*Article*

| 2026 | Vol. 10 | No. 1 | e53184 |

SOCIETY REGISTER

# Partnerships without polycentricity? Cybersecurity governance in the Indo-Pacific

Isti Marta Sukma[1] ✉

[1] University of Warsaw, Poland (ORCID: 0000-0003-1136-2181)

**ABSTRACT:** Cybersecurity governance in the Indo-Pacific increasingly relies on both public–private partnerships (PPPs) and polycentric governance arrangements, yet the relationship between these two frameworks remains empirically under-examined. Policy discourse and scholarship frequently conflate PPPs with polycentricity, obscuring their distinct governance functions. This study employs comparative qualitative content analysis of national cybersecurity strategy documents from Australia, Japan, and Singapore (2015–2025), supplemented by regional and geopolitical reference documents. Using a theory-driven codebook with 22 codes across six thematic clusters, 573 text segments were systematically coded in Taguette and analyzed through within-case interpretation and cross-case comparison. The analysis demonstrates that PPPs function primarily as operational mechanisms for information sharing, incident response, and co-investment within state-led frameworks. By contrast, polycentric governance features such as overlapping jurisdictions, multistakeholder involvement, and decentralized decision-making emerge independently through international cooperation, regional initiatives, and multi-actor regulatory platforms. The three cases reveal distinct governance configurations: Japan's technocratic polycentricity, Australia's resilience-oriented model, and Singapore's regionally projected governance, all positioned between U.S. multistakeholder polycentricity and China's centralized framework. This article provides the first systematic empirical comparison disentangling PPPs from polycentric governance in Indo-Pacific cybersecurity strategies, offering a more precise analytical framework for comparative governance research.

**KEYWORDS:** polycentric governance | public–private partnerships | cybersecurity | Indo-Pacific | comparative policy analysis | qualitative content analysis | digital governance

## 1. INTRODUCTION

Cybersecurity governance presents a fundamental challenge for states navigating digital interdependence and geopolitical rivalry. As critical infrastructure, economic systems, and military capabilities become increasingly digitized, governments confront threats that are transnational in scope, technically complex, and resistant to unilateral solutions. In this context, two governance frameworks have gained prominence: public–private partnerships (PPPs), through which governments engage private actors in securing shared infrastructure, and polycentric governance, which distributes authority across multiple autonomous but interacting decision-making centers (Ostrom, 2005; McGinnis & Ostrom, 2011). Both frameworks are widely



✉ i.sukma@uw.edu.pl

https://doi.org/10.14746/sr.53184

invoked in cybersecurity policy, yet their relationship remains poorly understood.

In policy discourse and parts of the academic literature, PPPs are frequently treated as manifestations of polycentric governance, as if establishing partnerships between public and private actors automatically produces the distributed, overlapping authority structures that polycentricity describes (Shackelford, 2012). This conflation is analytically problematic. PPPs are fundamentally mechanisms of operational collaboration: they enable information sharing, facilitate joint incident response, and integrate private-sector expertise into state-led policy processes (Carr, 2016; European Union Agency for Cybersecurity [ENISA], 2020). Polycentric governance, by contrast, describes a structural condition in which multiple decision-making centers possess genuine authority to establish and enforce rules within overlapping governance domains (Ostrom, 1991; Carlisle & Gruby, 2019). PPPs may contribute to polycentricity, but the two concepts are not interchangeable.

This distinction has both theoretical and practical significance. Theoretically, conflating PPPs with polycentricity inflates the scope of the polycentric governance concept and obscures the specific conditions under which distributed authority emerges. Practically, assuming that PPPs deliver polycentric governance may lead policymakers to overestimate the structural resilience of their cybersecurity architectures, neglecting the institutional mechanisms, from overlapping mandates, multi-actor regulatory platforms, internationalized decision-making, all that genuine polycentricity requires.

This article addresses this gap through a comparative analysis of national cybersecurity strategies in three Indo-Pacific states: Australia, Japan, and Singapore. These cases are positioned between the two dominant global cybersecurity governance paradigms—the multistakeholder polycentricity institutionalized in the United States and the centralized, sovereignty-driven framework of China—making them theoretically productive sites for examining how middle powers configure PPPs and polycentric governance under conditions of great-power competition. Each state has developed a distinctive approach to cybersecurity that balances domestic institutional traditions with regional and global pressures: Australia emphasizes market-oriented resilience, Japan pursues technocratic consensus across industry, government, and academia, and Singapore leverages regional institutions to project governance capacity beyond its borders. Three research questions guide the analysis:

> RQ1: To what extent do the cybersecurity strategies of Australia, Japan, and Singapore reflect polycentric governance, and what role do public–private partnerships play within them?
>
> RQ2: What is the empirical relationship between PPP institutionalization and polycentric governance features in these strategies?
>
> RQ3: How do the configurations of PPPs and polycentric governance differ across the three cases, and what explains this variation?

By systematically coding and comparing these strategies, the study contributes to governance theory by providing an empirically grounded basis for distinguishing PPPs from polycentric governance, and to cybersecurity policy by illuminating how Indo-Pacific middle powers design governance architectures under geopolitical constraint.

## 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

### 2.1. POLYCENTRIC GOVERNANCE: CONCEPT AND APPLICATION TO CYBERSECURITY

Polycentric governance, as developed by Vincent Ostrom, Charles Tiebout, and Robert Warren (1961) and elaborated by Elinor Ostrom (2005), describes institutional arrangements in which multiple decision-making centers operate with a degree of autonomy within an overarching set of rules. Unlike monocentric systems where authority is concentrated in a single hierarchy, polycentric systems feature overlapping jurisdictions, redundant institutional functions, and opportunities for experimentation and mutual adjustment (Aligica & Tarko, 2012). These properties generate adaptive capacity, allowing governance systems to respond flexibly to complex, uncertain, and cross-scale challenges. Carlisle and Gruby (2019) offer a systematic operationalization identifying three core features: multiple decision-making centers with genuine authority, an overarching governance framework linking these centers, and emergent patterns of interaction including cooperation, competition, and conflict resolution.

Cybersecurity governance is a domain where polycentric arrangements have particular relevance. Cyberspace is inherently layered, transnational, and populated by heterogeneous actors—governments, corporations, technical communities, international organizations, and civil society—whose interactions cross jurisdictional boundaries (Raymond & DeNardis, 2015). Shackelford (2012) was among the first to apply polycentric governance theory to cybersecurity, arguing that effective cyberpeace requires integrating multiple governance mechanisms: laws, norms, market incentives, self-regulation, partnerships, and multilateral cooperation. This multimechanism approach reflects the broader insight from governance network theory that complex policy problems require networked rather than hierarchical institutional responses (Rhodes, 1997; Klijn & Koppenjan, 2016). In the cybersecurity domain, even actors without formal rule-making authority, such as firms providing technical standards or incident-response expertise, play what Carlisle and Gruby (2019) term a critical supporting role in shaping norms, practices, and incentives. Legislatures, regulators, industry associations, and cross-border coalitions constitute the plural decision-making centers that polycentric theory foregrounds (Ostrom, 1999; Low et al., 2003).

### 2.2. PUBLIC–PRIVATE PARTNERSHIPS IN CYBERSECURITY

PPPs have become a ubiquitous feature of national cybersecurity strategies worldwide. Because the majority of critical digital infrastructure is privately owned and operated, governments cannot secure cyberspace without private-sector cooperation (Carr, 2016). PPPs in cybersecurity typically involve information-sharing agreements, joint incident-response protocols, co-investment in resilience measures, and industry participation in policy development (ENISA, 2020). Their operational value is widely acknowledged: they enable governments to access private-sector technical expertise and threat intelligence, while providing firms with access to classified threat information and channels for policy influence.

However, the governance function of PPPs is more circumscribed than is often assumed. Carr (2016) demonstrates that PPPs in national cybersecurity strategies primarily serve government-defined objectives, with private actors operating within parameters set by the state. In

Center for Strategic and International Studies (2013) they argue that without binding obligations and genuine shared authority, PPPs remain shallow instruments that do not fundamentally alter governance structures. Slayton and Clark-Ginsberg (2017) show that even well-developed public–private relationships in critical infrastructure protection tend to reproduce existing power asymmetries rather than distributing authority. These critiques suggest that PPPs, while valuable for operational coordination, do not automatically generate the autonomous, overlapping decision-making centers that polycentric governance requires.

### 2.3. THE GAP: PPPS AND POLYCENTRICITY AS DISTINCT PHENOMENA

The theoretical distinction between PPPs as mechanisms of operational collaboration and polycentric governance as a structural condition of distributed authority has been noted by several scholars (Shackelford, 2012; Carr, 2016) but has not been subjected to systematic comparative empirical analysis in the cybersecurity domain. Most studies either examine PPPs or polycentric governance independently, or implicitly treat the former as evidence of the latter. The Indo-Pacific region provides a particularly productive empirical context for this investigation because its leading cybersecurity states, Australia, Japan, and Singapore, are positioned between the institutionalized multistakeholder polycentricity of the United States and the centralized governance model of China, creating variation in how partnerships and governance structures are configured (Creemers, 2015). Moreover, these cases are embedded in regional frameworks, ASEAN, the Quad, and bilateral partnerships, that introduce additional layers of governance complexity. This study addresses the gap by developing a coding framework that operationalizes both PPP indicators and polycentric governance markers, applies it comparatively across three national strategies, and examines whether and how these phenomena intersect. The analytical framework builds on the proposition that the PPP–polycentricity relationship is not one of identity but of contingent co-presence, shaped by national governance traditions, strategic cultures, and geopolitical positioning. In sociological terms, the study examines how institutional isomorphism (DiMaggio & Powell, 1983) operates in cybersecurity: states adopt similar governance instruments (PPPs) while adapting their structural configurations to local institutional environments.

## 3. METHODS

### 3.1. RESEARCH DESIGN

This study employs a comparative qualitative content analysis of national cybersecurity strategy documents from three Indo-Pacific states: Australia, Japan, and Singapore. This study proceeds from an interpretivist epistemological position: policy documents are treated not as transparent windows onto governance practice but as constitutive texts that frame problems, distribute authority, and signal institutional intent. Qualitative content analysis is appropriate because the research questions require systematic interpretation of how policy texts frame governance arrangements, distribute authority, and institutionalize collaboration, analytic tasks that exceed purely quantitative measurement (Schreier, 2012; Hsieh & Shannon, 2005). The comparative design follows a most-similar systems logic (Przeworski & Teune, 1970): all three cases are advanced economies with high digital connectivity, mature cybersecurity

institutions, and active engagement in Indo-Pacific multilateral frameworks, yet they vary in governance traditions, strategic cultures, and the relative emphasis placed on state direction versus market coordination. This combination of shared contextual features and divergent institutional arrangements enables analytical leverage for identifying how different governance models produce distinct configurations of public–private partnerships and polycentric governance.

### 3.2. CASE SELECTION AND JUSTIFICATION

Three cases were selected based on theoretical and strategic criteria. Theoretically, Australia, Japan, and Singapore represent distinct governance archetypes within the Indo-Pacific: Australia combines centralized security institutions with liberal market-oriented cyber resilience; Japan exemplifies a technocratic, consensus-driven model rooted in industry–academia–government coordination; and Singapore operates a strong-state model that projects governance capacity outward through regional diplomacy. Strategically, all three occupy intermediate positions between the United States and China, the two dominant and contrasting cybersecurity governance models, making them critical cases for understanding how middle powers navigate competing governance paradigms. The selection of three cases balances depth of analysis with comparative breadth, consistent with established qualitative comparative practice (Ragin, 2014). To make the most-similar systems logic more precise: the variables held approximately constant across the three cases are (a) level of economic development (all three are high-income OECD-equivalent economies); (b) degree of digital infrastructure maturity (all rank in the top tier of global cybersecurity indices); (c) formal democratic governance institutions (all maintain rule-of-law systems with civilian oversight of security agencies); and (d) active participation in U.S.-led or U.S.-aligned Indo-Pacific security frameworks. The variables allowed to vary, and that constitute the study's explanatory focus, are governance tradition (technocratic vs. liberal-market vs. strong-state), strategic culture (security-centric vs. resilience-oriented vs. diplomatically projected), and relative emphasis on domestic versus externally-facing cybersecurity governance. This controlled variation enables cross-case inference about how distinct institutional logics shape the configuration of PPPs and polycentric governance under comparable structural conditions, without requiring a formal quantitative matching procedure inappropriate to a small-N qualitative design (Przeworski & Teune, 1970).

### 3.3. DATA COLLECTION

The primary data corpus consists of the most recent publicly available national cybersecurity strategy documents from each case: Japan's Cybersecurity Strategy (National Center of Incident Readiness and Strategy for Cybersecurity [NISC], 2021), Singapore's Cybersecurity Strategy (Cyber Security Agency of Singapore, 2021), and Australia's Cyber Security Strategy 2023–2030 (Department of Home Affairs, 2023). To situate these national strategies within their regional and geopolitical context, supplementary documents were incorporated: the Quad Cyber Challenge Joint Statement (Quad Leaders, 2024), China's Cybersecurity Law (National People's Congress of China, 2017), the U.S. National Cybersecurity Strategy Implementation Plan Version 2 (United States White House, 2024), and the ASEAN–Japan Cybersecurity Policy Meeting Joint Statement (ASEAN & Government of Japan, 2024). All documents

are publicly available official publications, ensuring transparency and replicability. The corpus was selected to capture both national policy orientations and the transnational governance frameworks in which they are embedded.

### 3.4. ANALYTICAL INSTRUMENT: CODEBOOK DEVELOPMENT

A structured codebook was developed through a hybrid deductive-inductive process. Initial codes were derived deductively from the theoretical framework: polycentric governance indicators (PG1–PG3) were operationalized from Ostrom's (2005) framework and subsequent applications to cybersecurity (Shackelford, 2012; Carlisle & Gruby, 2019), while PPP indicators (PPP1–PPP4) were drawn from Carr (2016) and ENISA (2020). Additional thematic codes, covering threat actors (TA), regional engagement (IP), policy postures (PP), and cybersecurity policy themes (CS), were developed iteratively through pilot coding of one document (Japan's strategy), refined through comparison with the remaining documents, and finalized prior to systematic coding. The codebook comprises six clusters and 22 individual codes (see Tab. 1). The deliberate analytical separation of PPP indicators from PG markers reflects the study's theoretical premise that these are distinct phenomena; the potential for circularity arising from this design choice is explicitly addressed below.

TA3 (The US) was identified inductively during pilot coding of Japan's strategy (one segment, referencing the US as a named bilateral partner rather than as a threat actor) but is not listed above as it functions analytically as an IP3 (Bilateral Partners) indicator in the cross-case analysis rather than as a threat actor equivalent to TA1, TA2, TA4, and TA5.

### 3.5. CODING AND ANALYTICAL PROCEDURE

Systematic coding was conducted using Taguette, an open-source, modest qualitative data analysis tool. Each document was coded in its entirety, with the unit of analysis being a meaningful text segment, defined as a clause, sentence, or paragraph expressing a single codable concept. Multiple codes could be applied to the same segment where warranted, enabling the identification of overlap between PPP and PG phenomena. Coding was performed by a single researcher in two rounds: an initial pass to apply codes systematically, and a verification pass to check consistency and resolve ambiguities. To mitigate single-coder bias, a subset of coded segments (approximately 15%) was reviewed against the codebook definitions for internal consistency. This review was structured as follows: segments were re-read against the relevant code definition, and any case where the original code assignment appeared questionable, because the passage was ambiguous, straddled two categories, or had been coded automatically on a first pass without adequate attention to definitional boundaries, was either reassigned or flagged for reflection in the thematic interpretation stage. In practice, the verification pass identified two recurring sources of ambiguity.

First, passages describing government agencies convening industry stakeholders for policy consultation proved difficult to distinguish between PPP3 (co-development) and PG1 (multistakeholder): the decisive criterion applied was whether the passage specified a binding or rule-making function for industry actors (coded PG1) or described them as providing input into a government-led process (coded PPP3). Second, passages referencing cross-border

cybersecurity cooperation required careful distinction between CS3 (International Cooperation, describing general cross-border collaboration) and IP1 (ASEAN Cooperation, reserved for cooperation explicitly framed within ASEAN institutional frameworks): the criterion was whether the passage invoked ASEAN as a named institutional context (coded IP1) or described bilateral or multilateral cooperation without ASEAN-specific framing (coded CS3).

| Tag | Description |
|---|---|
| TA – Threat Actors | Main categories of threat actors or sources of cybersecurity challenges identified in policy documents. |
| TA1 – China Linked | Threat actors, campaigns, or incidents attributed to Chinese state or affiliated groups. |
| TA2 – North Korea | Threat actors, campaigns, or incidents attributed to North Korean state or affiliated groups. |
| TA4 – Russia Linked | Threat actors, campaigns, or incidents attributed to Russian state or affiliated groups. |
| TA5 – Cybercrime | Criminal activities by non-state actors using digital means, including ransomware, fraud, and identity theft. |
| IP – Indo-Pacific | State positioning in regional cooperation frameworks. |
| IP1 – ASEAN Cooperation | Cybersecurity collaboration under ASEAN frameworks. |
| IP2 – Quad | Quad-led cyber initiatives and joint statements. |
| IP3 – Bilateral Partners | Bilateral cybersecurity cooperation agreements or frameworks. |
| IP4 – Regional Norms | Adoption of Indo-Pacific cyber norms (e.g., UNGGE). |
| PP – Policy Postures | A state's strategic orientation on cybersecurity. |
| PP1 – State-Led | Top-down regulation driven by national security priorities. |
| PP2 – Market-Driven | Self-regulation, liability mechanisms, and innovation incentives. |
| PP3 – Offensive Posture | Active or pre-emptive cyber operations as deterrence. |
| PP4 – Defensive Posture | Protecting national infrastructure and citizens from threats. |
| PP5 – Collaborative | Cooperation with private actors, civil society, and international partners. |
| CS – Policy Themes | Core focus areas within cybersecurity strategies. |
| CS1 – Threat Landscape | Description of cyber threats (APTs, ransomware, etc.). |
| CS2 – Critical Infrastructure | Policies for securing essential services. |
| CS3 – International Cooperation | Cross-border collaboration initiatives. |
| PPP1 – Formal Agreements | Contracts, Memoranda of Understanding (MoUs), or structured public–private frameworks. |
| PPP2 – Information Sharing | Exchange of threat intelligence between government and private actors. |
| PPP3 – Co-Development | Private-sector input in policy drafting or standards. |
| PPP4 – Joint Incident Response | Collaborative cyberattack mitigation protocols. |
| PG1 – Multistakeholder | Multiple actors (government, private sector, academia, NGOs) in governance. |
| PG2 – Decentralized Decision-Making | Authority distributed across agencies/entities. |
| PG3 – Overlapping Jurisdictions | Shared responsibilities across sectors and levels of governance. |

Tab. 1. Codebook: Tag Clusters and Descriptions
Note: Codebook developed through a hybrid deductive-inductive process. PPP and PG code clusters are deliberately separated to enable independent analysis of their relationship.

In several instances in Singapore's strategy, segments received dual codes (both CS3 and IP1) because the strategy language simultaneously invoked ASEAN frameworks and broader international cooperation goals. No codebook definitions were formally revised during the verification pass, but one segment in Japan's strategy was reclassified from PPP3 to PG1 after the verification check confirmed it specified a formal multi-stakeholder mandate rather than government-led policy input. While the absence of a second independent coder limits formal intercoder reliability claims, the structured codebook, iterative coding, and documented verification process enhance internal consistency within the constraints of a single-researcher design (Schreier, 2012). A transparency note on PG sub-codes: PG2 (Decentralized Decision-Making) and PG3 (Overlapping Jurisdictions) received zero coded segments across all three strategies. This is itself a substantive finding: polycentric governance, where present in the corpus, manifests exclusively through PG1 (Multistakeholder Involvement) rather than through formal decentralization of authority or explicit jurisdictional overlap. The absence of PG2 and PG3 coded segments is consistent with the paper's central argument that the three cases exhibit partial or emergent polycentricity, not the full structural distribution of authority that Carlisle and Gruby (2019) describe as ideal-typical polycentricity. References to overlapping jurisdictions or decentralized decision-making in the Analysis section reflect interpretive characterizations of the governance logic suggested by PG1-coded passages, not claims resting on independent PG2 or PG3 coding.

Analysis proceeded in three stages. First, code frequencies were tabulated for each document to identify patterns in emphasis and thematic distribution. Because the three core strategy documents differ substantially in length, raw frequencies were supplemented with proportional analysis, codes as a percentage of total coded segments per document, to enable valid cross-case comparison. A note on how coded references are counted throughout the Analysis: because Taguette records each tag application as a separate row, a single text segment coded with both the PG parent tag and the PG1 sub-tag generates two counted references. PG figures reported per case therefore reflect total PG-related tag applications (PG parent plus PG1 subcode), while PPP figures reflect parent-tag counts only, since the focus of the PPP analysis is on the aggregate partnership indicator rather than sub-type distribution. This counting asymmetry is a product of the analytical emphasis in each section and does not affect the substantive interpretation. Second, coded segments were subjected to thematic interpretation within each case, examining how PPP indicators and PG markers manifested in specific policy contexts and what governance functions they served. Third, cross-case comparison identified convergences, divergences, and distinctive configurations across the three cases, with reference to the supplementary documents (U.S., China, Quad, ASEAN) as contextual benchmarks. This three-stage procedure, quantitative description, within-case interpretation, cross-case comparison, follows established protocols for comparative qualitative content analysis (Schreier, 2012; Bryman, 2016).

A potential methodological concern is that separating PPP and PG codes in the codebook could predetermine the finding that PPPs and polycentric governance are distinct. Three design features mitigate this risk. First, the codebook permitted dual coding: any segment exhibiting both PPP and PG characteristics received both codes, allowing the analysis to capture overlap where it existed empirically. Second, the qualitative interpretation stage examined the

substantive content of coded segments to assess whether PPP-coded passages also reflected polycentric governance features in practice, regardless of their primary code assignment. Third, the cross-case comparison examined whether any case demonstrated structural integration of PPPs into polycentric governance arrangements, thereby testing the analytical premise against empirical variation. The finding of analytical distinctness is therefore an empirical result derived from the data, not an artifact of the coding scheme.

## 4. LIMITATIONS

Several limitations should be acknowledged. First, the study analyzes official policy documents, which represent strategic aspirations and discursive framing rather than implemented governance practices. The gap between policy rhetoric and institutional reality cannot be assessed through document analysis alone, though policy documents remain significant objects of study insofar as they shape institutional design and signal governance intent. To be explicit: what this study demonstrates is how governance is framed and imagined in national strategy documents, not how it operates on the ground. Claims in the Analysis and Discussion sections should be read accordingly: when the text states that "PPPs function as operational mechanisms" or that "polycentric features emerge through separate institutional channels," these are observations about the discursive and institutional architectures expressed in policy texts, not verified accounts of governance practice. Validating such claims empirically would require supplementary evidence from practitioner interviews, institutional ethnography, or process-tracing of specific governance episodes, all identified as priority directions for future research. Second, the reliance on a single coder, while mitigated by structured codebook use and iterative coding, limits intercoder reliability claims. Third, the three selected cases, while strategically important, do not capture the full diversity of Indo-Pacific cybersecurity governance, notably excluding South Korea, India, and Southeast Asian states beyond Singapore. Fourth, the study covers a ten-year period (2015–2025) through strategy documents published at particular points within this window, limiting temporal analysis of policy evolution. Fifth, the use of coding frequencies requires careful interpretation: variation in code counts across cases reflects differences in discursive emphasis and document length, not differences in actual governance capacity, commitment, or effectiveness. A country that mentions PPPs more frequently in its strategy document is not thereby more partnership-oriented in practice, only more rhetorically oriented toward partnership language.

All interpretations in the Analysis section are grounded in this caveat, but readers should apply the same caution when drawing inferences from the quantitative summaries in Figures 1–3. Sixth, while this study addresses reliability through the structured codebook and verification process, constructing validity, the question of whether the PPP and PG categories adequately capture the phenomena they purport to measure, merits explicit reflection. The construct definitions are grounded in established theoretical frameworks (Carlisle & Gruby, 2019; Carr, 2016), and the codebook was developed through a hybrid deductive-inductive process that tested definitions against empirical material before finalizing them. Nevertheless, alternative operationalizations are possible: for example, a broader definition of PG1 (multistakeholder) that included advisory roles alongside binding ones would have produced higher PG counts, particularly for Japan and Australia. The narrower operationalization adopted here, requiring

evidence of formal authority, was chosen precisely because the study's theoretical argument hinges on distinguishing genuine authority distribution from collaborative participation. This choice is theory-driven and transparent, but scholars working with broader conceptions of polycentricity may reach different empirical conclusions. Future research should incorporate interviews with policymakers and practitioners, multi-coder designs, and longitudinal analysis to address these constraints. The codebook used in this study is provided in Appendix A. The full coded dataset (573 segments across three national cybersecurity strategy documents, coded in Taguette) is available from the corresponding author upon reasonable request.

## 5. ANALYSIS

The analysis produced 573 coded segments across the three national cybersecurity strategies: Japan (251 segments, 43.8%), Australia (222 segments, 38.7%), and Singapore (100 segments, 17.5%). The variation in coding intensity reflects differences in document length, discursive depth, and policy breadth rather than differences in cybersecurity commitment or capability. To account for these differences, proportional analysis supplements raw frequencies throughout the cross-case comparison. It bears emphasis that code frequencies throughout this analysis measure discursive emphasis, how prominently a theme is foregrounded in the strategic text, not substantive governance capacity or operational effectiveness. A higher PPP count indicates that partnership mechanisms receive greater rhetorical attention in a given strategy document, not that the partnerships in question are better resourced, more institutionally embedded, or more effective in practice. Readers should interpret all quantitative summaries in Figures 1–3 with this caveat in mind. Tag distribution reveals significant variation in emphasis across all six coding clusters, with each state displaying a distinctive thematic profile shaped by its governance tradition, threat environment, and strategic positioning (see Figure 1). The sections below examine each case in terms of its governance configuration, focusing on polycentric governance features and PPP indicators, followed by a comparative synthesis that addresses the research questions directly.

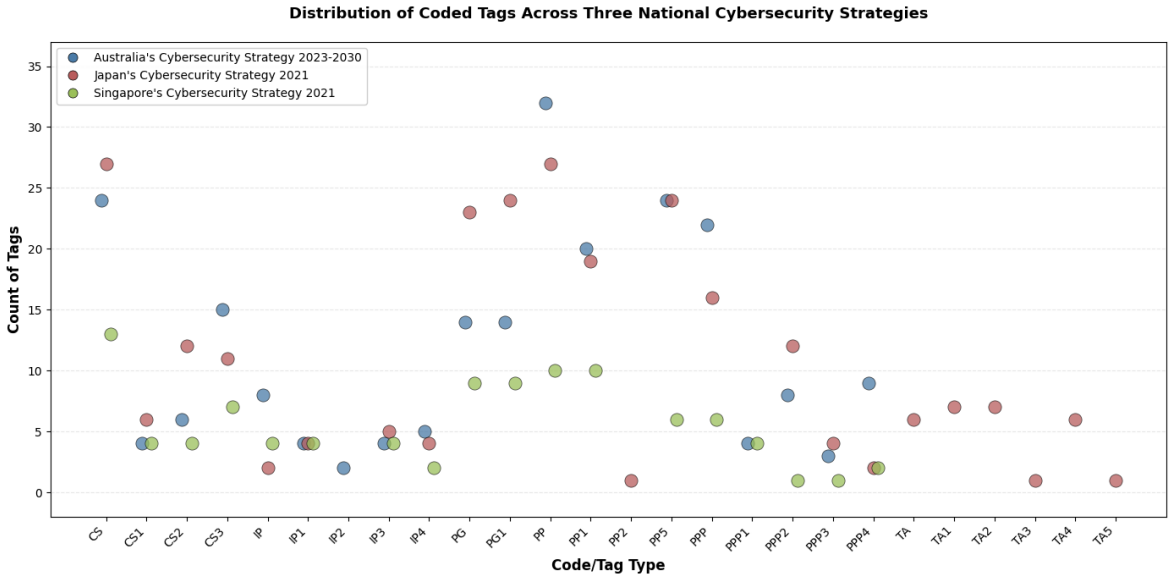


Fig. 1. Distribution of Coded Tags Across Three National Cybersecurity Strategies

## 5.1. JAPAN: TECHNOCRATIC POLYCENTRICITY UNDER STATE COORDINATION

Japan's 2021 Cybersecurity Strategy demonstrates the highest coding intensity among the three cases, reflecting a document characterized by conceptual breadth, institutional detail, and extensive integration of cybersecurity into national security planning. The governance model that emerges is best characterized as technocratic polycentricity: multiple actors, government agencies, private firms, and academic institutions, participate in governance through coordinated mechanisms, but the state retains overarching authority and strategic direction.

Threat framing serves as a structuring device. China, North Korea, and Russia are explicitly identified as state-linked cyber adversaries (TA1, TA2, TA4), alongside sustained attention to transnational cybercrime (TA5). This security-oriented framing positions cybersecurity as an existential national challenge intertwined with Japan's alliance relationships and geopolitical environment, reinforcing the rationale for strong state coordination. The strategy's emphasis on defensive posture (PP4), combined with acknowledgment of the need for proactive deterrence, reflects a governance approach that treats cybersecurity as inseparable from national defense policy. Japan's strategy also demonstrates temporal responsiveness to global cyber events: the WannaCry ransomware attack of 2017 and the SolarWinds compromise of 2020 are referenced as catalysts for supply-chain resilience reforms and enhanced public–private information exchange. This suggests that Japan's technocratic approach is adaptive to external shocks, even as it remains anchored in centralized coordination.

Polycentric governance features are prominent, with 47 coded references constituting the highest PG count among the three cases (see Figure 2 below). Japan's tri-sectoral model integrates government, industry, and academia through research platforms, knowledge-sharing mechanisms, and coordinated innovation hubs. These arrangements exemplify multistakeholder involvement (PG1), the only PG sub-code that received coded segments in this study (PG2 and PG3 recorded zero hits across the full corpus, as noted in the Coding Procedure section), and the overlapping jurisdictions and decentralized authority they suggest remain interpretive rather than independently coded findings. However, this is structured polycentricity: authority remains centralized, with non-state actors empowered through formal mechanisms but operating within state-defined parameters. The strategy consistently emphasizes government leadership in ensuring that all stakeholders act in alignment with national priorities, indicating that coordination rather than autonomous authority characterizes stakeholder participation.

PPP indicators (16 coded references) reveal formalized partnerships for information sharing, regulatory co-development, and joint incident exercises. Crucially, these PPPs function as extensions of state-led programs rather than as autonomous decision-making centers. Partnerships are advanced through government-led frameworks that ensure alignment with national priorities, confirming their operational rather than structural governance character. Japan's case thus illustrates a critical empirical finding: extensive stakeholder engagement and formalized PPPs can coexist with, and remain subordinate to, centralized governance authority. The polycentric features emerge not from PPPs but from the broader institutional architecture of distributed research platforms, multi-agency mandates, and international cooperation.

## 5.2. AUSTRALIA: RESILIENCE-ORIENTED GOVERNANCE WITH EXTENSIVE PPPS

Australia's Cyber Security Strategy 2023–2030 presents a governance model oriented toward societal resilience. Unlike Japan's security-centric framing, Australia emphasizes business readiness, community preparedness, and civil resilience as the foundations of cybersecurity governance. The strategy rarely frames threats in geopolitical or military terms, instead focusing on ransomware, supply-chain vulnerabilities, and the societal impacts of cyber incidents. This civilian orientation shapes both the prominence of PPPs and the nature of polycentric governance features.

PPPs are central to Australia's approach, with 22 coded references representing the highest PPP count among the three cases (see Figure 3 below). The strategy institutionalizes partnerships through co-investment schemes, structured threat-response protocols, and collaborative frameworks that mobilize businesses and communities alongside government agencies. This shared-responsibility model reflects Australia's liberal governance tradition and its emphasis on market coordination as a complement to state direction. Partnerships serve concrete operational functions: they enhance threat intelligence sharing, coordinate incident response across sectors, and distribute resilience-building responsibilities across society. The prioritization of ransomware mitigation and critical infrastructure resilience has made PPPs a core element of what can be described as a civil-centric cybersecurity architecture, one oriented toward protecting societal functions rather than projecting state power.

Polycentric governance markers (28 coded references) are evident through decentralized preparedness mechanisms and the functional distribution of resilience responsibilities across government agencies, businesses, and local communities. Yet the analytical separation of PPPs and polycentricity is particularly instructive in Australia's case. Despite the prominence of partnerships, polycentric features emerge not from PPPs themselves but from the broader institutional architecture: overlapping agency mandates, community-level resilience programs, multi-sector regulatory frameworks, and engagement with international institutions. Extensive partnerships coexist with polycentric features, but the two operate through distinct institutional channels. The centralized policy framework, in which the government sets strategic priorities, regulatory standards, and investment parameters, remains intact even as operational collaboration is distributed.

## 5.3. SINGAPORE: REGIONALLY PROJECTED GOVERNANCE

Singapore's Cybersecurity Strategy 2021 is the most concise of the three documents (100 coded segments), reflecting a strategy oriented toward international engagement and regional capacity-building rather than extensive domestic institutional elaboration. Singapore's distinctive governance feature is its outward-facing orientation: the strategy positions Singapore as a regional hub for cybersecurity norm-setting, legal development, and capacity-building, leveraging institutions such as the ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE) and the ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC).

PPP indicators are least frequent (6 coded references), and domestic public–private partnerships receive substantially less emphasis than in Japan or Australia. Where PPPs appear, they are most visible in externally oriented initiatives, collaboration with Japan on ASEAN-based

cybersecurity centers, for instance, rather than as core domestic governance mechanisms. This reflects Singapore's strategic choice to leverage partnerships primarily as instruments of regional diplomacy and influence rather than as pillars of domestic cybersecurity architecture. Domestically, Singapore supports academic partnerships and multistakeholder participation, but these remain secondary to the state's centralizing authority over cybersecurity policy. The low PPP count does not indicate a lack of private-sector engagement but rather its subordination to a coherent, state-directed strategy that channels collaborative efforts outward.

Polycentric governance features (18 coded references) emerge primarily through Singapore's international engagement: ASEAN cooperation, bilateral partnerships, and contributions to global norm development through frameworks such as the United Nations Group of Governmental Experts (UNGGE). Domestically, Singapore's governance model remains centralized and state-directed. The Cyber Security Agency of Singapore operates as a strong central authority with clear regulatory mandates, and domestic policy-making is top-down. The polycentricity that exists is thus projected outward, manifesting in regional institutional frameworks and multilateral initiatives rather than in the domestic distribution of governance authority. Singapore's case demonstrates that polycentricity need not be exclusively domestic: a state can contribute to polycentric governance externally through regional norm-setting and capacity-building while maintaining monocentric domestic arrangements. This outward projection of governance capacity reflects Singapore's broader small-state strategy of leveraging institutional entrepreneurship to amplify its influence beyond its demographic and territorial constraints.

## 5.4. COMPARATIVE SYNTHESIS

Cross-case comparison reveals three distinct configurations of PPPs and polycentric governance (Fig. 2 and 3), none of which treats the two as equivalent or structurally integrated. Japan embodies technocratic polycentricity, integrating multiple stakeholders through state-coordinated platforms while maintaining centralized authority; PPPs function as operational extensions of this state-led system. Australia institutionalizes resilience-oriented governance with the most extensive PPP framework, yet polycentric features emerge separately through distributed preparedness mechanisms and international engagement. Singapore projects polycentricity regionally through ASEAN and bilateral frameworks while maintaining domestic centralization, with PPPs serving primarily diplomatic functions.

These configurations occupy an intermediate position between two global benchmarks. The United States represents a case where PPPs are embedded within a formalized multistakeholder polycentric system, exemplified by the Cybersecurity and Infrastructure Security Agency (CISA) and its Joint Cyber Defense Collaborative (JCDC; World Economic Forum, 2023). In the U.S. model, partnerships are nested within a broader governance architecture that also features independent regulatory agencies, Congressional oversight, judicial review, and autonomous private-sector governance bodies, producing genuine polycentricity through the multiplication of authoritative decision-making centers. China represents the opposite pole, where PPPs exist, private technology firms participate actively in cybersecurity infrastructure, but are state-mandated within a monocentric, sovereignty-driven framework in which the state

retains unambiguous hierarchical authority (Creemers, 2015). The three Indo-Pacific cases examined here fall between these poles, exhibiting neither the formalized multi-center authority of the U.S. system nor the tight state control of the Chinese model. The Quad's flexible multilateral initiatives and ASEAN's capacity-building programs represent additional pathways to polycentric governance that operate at the regional level, independently of bilateral PPPs, and that merit further comparative investigation.

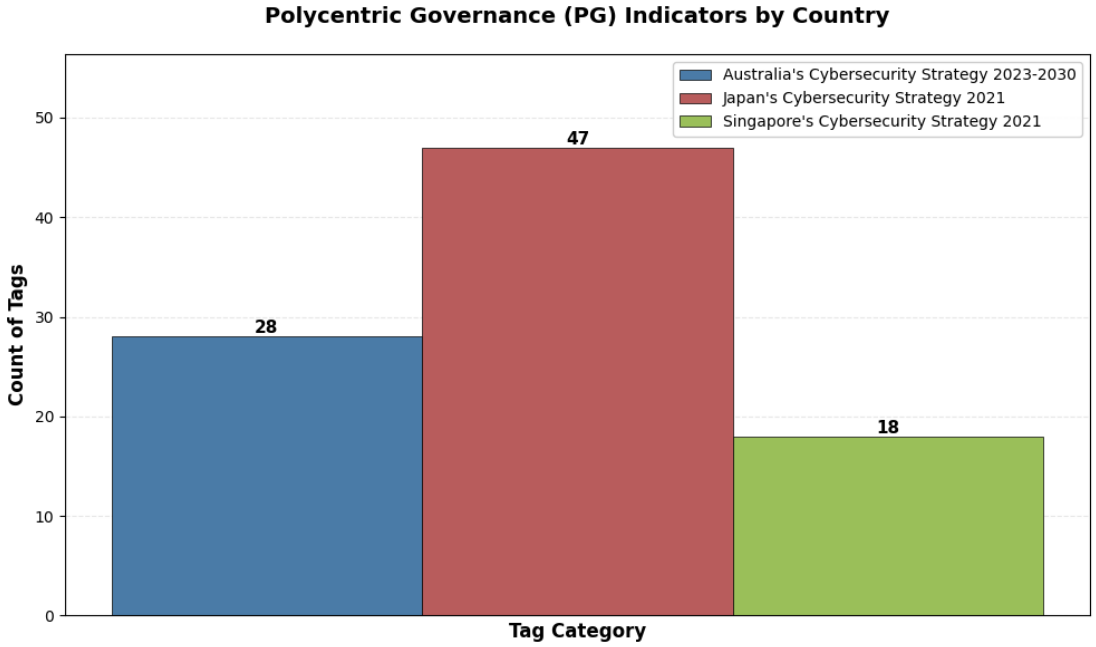


Fig. 2. Polycentric Governance (PG) Indicators by Country

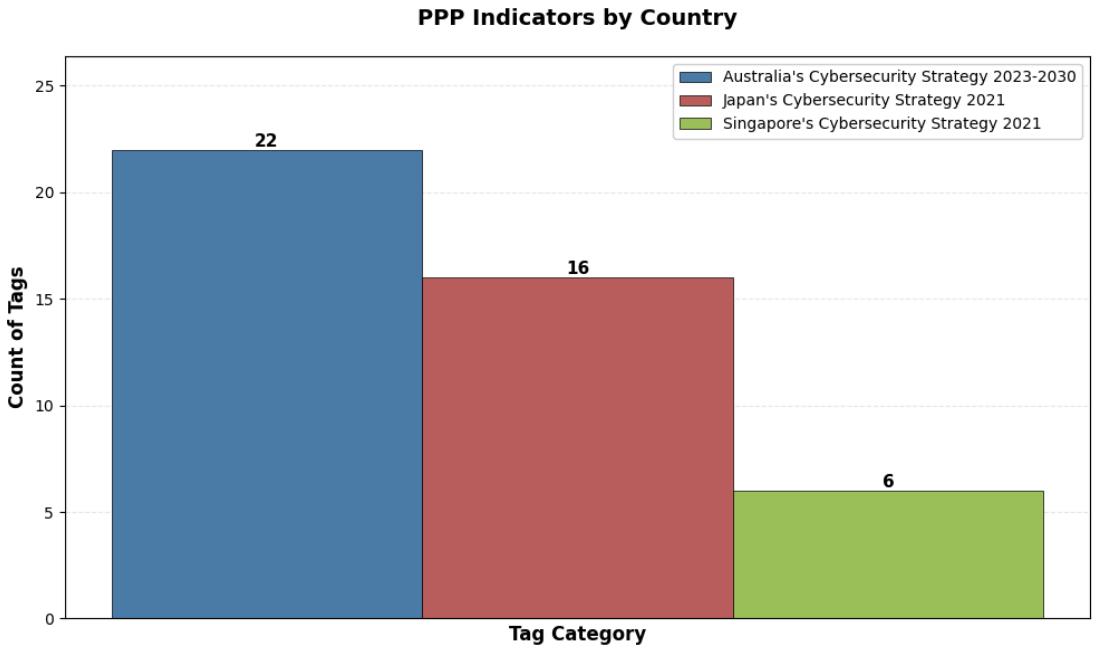


Fig. 3. Public–Private Partnership (PPP) Indicators by Country

Across all three cases, the central empirical finding holds: PPPs and polycentric governance are co-present but analytically and institutionally distinct. PPPs serve operational functions within state-led architectures, while polycentric features emerge through separate institutional channels, international cooperation, overlapping institutional mandates, and multi-actor regulatory frameworks. The nature and extent of both phenomena vary systematically by case, shaped by national governance traditions, strategic cultures, and geopolitical positioning.

## 6. DISCUSSION

The findings speak directly to the three research questions guiding this study and carry implications for both governance theory and cybersecurity policy practice. Addressing RQ1, all three strategies exhibit polycentric governance features alongside institutionalized PPPs, but the two phenomena serve distinct governance functions. PPPs address operational needs, including information sharing, incident coordination, capacity co-investment, while polycentric governance features reflect structural properties of the governance architecture: the distribution of authority across multiple centers, the overlap of jurisdictions, and the participation of diverse actors in rule-making. This finding confirms the theoretical premise, advanced conceptually by Shackelford (2012) and Carr (2016), that PPPs are instruments of collaboration rather than evidence of polycentricity per se, and provides the first comparative empirical support for this distinction in the cybersecurity domain.

Addressing RQ2, the empirical relationship between PPPs and polycentric governance is one of co-presence without structural integration. In no case do PPPs generate the autonomous decision-making centers or overlapping authority structures that characterize polycentric governance. Even in Australia, where PPPs are most extensive, polycentric features derive from separate institutional sources: overlapping agency mandates, community-level resilience mechanisms, and engagement with international frameworks. In Japan, the most polycentrically featured case, the tri-sectoral innovation platforms that produce overlapping jurisdictions are distinct from the PPP mechanisms that facilitate information sharing and incident response. This finding suggests that the pathway from operational partnerships to structural polycentricity is not automatic and may require additional institutional design, binding authority-sharing arrangements, formalized multi-actor regulatory mandates, or internationalized governance mechanisms, that exceeds what conventional PPPs provide. The implications for governance theory are significant: if partnerships and polycentricity are institutionally separable, then the widely held assumption that expanding PPPs inherently moves governance systems toward greater distribution of authority is empirically unfounded, at least in the cybersecurity domain.

Addressing RQ3, cross-national variation is substantial and interpretable through institutional and strategic lenses. Japan's technocratic polycentricity reflects its governance culture of consensus-driven coordination and the deep institutionalization of industry–academia–government relationships. Australia's resilience-oriented model reflects a liberal governance tradition that emphasizes market coordination and community preparedness alongside centralized strategic direction. Singapore's outward-facing model reflects its small-state strategy of leveraging regional institutions for influence and norm-setting. These patterns suggest that insti-

tutional context, shaped by governance traditions, state capacity, and geopolitical positioning, mediates how PPPs and polycentric governance are configured within national cybersecurity strategies. In sociological terms, we observe institutional isomorphism (DiMaggio & Powell, 1983) at the instrumental level, all three states adopt PPPs, but institutional divergence at the structural level, with polycentric features shaped by nationally specific institutional logics.

Theoretically, the study advances governance research by providing empirical evidence for a distinction that prior scholarship has largely argued in conceptual terms. The proposed analytical framework, from differentiating operational collaboration (PPPs) from structural governance distribution (polycentricity) to offering a tool applicable beyond cybersecurity to domains such as environmental governance, public health, and digital regulation where public–private collaboration is embedded within complex governance architectures. The concept of contingent co-presence, PPPs and polycentricity as analytically separable phenomena whose relationship is mediated by institutional context, adds precision to comparative governance research. This concept resonates with governance network theory (Rhodes, 1997; Klijn & Koppenjan, 2016), which similarly distinguishes between the existence of network relationships and the structural properties of governance systems. Just as governance networks do not automatically produce distributed authority, public–private partnerships do not automatically produce polycentricity. The structural conditions of genuine polycentricity, autonomous decision-making centers, overlapping jurisdictions, emergent coordination, require institutional foundations that go beyond bilateral collaboration.

For a sociological audience, the findings illuminate how the global diffusion of governance instruments intersects with local institutional variation. The three Indo-Pacific states studied here have all adopted PPPs as a governance instrument, consistent with coercive and mimetic isomorphism in the cybersecurity policy field (DiMaggio & Powell, 1983), but have embedded them within nationally distinctive institutional configurations. Japan's consensus-driven technocracy, Australia's liberal resilience model, and Singapore's diplomatic projection strategy each reflect deeply embedded governance cultures that shape how imported instruments are adapted to local institutional logics. This observation extends the institutional isomorphism framework by demonstrating that isomorphism at the instrument level can coexist with substantial divergence at the structural level, a pattern likely to be found across other policy domains where global governance scripts encounter diverse national institutional environments.

For policymakers, the findings caution against treating PPPs as sufficient instruments for achieving resilient, distributed governance. While partnerships are essential for operational coordination, mobilizing private-sector resources, and improving incident response, genuine polycentricity requires institutional mechanisms that distribute authoritative decision-making across autonomous centers, overlapping mandates, multi-actor regulatory platforms, and internationalized governance structures. Indo-Pacific states seeking to enhance cybersecurity governance should therefore design PPPs and polycentric institutions as complementary but distinct components of their governance architectures. The three models identified in this study, technocratic, resilience-oriented, and regionally projected, offer differentiated templates for how this complementarity might be realized under varying institutional conditions.

## 7. CONCLUSION

This comparative analysis of cybersecurity strategies in Australia, Japan, and Singapore demonstrates that public–private partnerships and polycentric governance are co-present but analytically and institutionally distinct governance phenomena. PPPs function as operational mechanisms, from facilitating information sharing, incident response, to co-investment, within state-led frameworks that retain centralized strategic authority. Polycentric governance features, such as overlapping jurisdictions, multistakeholder involvement, and decentralized decision-making emerge through separate institutional channels: international cooperation frameworks, multi-agency regulatory mandates, and regional capacity-building initiatives. The finding holds consistently across three distinct governance configurations: Japan's technocratic polycentricity, Australia's resilience-oriented governance, and Singapore's regionally projected model.

The theoretical contribution lies in providing the first systematic comparative empirical evidence for the PPP–polycentricity distinction in cybersecurity governance. The concept of contingent co-presence, whereby PPPs and polycentric governance coexist but their relationship is mediated by national institutional contexts rather than being structurally necessary, offers a more precise analytical framework for comparative governance research. This framework extends beyond cybersecurity to any policy domain where public–private collaboration operates within complex, multi-level institutional environments.

Empirically, the study maps three governance archetypes that occupy the intermediate space between U.S. multistakeholder polycentricity and Chinese centralized governance, demonstrating how Indo-Pacific middle powers navigate competing global paradigms while retaining institutional autonomy. The cross-national variation reveals that governance traditions, strategic cultures, and geopolitical positioning shape not only the extent of PPPs and polycentric governance but their configuration, how these phenomena are institutionally housed, politically legitimated, and strategically deployed. For practitioners, the findings caution against the assumption that establishing public–private partnerships automatically produces distributed, resilient governance. Policymakers seeking genuine polycentricity must complement operational partnerships with institutional mechanisms of shared authority. The three models identified here, technocratic, resilience-oriented, and regionally projected, provide templates for how PPPs and polycentric governance can be designed as complementary components of cybersecurity architectures under varying institutional conditions.

Future research should extend this analytical framework in several directions: applying the coding instrument to additional regions, particularly Europe and the Global South, to test generalizability; incorporating practitioner interviews and institutional ethnography to capture the gap between policy discourse and governance practice; conducting longitudinal analysis to track how major cyber incidents reshape the PPP–polycentricity relationship; and investigating the conditions under which operational partnerships evolve into autonomous governance centers, approximating genuine polycentricity over time. This last question, the institutional dynamics of the partnership-to-polycentricity transition, represents a theoretically significant and practically consequential research agenda for governance scholarship.

**FUNDING:** This research received no external funding.
**CONFLICT OF INTEREST:** The authors declare no conflict of interest.
**ACKNOWLEDGEMENTS:** This article's initial draft was presented at the International Public Policy Association Conference (ICPP7) in Chiang Mai, Thailand, which was funded by University of Warsaw's microgrant under Action IV.4.1 "A complex programme of support for UW PhD students" implemented in the programme "Excellence Initiative—Research University," 2025.

## REFERENCES

Aligica, P. D. & Tarko, V. (2012). Polycentricity: From Polanyi to Ostrom, and beyond. Governance, 25(2), 237–262.

ASEAN & Government of Japan. (2024). ASEAN–Japan cybersecurity policy meeting joint statement. https://www.cyber.go.jp/eng/pdf/17thAJCPM_en.pdf

Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.

Carlisle, K. & Gruby, R. L. (2019). Polycentric systems of governance: A theoretical model for the commons. Policy Studies Journal, 47(4), 927–952.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62.

Creemers, R. (2015). The pivot in Chinese cybergovernance: integrating internet control in Xi Jinping's China. China Perspectives, 4, 5-13.

Center for Strategic and International Studies. (2013). Public-Private Partnerships for Critical Infrastructure Protection. Report, August 19. https://www.csis.org/analysis/public-private-partnerships-critical-infrastructure-protection

Cyber Security Agency of Singapore. (2021). Singapore cybersecurity strategy 2021. https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021

Department of Home Affairs. (2023). Australia's cyber security strategy 2023–2030. Australian Government. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

DiMaggio, P. J. & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160.

European Union Agency for Cybersecurity. (2020). Public–private partnerships (PPPs) in cybersecurity. https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

Hsieh, H.-F. & Shannon, S. E. (2005). Three approaches to qualitative content analysis. Qualitative Health Research, 15(9), 1277–1288.

Klijn, E. H. & Koppenjan, J. (2016). Governance networks in the public sector. Routledge.

Low, B. S., Ostrom, E., Simon, C. P., & Wilson, J. (2003). Redundancy and diversity: Do they

influence optimal management? In F. Berkes, J. Colding & C. Folke (Eds.), Navigating social-ecological systems: Building resilience for complexity and change (pp. 83–114). Cambridge University Press.

McGinnis, M. D. & Ostrom, E. (2011). Reflections on Vincent Ostrom, public administration, and polycentricity. Public Administration Review, 72(1), 15–25.

National Center of Incident Readiness and Strategy for Cybersecurity. (2021). Cybersecurity strategy of Japan. https://www.nisc.go.jp/eng/index.html

National People's Congress of China. (2017). Cybersecurity law of the People's Republic of China. https://www.chinalawtranslate.com/cybersecurity-law/

Ostrom, E. (1999). Coping with tragedies of the commons. Annual Review of Political Science, 2(1), 493–535.

Ostrom, E. (2005). Understanding institutional diversity. Princeton University Press.

Ostrom, V. (1991). The meaning of American federalism: Constituting a self-governing society. ICS Press.

Ostrom, V., Tiebout, C. M., & Warren, R. (1961). The organization of government in metropolitan areas: A theoretical inquiry. American Political Science Review, 55(4), 831–842.

Przeworski, A. & Teune, H. (1970). The logic of comparative social inquiry. Wiley.

Quad Leaders. (2024). Quad cyber challenge joint statement. https://2021-2025.state.gov/2024-quad-cyber-challenge-joint-statement/

Ragin, C. C. (2014). The comparative method: Moving beyond qualitative and quantitative strategies (2nd ed.). University of California Press.

Raymond, M. & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. International Theory, 7(3), 572–616.

Rhodes, R. A. W. (1997). Understanding governance: Policy networks, governance, reflexivity, and accountability. Open University Press.

Schreier, M. (2012). Qualitative content analysis in practice. SAGE.

Shackelford, S. J. (2012). Toward cyberpeace: Managing cyberattacks through polycentric governance. American University Law Review, 62, 1273–1330.

Slayton, R. & Clark-Ginsberg, A. (2017). Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. Regulation & Governance, 14(3), 451–467.

United States White House. (2024). National cybersecurity strategy implementation plan (Version 2). https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

World Economic Forum. (2023). Global cybersecurity outlook 2023. https://www.weforum.org/publications/global-cybersecurity-outlook-2023/

**ARTICLE HISTORY:** Received 2026-02-28 / Accepted 2026-04-19