60 recorded incidents, coinciding with heightened geopolitical frictions and the COVID-19 pandemic. Economic statecraft and legal-political activities display more cyclical patterns, with spikes during trade disputes and periods of intensified diplomatic confrontation. Paramilitary incidents rise gradually after 2016, reflecting China's increasingly assertive behaviour in the South and East China Seas. While physical sabotage and violence remain relatively rare, their persistence highlights a consistent though low-level willingness to employ disruptive tools alongside informational and economic measures. Taken together, the time-series trends point to a broadening and intensification of hybrid activity, with tactical emphases shifting in line with global crises and regional tensions.



Source: China Latent Activity and Related Interference Scanner

Figure 3- Total Incidents per Threat Type

Each of these categories is further disaggregated into subtypes (Table 1), which specify the mechanisms through which threats manifest in practice – from cyber intrusions, disinformation campaigns, and espionage to debt-trap diplomacy, proxy violence, infrastructure sabotage, and lawfare. This subcategorisation ensures a granular representation of China's hybrid toolkit and allows the dashboard to capture the full breadth of tactics employed across regions.

Table 1: Threat Subcategories with definitions and examples

Category	Subtype	Description	Example
Digital and information warfare	*Cyber operations and attacks*	Malicious activities in cyberspace to compromise, damage, or disrupt information systems.[15]	Hacking of government servers to disrupt communications. *Hacking group Breaches Taiwan Government Network*[16]
	Foreign Interference and Misinformation (FIMI)	Dissemination of false or misleading information (e.g., via bot farms) to influence	Coordinated bot activity amplifying false narratives on social media.

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

[16] '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', EuRepoC: European Repository of Cyber Incidents, 15 November 2022, https://eurepoc.eu/table-view/.

		perceptions, manipulate public opinion, or exploit social vulnerabilities.[17]	*Beijing Disinformation Campaign Targets Taiwan Election*[18]
	Digital Espionage	Use of phishing or malware to gain access to sensitive data; often carried out through proxies or state-sponsored actors.[19]	Malware targeting energy grid systems to steal sensitive operational data. *Huawei Employee Suspected of Data Sharing*[20]
Economic Statecraft	*Economic coercion or dependence*	Manipulation of economic systems (investment restrictions, trade embargoes, punitive tariffs) to enforce political alignment.[21]	Imposing tariffs on imports from a state following political disputes. *Beijing Threatens Economic Retaliation Against Sweden*[22]
	Malign finance	Illicit financial practices that disrupt economies or coerce alignment through hidden influence channels.[23]	Covert donations to influence national elections. *Pro-China Think Tank Launched in Belgrade*[24]
Paramilitary operations	*Military exercises and build-up*	Use of units affiliated with the state but not formally military to exert pressure without open conflict.[25]	Deployment of maritime militias in contested waters. *Navy Flotilla Conducts Drills Near Australia*[26]
	Organised violence (riots, protests, terrorism)	Orchestration or covert support of violent groups (riots, protests, terrorism) to destabilise societies.[27]	Covert funding of militant groups in border regions. *Water Cannons used in territorial dispute*[28]
Physical sabotage & violence	*Arson/explosions*	Setting fires or detonating explosives to cause destruction, fear, or disruption, often targeting infrastructure.	No records in dataset

[17] Aldo Podavini et al., *Understanding Citizens' Vulnerability to Disinformation and Data-Driven Propaganda: Case Study : The 2018 Italian General Election* (Publications Office of the European Union, 2019), 7–8, https://data.europa.eu/doi/10.2760/919835.

[18] 'Analysis: "Fake News" Fears Grip Taiwan Ahead of Local Polls – BBC Monitoring', accessed 28 August 2025, https://monitoring.bbc.co.uk/product/c200fqlq.

[19] *What Is Cyber Espionage? | Cyble*, Cybersecurity, 18 October 2024, https://cyble.com/knowledge-hub/what-is-cyber-espionage/.

[20] 'Huawei Employees in Czech Republic Report Personal Client Information to Chinese Embassy', Alliance For Securing Democracy, accessed 28 August 2025, https://securingdemocracy.gmfus.org/incident/huawei-employees-in-czech-republic-report-personal-client-information-to-chinese-embassy/.

[21] Tinatin Khidasheli, *Hybrid Threats and Resilience: Safeguarding Democratic Values in a Connected World* (Friedrich Naumann Foundation Caucasus, 2024), 10.

[22] 'China Tries to Put Sweden on Ice', accessed 28 August 2025, https://thediplomat.com/2019/12/china-tries-to-put-sweden-on-ice/.

[23] Aleksi Aho et al., *Hybrid Threats in the Financial System*, no. 8 (European Center of Excellence for Countering Hybrid Threats, n.d.), 14–17, accessed 22 August 2025, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-8-hybrid-threats-in-the-financial-system/.

[24] 'CEFC Help Vuk Jeremic Establish a Pro-Beijing Think-Tank in Serbia', Alliance For Securing Democracy, accessed 28 August 2025, https://securingdemocracy.gmfus.org/incident/cefc-help-vuk-jeremic-establish-a-pro-beijing-think-tank-in-serbia/.

[25] 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.

[26] Victoria Kim Sydney and Australia, 'Chinese Warships Circle Australia and Leave It Feeling "Near-Naked"', World, *The New York Times*, 12 March 2025, https://www.nytimes.com/2025/03/12/world/australia/china-warships-australia-aukus.html.

[27] Avinash Paliwal and Paul Staniland, 'Strategy, Secrecy, and External Support for Insurgent Groups', *International Studies Quarterly* 67, no. 1 (2022): 1–2, https://doi.org/10.1093/isq/sqad001.

[28] Jim Gomez, *Filipino Activists and Fishermen Sail in 100-Boat Flotilla to Disputed Shoal Guarded by China | AP News*, 15 May 2024, https://web.archive.org/web/20240515042132/https:/apnews.com/article/south-china-sea-scarborough-shoal-philippines-991e0ecee638f917e30b4947ee8c91ca.

	Assassination (attempt)	Premeditated killing of individuals for strategic or ideological purposes, aiming to intimidate or destabilise.[29]	Targeted killing of dissidents abroad. *Allegations of Political espionage uncovered*[30]
	Sabotage of infrastructure	Intentional damaging or destruction of critical infrastructure, undermining stability and sovereignty.[31]	Cyber-physical sabotage of rail transport systems. *Suspected sabotage of Baltic connector Pipeline*[32]
Legal & political manoeuvres	*Political undermining*	Actions including covert financial support, corruption, or orchestrated campaigns to influence political processes.[33]	Covert funding of political parties to shift domestic policy. *Hackers target UN Security Council Members*[34]
	Lawfare	Exploiting international legal mechanisms or ambiguities to obstruct responses, create narratives, or weaken opponents.[35]	Filing legal claims to delay sanctions enforcement. *Hong Kong suspends extradition agreements*[36]
	Espionage	The conscious, deceitful collection of information, ordered by a government hostile to or suspicious of those the information concerns.[37]	Infiltrating ranks and collecting information *Espionage Network Uncovered, Suspect arrested*[38]

To capture this complexity, each incident in CLARIS is coded using a structured metadata profile (actor, target, sector, timing, intended effect). This framework enables both horizontal comparisons (e.g., which tactics dominate globally) and vertical drilldowns (e.g., how cyber and disinformation campaigns evolve when deployed against small versus middle powers).

3.3 Target Types

Understanding who is targeted is as important as what tactic is used. Hybrid operations seek leverage by striking different decision-nodes in a society: governments (policy authority), firms and infrastructure (economic lifelines), publics (opinion and cohesion), and knowledge or security communities (agenda-setting and deterrence). This division allows to look at a broad spectrum of targets, while highlighting

[29] Simon Frankel Pratt, 'Crossing off Names: The Logic of Military Assassination', *Small Wars & Insurgencies* 26, no. 1 (2015): 3, https://doi.org/10.1080/09592318.2014.959769.

[30] *Australia Investigates Alleged Chinese Plot to Install Spy MP*, November 2019, https://www.bbc.com/news/world-australia-50541082.

[31] Muntazar Mehdi et al., 'Hybrid Warfare: Geopolitics, Sabotage, and Subversive Activities in Baluchistan', *The Dialogue* 16, no. 4 (2021): 3.

[32] Claudia Chiappa and Pierre Emmanuel Ngendakumana, '"Everything Indicates" Chinese Ship Damaged Baltic Pipeline on Purpose, Finland Says', POLITICO, 1 December 2023, https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/.

[33] Khidasheli, *Hybrid Threats and Resilience: Safeguarding Democratic Values in a Connected World*, 10.

[34] 'Significant Cyber Incidents', Center for Strategic and International Studies, accessed 5 September 2025, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[35] Douglas Guilfoyle, 'The Rule of Law and Maritime Security: Understanding Lawfare in the South China Sea.', *International Affairs* 95, no. 5 (2019): 1010, 138865248, https://doi.org/10.1093/ia/iiz141.

[36] 'China Says Hong Kong Suspends Extradition Agreement with New Zealand', World, *Reuters*, 4 August 2020, https://www.reuters.com/article/world/china-says-hong-kong-suspends-extradition-agreement-with-new-zealand-idUSKBN24Z0RZ/.

[37] Matteo Tondini, 'Espionage and International Law in the Age of Permanent Competition', *Military Law and Law of War Review* 57, no. 1 (2018): 25.

[38] Cliff Harvey Venzon, 'Philippines Probing Network of Hundreds of Alleged Chinese Spies', *Bloomberg.Com*, 7 March 2025, https://www.bloomberg.com/news/articles/2025-03-07/philippines-probing-network-of-hundreds-of-alleged-chinese-spies.

how hybrid threats can focus on different societal segments. It not only distinguishes between private and public spheres but also between civilian and military dimension, underlining the multifaceted nature of hybrid threats' application. Disaggregating incidents by target type helps explain effect pathways (e.g., policy change vs. market signalling vs. intimidation) and informs resilience design (which ministries, sectors, or networks need what kind of protection). It also reduces attribution bias: the same tactic – say, a cyber intrusion – implies different risks if aimed at a grid operator, a ministry, or a university.

Table 2- Target types with definitions and examples

Category	Description	Example
Government	Central, regional, or local state bodies; independent agencies and regulators. Actions intended to shape policy, decision-making, or state capacity.	Phishing against a foreign ministry; pressure on regulators to approve a vendor. *Sustained Cyberespionage Campaign Targets Governments*[39]
Private Sector	Firms and industry associations, including media companies and platforms. Focus on market access, supply chains, or corporate speech.	Coercive boycotts or punitive customs checks after a policy dispute. *Hacker exploits NSA tools for attacks*[40]
Public Sector	State-owned enterprises, public service providers, and entities delivering essential services (e.g., health, education, utilities). Targeted to undermine state capacity, service delivery, or public trust.	Cyber intrusion into a national health system; interference in public broadcasting services. *Bots amplify disinformation in Italy*[41]
Multi-Sector	Coordinated activity that simultaneously targets ≥2 categories (e.g., government + private sector + public). Use when segmentation is not analytically meaningful.	Disinformation plus tariff threats during an investment approval fight. *COSCO expands control over Piraeus Port*[42]
General Public	Mass audiences, civic groups, diaspora communities. Effects on perceptions, cohesion, and turnout.	Bot-amplified false narratives during an election campaign. *Beijing influences Vietnamese Media Narratives*[43]
Infrastructure	Critical services and operators (energy, telecoms, ports, rail, cables, satellites). Emphasis on service disruption or leverage.	Interference with a landing station; pressure on a 5G rollout. *BH Telecomm upgrades 4G network with Huawei*[44]

[39] Phil Muncaster, 'Chinese APT FunnyDream Runs Riot in Southeast Asia', *Infosecurity Magazine*, 18 November 2020, https://www.infosecurity-magazine.com/news/chinese-apt-funnydream-runs-riot/.

[40] 'Chinese Intelligence Repurposed NSA Tools to Attack Private Companies | CFR Interactives', Council on Foreign Relations, May 2019, https://www.cfr.org/cyber-operations/chinese-intelligence-repurposed-nsa-tools-attack-private-companies.

[41] 'Chinese State Narratives on Medical Shipments to Italy Promoted Online via Inauthentic Means', *Alliance For Securing Democracy*, n.d., accessed 28 August 2025, https://securingdemocracy.gmfus.org/incident/chinese-state-narratives-on-medical-shipments-to-italy-promoted-online-via-inauthentic-means/.

[42] Paul Antonopoulos, 'Growing Concerns Around Chinese Investments in European Seaports, Especially Piraeus -', *Greek City Times*, 31 August 2024, https://greekcitytimes.com/2024/08/31/concerns-chinese-investment-piraeus/.

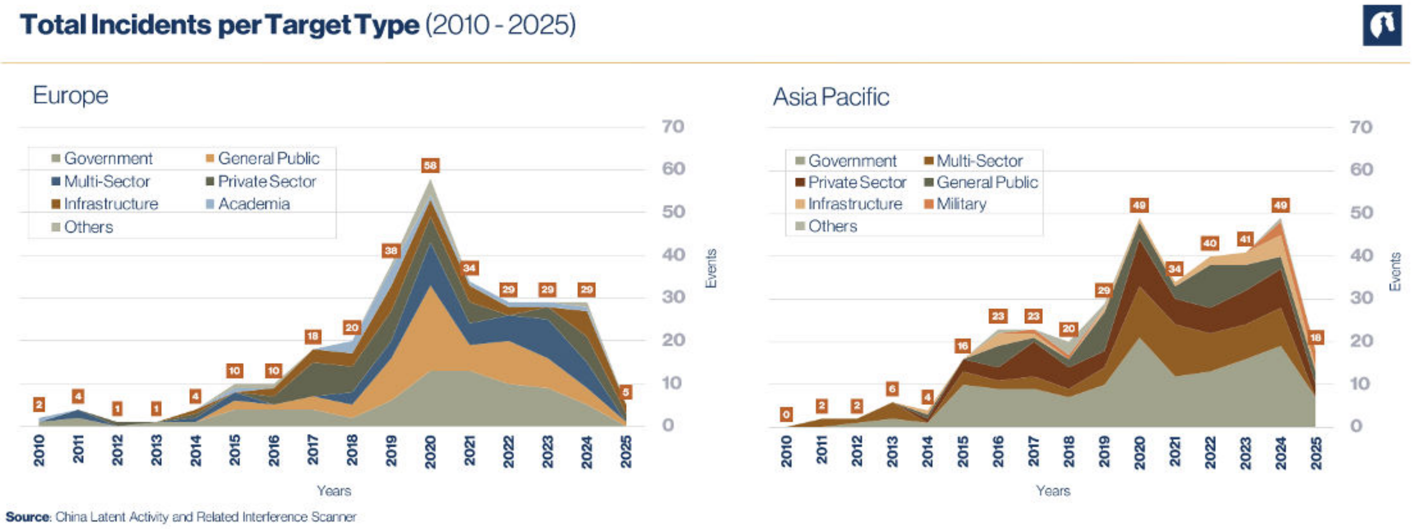
[43] Ryan Loomis and Heidi Holz, *China's Efforts to Shape the Information Environment in Vietnam* (CNA, 2020).

[44] 'BH Telecom Signs 4G Network Upgrade Contract with Huawei', Telecompaper, November 2024, https://www.telecompaper.com/news/bh-telecom-signs-4g-network-upgrade-contract-with-huawei--1520436.

Academia	Universities, think-tanks, and research labs; knowledge capture and agenda-setting.	Funding front groups to influence China-related curricula. *Confucius Institute influence exposed.*[45]
Military	Armed forces and defence institutions short of overt interstate conflict; signalling and coercion.	Targeting a defence ministry network; harassment of patrol aircraft. *Coercive control in disputed waters*[46]

The stacked charts in **Error! Reference source not found.** show how the types of targets have changed since 2010. In Europe (left), incidents begin to rise sharply around 2016 and peak between 2019 and 2021. Most of the surge targeted governments and the public, with multi-group attacks increasing during political debates, such as over investment rules or telecoms. Universities and research institutes are less frequent targets but still appear regularly, reflecting China's efforts to influence knowledge production and public debate. After 2021, the numbers dip but remain higher than before 2018, showing that this activity has become a lasting pattern rather than a one-off spike.

In the Asia Pacific (right), the growth is more gradual, with more focus on governments and the private sector, reflecting regional disputes over territory and trade. Attacks against the military start to appear after 2016 and rise around times of maritime stand-offs. Both regions also show a rise in 2024 in incidents that combine several targets at once, suggesting a shift towards more layered pressure strategies.


Total Incidents per Target Type (2010 - 2025)

Europe

Asia Pacific

Source: China Latent Activity and Related Interference Scanner

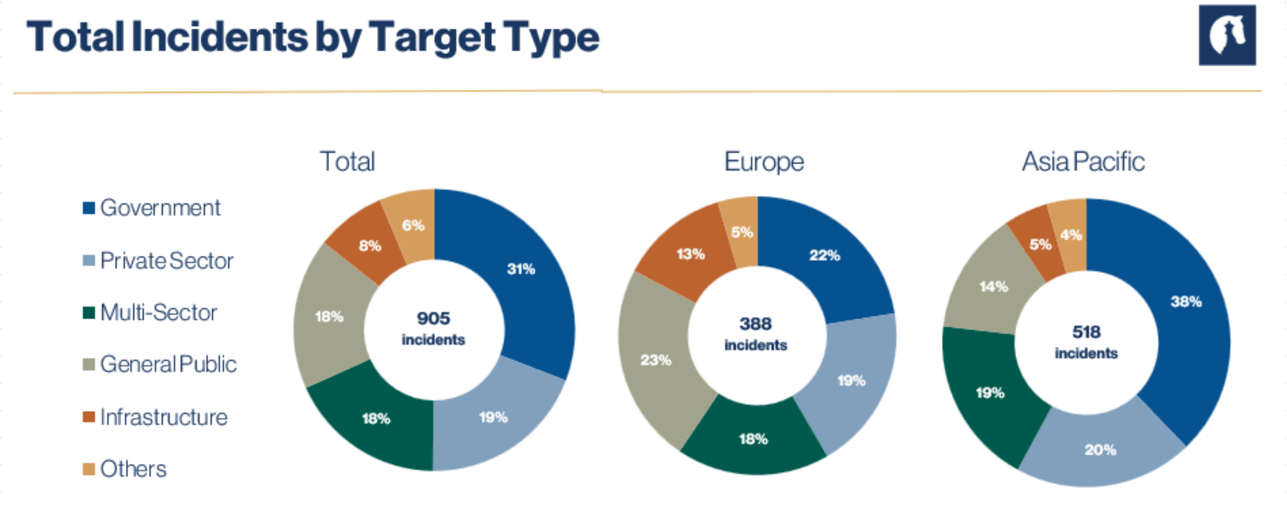
Figure 4 - Number of Incidents per Target Type in Europe (left) and Asia Pacific (right)

The donut charts in Figure 5 show the total number of incidents by target type: 920 in total, with 402 in Europe and 518 in Asia Pacific. Looking at the global picture, governments are the most common target (31%), followed by the private sector (19%), multi-sector incidents that hit several groups at once (18%),

[45] 'Co-Founder of Confucius Institute in Budapest Admits Chinese Officials Influence Decision-Making', Alliance For Securing Democracy, 2020, https://securingdemocracy.gmfus.org/incident/co-founder-of-confucius-institute-in-budapest-admits-chinese-officials-influence-decision-making/.

[46] 'PRC Structures Are Sign of Sovereignty Push against South Korea, Analysts Say', *Indo-Pacific Defense FORUM*, n.d., accessed 28 August 2025, https://ipdefenseforum.com/2025/01/prc-structures-are-sign-of-sovereignty-push-against-south-korea-analysts-say/.

and the general public (18%). Attacks on infrastructure and other groups are less frequent but still present. In Europe (, the picture is more spread out, with multi-sector incidents making up a larger share, showing how European states are often pressured through a mix of government, corporate, and public channels. In the Asia Pacific, the focus is clearer: governments dominate (38%), with the private sector and multi-sector also significant.



Source: China Latent Activity and Related Interference Scanner

Figure 5 - Number of Incidents per Target Type in Total (right), Europe (middle) and Asia Pacific (right)

4. Analytical Lens

This section introduces the three analytical lenses through which CLARIS enables a systematic exploration of Chinese hybrid threat activity. Each lens represents a different scale of analysis, allowing users to move from global patterns to national contexts and individual incidents. Section 4.1 presents the Global Lens, which maps the worldwide distribution of verified incidents, highlights regional concentrations, and ranks countries by frequency and type of threat. Section 4.2 introduces the National Lens, which zooms in on individual states, detailing the most recurrent targets, tactics, and temporal dynamics of hybrid activity. Section 4.3 focuses on the Incident Lens, providing the most granular level of analysis through detailed case files, contextual information, and cross-references to related events.

4.1 Global Lens

The global lens provides an overview of China's most frequent hybrid threat activity from January 2010 until 2025. CLARIS draws on an HCSS dataset of verified incident representing how China's hybrid threats are distributed across different SMPs that has been constructed between January and June 2025. On this page, the map allows for a global or regional (Europe or Asia Pacific) understanding of China's main targets where the number of incidents is reflected. The viewer also has the possibility to select the type of threat organised in five categories and the target as described in chapter 3. The interactive map also allows the viewer to directly access a detailed record of incidents by country and selected threat or target category by clicking on the map.

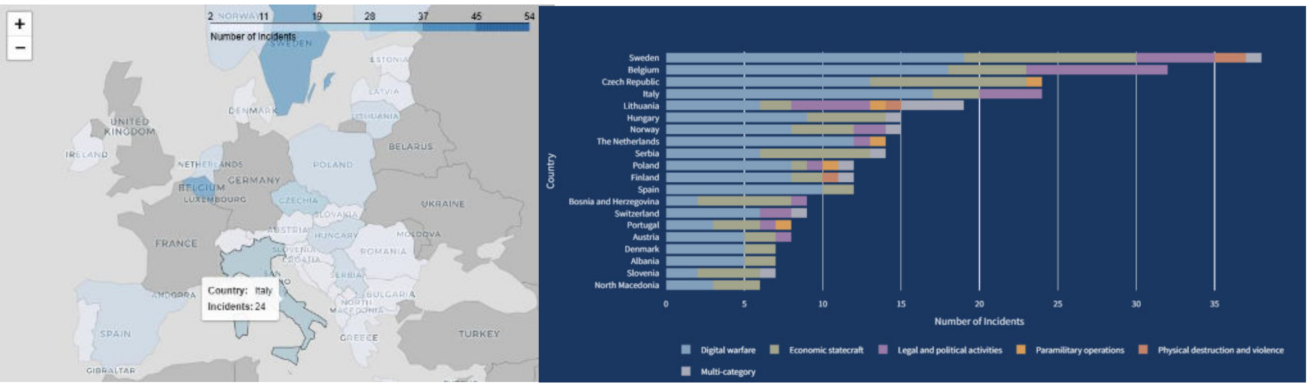


Figure 6 - Geographical (left) and Categorical (right) representation of events in CLARIS

The Global Lens also includes a table ranking countries based on the number of recorded verified incidents and the distribution of threat category associated. This table provides a clear picture of China's most frequent targets, as well as its most recurrent mode of action. The table for example allows users to track the proportion of all five threat types in different SMPs, displaying trends of China's hybrid warfare activities and track similarities and differences across countries, regions and types of targets. This table also allows the viewer a direct access to the country's National Lens page filtering for threat categories and target type.

4.2 National Lens

The National Lens page is designed to provide more detailed information on recorded incidents in each specific country, offering analysis of the most recurrent target sector and the distribution of different threat categories, informing on China's hybrid threat strategy in the specific country. The viewer also has the possibility to filter the National Lens analysis by threat category and target type.

The features of this page allows the user to observe the distribution of subcategories incidents representing the total number of recorded incidents in the country. The bar chart then ranks incidents from the most recurrent subcategory to the least recurrent. The page also provides a contextual map allowing the viewer to situate the intensity and scale of China's hybrid threat strategy in the specific country and for the selected threat type/target type by comparing the amount of selected recorded incidents with other SMPs.

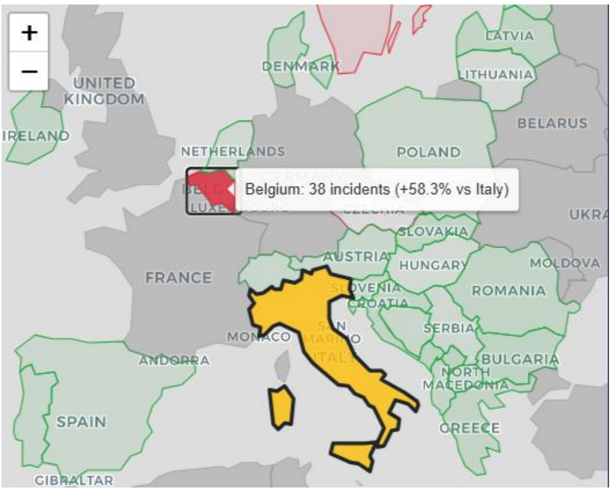
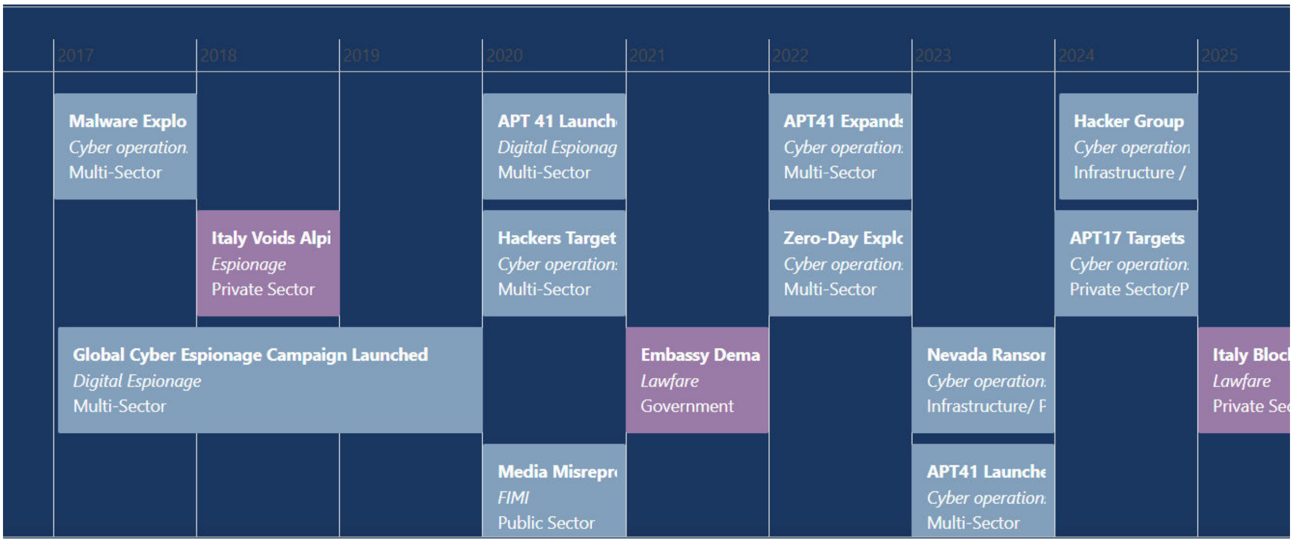


Figure 7 - Geographical incident Comparison in CLARIS

At the bottom of the national page, a panel lays out every recorded incident in a given country as a single timeline, so users can see how different hybrid tactics unfolded over time. Each bar represents an event or campaign; its length shows duration, and its colour matching the sub-category legend. Hover for quick details or click a bar to open the full case file – including sources, sectoral impact, and links to related incidents. Use the category and target-type filters above to refine what appears on the timeline.



Malware Explo
Cyber operation.
Multi-Sector

Italy Voids Alpi
Espionage
Private Sector

Global Cyber Espionage Campaign Launched
Digital Espionage
Multi-Sector

APT 41 Launch
Digital Espionag
Multi-Sector

Hackers Target
Cyber operation:
Multi-Sector

Media Misrepr
FIMI
Public Sector

Embassy Dema
Lawfare
Government

APT41 Expands
Cyber operation.
Multi-Sector

Zero-Day Explo
Cyber operation.
Multi-Sector

Nevada Ransor
Cyber operation.
Infrastructure/ F

APT41 Launche
Cyber operation.
Multi-Sector

Hacker Group
Cyber operation
Infrastructure /

APT17 Targets
Cyber operation.
Private Sector/P

Italy Bloc
Lawfare
Private Se

Figure 8 - - Temporal Incident Timeline in CLARIS

4.3 Incident Lens

The Incident Lens provides the most detailed view in CLARIS, focusing on individual recorded cases of Chinese hybrid activity. Each incident page contains a summary of what happened, including the main tactic used, the target, timing, and intended effect, along with the original sources. Users can quickly understand the context and relevance of a case and then dive deeper into the specifics.

At the top of the page, incidents are tagged by threat category (e.g., digital warfare, economic coercion) and target type (e.g., government, private sector, multi-sector), making it easy to see how the case fits within the broader typology. The details panel provides metadata such as the country affected, the timeframe of the operation, and direct links to the first available sources. The summary panel highlights the narrative of the incident – what happened, who was involved, and what strategic objectives may have been pursued.

Below this, the '*More Like This'* recommendation system allows users to explore connected cases. Recommendations are divided into two streams: the *Regional Context,* which highlights incidents in the same country or neighbouring states, helping to situate the case within its immediate geopolitical environment.[47] *Global Parallels,* which identifies similar incidents elsewhere in the world, showing how comparable tactics or target types have been deployed in different regions.[48] Together, these features ensure that the Incident Lens is not only a repository of cases but also a gateway for comparative analysis. By following links to related incidents, users can trace tactical patterns across borders, compare how different SMPs have been targeted, and build a richer picture of China's hybrid threat strategies over time.

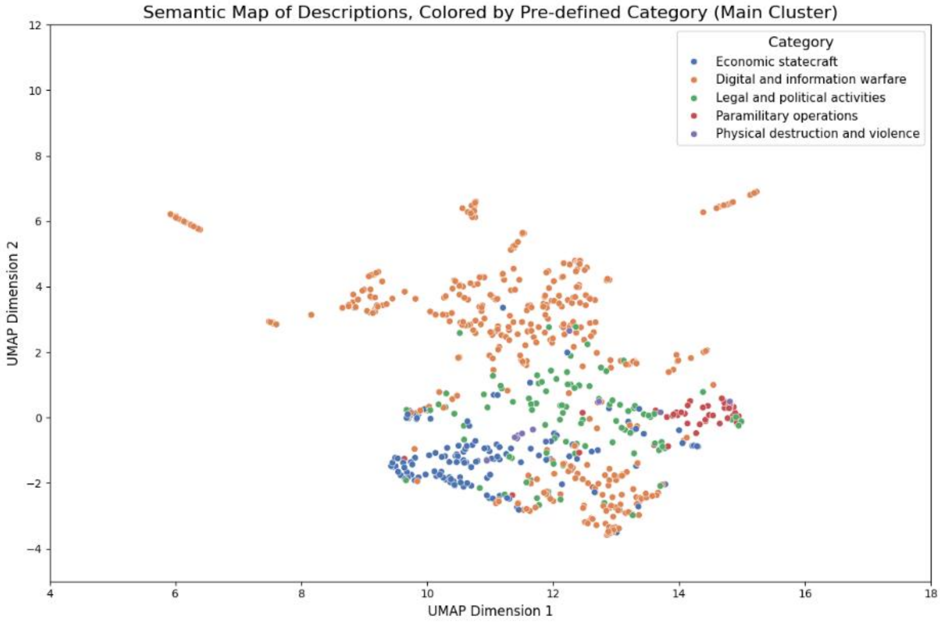


Figure 9 - Scatter Plot with Semantic Clustering of Incident Descriptions, Separated by Category

Figure 9 reflects an exploratory analysis which investigated the semantic clustering of the descriptions of incidents, taking a closer look at the relationship between the language found in the sources and the five categories of threat types. It shows that the predetermined categories do have semantic relationships based on the language used in their descriptions, but they are clustered with a lot of overlap between categories, reflecting the similarity in the language used across the database. Certain categories are more separable than others, for instance *Paramilitary operations* in red forms a tight cluster, meanwhile *Digital and information warfare* is much more spread out, meaning the language used is less distinct. in the scatter plot in Figure 9. The points were coloured according to their pre-defined category, not based on identified clusters. This overlay reveals how categories are distributed across the semantic space. The density heatmap in Figure 10 also shows the central points of the clusters, and the high overlap of the categories

[47] These recommendations are generated through a rules-based weighting system that prioritizes geographic similarity. Incidents In the same category receive a high base score of +100, while those in strategically linked countries are weighted +50. Additional weights are added based on Threat or Target types, maximally +30, alongside marginal weights for recency.
[48] These recommendations use the same scoring framework, but exclude those cases captured In the Regional Context, and are therefore only ranked by Threat Type subcategory and Target Type, which occur in different geographic regions.

- To analyse the incident descriptions, each text was first converted into a numerical format that captures its meaning. This made it possible to compare descriptions based on their semantic similarity.
- Because the data lives in many dimensions, we used a method to project it down into two dimensions. This makes the relationships between incidents easier to see in a visual map, where the distance between points shows how similar they are.
- The results are visualized in scatter plots and density maps across these two dimensions. The distance between dots represents how similar the language used in the *Descriptions* is.
- The clusters were then identified using the 5 existing Threat Type labels. These visualizations reveal both the

Both Figure 9 and Figure 10 reveal a difference between the way the incidents are described in the sources and the threat type category they are placed in. Some categories, like *Economic statecraft* and *Paramilitary operations* are very consistent and showed strong semantic cohesion. The language used in their descriptions is closely related, which is why they appear as tight groups in the graphics. In contrast, the category *Digital and information warfare* is more scattered, as the descriptions for it use a wider range of language, and is used to classify a broad range of thematically distinct incidents.

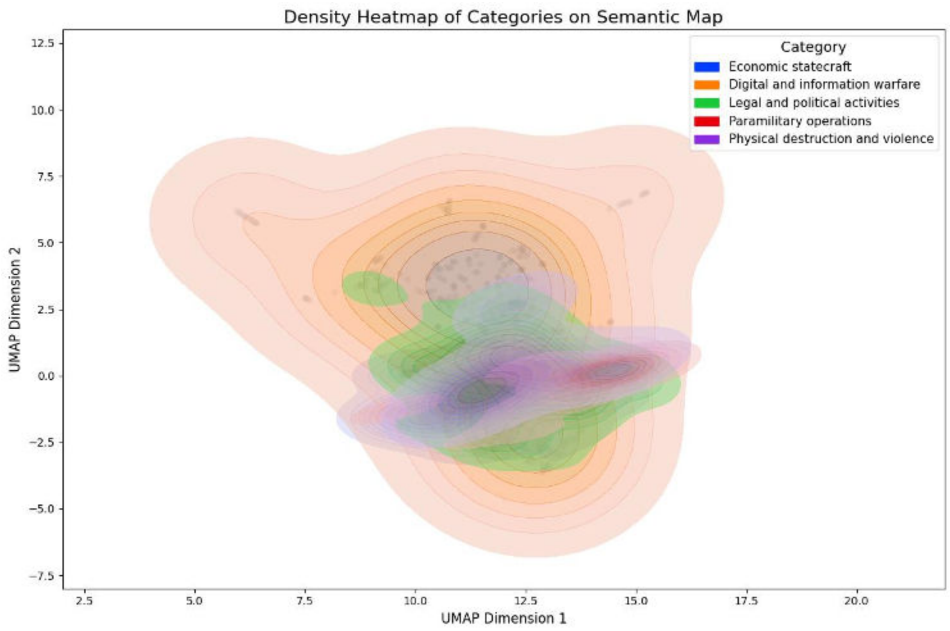


Figure 10 - Heatmap with Semantic Clustering of Incident Descriptions, Separated by Category

Table 3 confirms this. After computingentropy scores, which measures how cohesive or fragmented the language is. D*igital and information warfare* has a score of nearly 1, which is considered highly fragmented. Meanwhile the tighter clusters with lower scores are more cohesive. This means the mathematical representation of language similarity of the sources is much more coherent in categories with low entropy scores, while the fragmented ones are broader labels and relate to a wider range of language.

Table 3 - Entropy scores per Category Indicating cohesion and fragmentation

Category	**Normalised Entropy**	**Interpretation**
Digital and information warfare	0.925	Extremely fragmented
Legal and political activities	0.576	Moderately fragmented
Physical destruction and violence	0.397	Cohesive
Paramilitary operations	0.307	Cohesive
Economic statecraft	0.306	Cohesive

5. Limitations

As with any data-driven framework designed to capture complex and covert geopolitical phenomena, CLARIS faces important limitations. These stem from the availability and reliability of source material, the challenges of attribution, the simplifications inherent in coding multi-dimensional activity, and the representativeness of the dataset itself. This section outlines the key methodological caveats that users should bear in mind when interpreting results across the global, national, and incident lenses. Section 5.1 reflects on data completeness and open-source dependency, Section 5.2 addresses source bias, Section 5.3 highlights the challenges of attribution, and Section 5.4 discusses issues of scope and representativeness.

5.1 Data Completeness

As with all approaches to representing the complexity of the social world, creating a single composite indicator to represent a set of concepts as broad as “geopolitical stability”, “geopolitical risk”, and “geopolitical volatility” has significant drawbacks in addition to advantages. The indicator may conceal extreme values in individual measures through the “averaging out” effect of combining several indicators. For example, the amalgamating of even two indicators into a single measure can assign a situation in which both indicators are broadly average with the same score as a situation in which one is at an extremely above average and the other an extremely below average level. As such, as much attention should be paid to the individual components as the domain level and overall index aggregations when assessing this data.

For users, this implies that CLARIS should be interpreted as a conservative baseline rather than a comprehensive record. The number of incidents recorded does not necessarily reflect the true intensity of hybrid activity in a given country or sector, but rather the portion of that activity that has been reported and validated. Analysts and policymakers should therefore use CLARIS to understand patterns and comparative trends, while recognising that the absolute scale of activity is likely underreported.

5.2 Source Availability Bias

The quality and volume of incident reporting vary significantly across regions, sectors, and time periods. Media ecosystems differ in their ability to identify and report on hybrid threats, while restrictive information environments may suppress disclosure altogether. In addition, language barriers and uneven access to local sources create structural biases: incidents in countries with strong investigative journalism and English-language reporting are more likely to be captured than those in smaller or less open states.

The result is a dataset that may overrepresent certain geographies or threat categories while underrepresenting others. Users should therefore avoid drawing conclusions solely from raw counts of incidents and instead consider how structural reporting differences may shape what is visible. For comparative analysis, this means treating CLARIS outputs as indicative of relative exposure trends, not as a definitive measure of which states or sectors are “most targeted.”

5.3 Attribution Challenges

Hybrid threats are deliberately designed to blur responsibility. The use of proxies, covert financing, or deniable digital operations complicates the task of attributing incidents to China with certainty. CLARIS includes only cases where attribution meets a threshold of independent verification, which helps maintain analytical credibility but also excludes many suspected activities that lack sufficient evidence. This conservative coding approach limits false positives but risks overlooking relevant grey-zone behaviour.

For users, this creates a trade-off: the dataset is robust in terms of reliability but incomplete in scope. Incidents included in CLARIS can be treated with a high degree of confidence, yet the absence of an incident in the database should not be read as proof that no Chinese involvement occurred. Analysts should therefore treat CLARIS as a tool for identifying substantiated trends rather than for providing forensic attribution on its own.

5.4 Scope and Representativeness

The scope of CLARIS is deliberately restricted to SMPs in Europe and the Asia Pacific. This reflects both the strategic relevance of these states and the practical requirement of data availability. However, it also means that the tool omits large swathes of global Chinese activity, particularly in Africa, Latin America, and the Middle East, where Beijing also deploys hybrid tactics. Similarly, great powers such as the United States, Russia, and India are excluded from the dataset by design.

This restriction limits the representativeness of CLARIS. While the included sample provides valuable insights into Chinese strategies towards SMPs, it does not offer a fully global picture. Users should therefore be careful not to overgeneralise findings from the dataset to all Chinese foreign policy behaviour. Instead, CLARIS is best understood as a targeted analytical instrument, highlighting how hybrid threats manifest against states that are strategically significant yet structurally vulnerable.

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