ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Hypersecuritisation and Norm-Grafting in Middle-Power Cybersecurity: The Strategic Evolution of South Korea

Kuang-Ho Yeh | Graduate School of International Studies and Regional Development, University of Niigata Prefecture, Japan | ORCID: 0009-0002-4505-4670

Abstract

Since the 2010s, South Korea's cybersecurity strategy has undergone a pronounced shift towards a proactive orientation propelled by interrelated pathways. First, via hypersecuritisation, the country has cultivated a threat-centric discourse that heighten societal sensitivity to cyber risks and its narratives. Second, through norm-grafting, it has aligned with international cybersecurity norms to legitimise strategic repositioning. This article advances a focussed analytical framework integrating political–discursive dynamics with standing-seeking norm politics to explain and assess the evolution of national cybersecurity strategies, addressing gaps in the existing scholarship that has often remained descriptive and under-theorised regarding the mechanisms of strategic change. Empirically, viewed through a power lens, South Korea conjoins alliance-anchored deterrence with middle-power diplomacy – leveraging regional fora and capacity-building platforms to translate cyber capabilities into political influence and legitimating authority. Transformations hedge against skepticism as well as institutional resistance domestically and internationally, reflecting a realist convergence of security conceptions on the Korean Peninsula. Over time, Seoul's posture has approached the threshold of its long-standing prudent principle, signalling a move from a predominantly defensive orientation to a more proactive, agentic, and

Received: 27.11.2025

Accepted: 24.03.2026

Published: 30.05.2026

Cite this article as:
K.H. Yeh, "Hypersecuritisation and norm-grafting in middle-power cybersecurity: The strategic evolution of South Korea," ACIG, vol. 5, no. 1, 2026, doi: 10.60097/ACIG/219971.

Corresponding author:
Kuang-Ho Yeh, Graduate School of International Studies and Regional Development, University of Niigata Prefecture, Japan. E-mail: n25m102f@gks.unii.ac.jp/ry1207@gmail.com
0009-0002-4505-4670

assertive rationale of strategic practice. Nevertheless, given persistent external threats, operational controversies, and structural limitations of cybersecurity capabilities, South Korea continues to rely on the synergy of hypersecuritisation and norm-grafting. This configuration constitutes the pillar of contemporary policy and is poised to shape the architecture and trajectory of its cybersecurity strategy in the foreseeable future.

Keywords

cybersecurity, legitimacy, hypersecuritisation, norm-grafting, US–ROK alliance

1. Introduction

Nowadays, South Korea possesses the world's highest high-speed internet penetration rate, efficient computer networks, and the cutting-edge digital technology. Yet, compared to material strengths, the country's approach to cybersecurity remained relatively complacent until around 2010 [1]. Since then, South Korea has accelerated its retreat from the earlier mindset, in terms of both public awareness of cyber threats and implementation of security policies, exhibiting a move towards systematisation, coordination, and a more proactive strategic stance. On account of the pivotal role of cyberspace in facilitating cross-domain operations, cybersecurity has advanced to the forefront of military security configuration, catalysing policy reforms and capability development across land, maritime, air, and outer space [2]. Thus, cybersecurity has presented not only an emerging fulcrum for (re-)structuring South Korea's security apparatus but also an essential lever for expanding national influence as a middle power[1] on the Korean Peninsula and within the Northeast Asia region. Thereby, the development of South Korean cybersecurity strategy faces multiple challenges. Domestically, comparative lags in frontier normative and legal frameworks constitute an institutional bottleneck. Regionally, neighbouring state actors – particularly North Korea and China – display counteractive tendencies rooted in the regional security dilemma, amplifying the uncertainty surrounding strategic implementation [3].

These dynamics give rise to the following core research questions: On what conceptual models can the transformation of South Korea's cybersecurity strategy be understood? What is the generative logic linking these security choices to the broader doctrinal shifts? And how can the future trajectory of the country's cybersecurity policy,

1——The term 'Middle Power' originated from Canadian and Australian political elites in the aftermath of WWII, highlighting global positioning and diplomatic autonomy initially. Over time, the concept evolved into a cognition for the expanding group of emerging states, operationalised through control of critical resources, advanced technologies, or discourses in specific policy domains. A salient example is South Korea's established strength in Information and Communications Technology (ICT) and the extensive digitalisation of its public infrastructure amid the Fourth Industrial Revolution. By leveraging comparative advantages, middle powers exert influence and advance functional governance on pressing global issues.

as well as its overarching security strategy be assessed? Given the close interrelationship between South Korea's cybersecurity initiatives under its extensive security posture, and in light of the growing likelihood of the US–Republic of Korea (ROK) alliance in cyberspace alongside the context of global strategic competition, a systematic analysis of the thorough behavioural patterns underpinning South Korea's adaptive changes in cybersecurity – along with the construction of an analytical framework for assessing its continuum – carries both policy and scholarly significance. By tracing the fabric of South Korea's cybersecurity discourse and associated policy actions over the past decade, this article endeavours to develop pertinent academic concepts and to provide a balanced perspective that integrates theoretical insights with empirical observations in addressing the aforementioned issues.

2. Review of the Scholarly Landscape

Persistent vulnerabilities in cyberspace, coupled with the escalating tempo of malicious intrusions, poses enduring risks to national security, economic stability, and the everyday life of citizens [4]. Accordingly, governments worldwide are formulating and implementing comprehensive cybersecurity strategies. The existing scholarship on South Korea's cybersecurity strategy has largely commenced with the examination of its policy development path. Analysts consistently observe notable shifts in strategic vision, institutional architecture, and patterns of international cooperation, prompting inquiries into the driving forces and implications of these changes [5, 6, 7]. Yet much of this literature is predominantly descriptive and context-focussed, offering limited elaboration and theoretical depth on the mechanisms underpinning stepwise development. One prominent research strand of inquiry adopts the alliance-strategy perspective [8, 9, 10], positing that South Korea's cybersecurity policy adjustments are intended to both compensate for deficiencies in its own defensive capabilities, and signal alignment with the US-led international cybersecurity collaborations. In return, Seoul seeks United States' support in the areas such as technical competency augmentation and the enhancement of national defence autonomy. This perspective illuminates significant linkages between foreign policy and cybersecurity strategy. However, the causal pathways remain under specified, leaving considerable scope for theorisation in academic research. Drawing on the structural–geopolitical lens of the Korean Peninsula, another body of work attributes strategic change to security threats from external cyberattacks [11, 12, 13, 14]. Yet the indirect and non-kinetic nature of cyber operations means that, under commensurable scenarios,

they have not yet posed an immediate existential danger to physical infrastructures and populations.[2] Moreover, temporal variation in South Korea's cybersecurity policy warrants closer scrutiny. In articulating and promoting relevant policies, the Korean government has invoked its self-identification as a global middle power, cultivating its 'middlepowerhood' [15, 16] – a mixed positional role as both 'knowledge creator' and 'norm disseminator' in internal cyber policy debates and external cyber diplomacy exertions [17]. This underscores the need for in-depth analysis on how these imageries are constructed, circulated, and institutionalised. Some scholars contend that South Korea's vital advantage in cybersecurity lies in its capacity to possess both contextual and positional intelligence, enabling the country to continuously interpret an ever-evolving security environment, and to accurately discern its dynamic position within the global cyberspace order [18].

Correspondingly, scholarly assessments of continuity and change in South Korea's cybersecurity posture diverge sharply, particularly regarding the impact of proactive cyber defence on strategic evolution. Some scholars contend that Seoul's increasingly assertive responses to cyber threats have reinforced the effectiveness of the US–ROK alliance in this domain, producing spillover effects that shape regional security architectures spanning both traditional and non-traditional spheres [19, 20, 21]. Others emphasise that regulatory constraints and uncertainties in advanced technological innovation have kept strategic change moderate and cautious [22, 23, 24]. While the literature has addressed the historical trajectory, drivers, and emergent trends of South Korea's cybersecurity strategy, it provides limited explanation of the distinctive characteristics and internal transformative logic of this development. The divergence of views underscores the difficulty of situating South Korea's strategic evolution within binary typologies, such as 'conservative' versus 'radical', or 'reactive' versus 'proactive', thereby highlighting the imperative for further exploration of its intrinsic determinants. In reality, its approach blends elements of *status quo* preservation with revisionist impulses – emphasising incremental adaptation in a short administrative process, while exhibiting a complex strategic dynamic trending from defence towards offence over a longer policy cycle.

This article argues that South Korea's cybersecurity strategy is underpinned by two rational functions. On one hand, adopting a sober realist diagnostics of cyberspace security, reinforcing – through both threat discourse and operational measures – awareness of the Peninsula's precarious security environment and domestic vulnerability to cyberattacks. On the other hand, informed

2——This non-assertive stance is evident in the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, particularly in its treatment of the threshold at which a cyberattack qualifies as a 'use of force'. Rule 11 of the Manual adopts the 'scale and effects' formulation with the comment explicitly stating that physical consequences serve as the major criterion. States have largely denied extending the definition to encompass economic or political coercion; therefore, merely providing state sponsorship to a hacktivist group conducting cyberattacks is relatively deemed insufficient to constitute a use of force.

by its existing diplomatic image, self-perceived international role, and the necessities of relationship-building, South Korea maintains acute sensitivity to the international cyberspace norms and corresponding domestic legal frameworks governing cyber operations, thereby ensuring the docking of strategic adjustments with legitimacy requirements at both levels. Against this backdrop, the driven strategy can be dissected as a dual-track theoretical approach comprising 'hypersecuritisation' and 'norm-grafting'. The former grants the agency to initiate strategic development by employing rhetoric to amplify threat narratives in the digital domain, while the latter furnishes the normative foundations and legitimacy leverage for determining direction and scope of cybersecurity policy transformation. Accordingly, this article envisions the conceptual paradigm of hypersecuritisation and constructs the metatheoretical model of norm-grafting, subsequently seeks to articulate the synergistic connections in the context of South Korea's cybersecurity strategy evolution. This integrated framework is designed to reify the response to the research questions and the empirical analysis.

3. Hypersecuritisation and Norm-Grafting in Convergence: An Analytical Framework

This article adopts the concept of hypersecuritisation to depict the political-discursive mechanism of threat amplification that transcends the rationale of conventional securitisation. Through this process, South Korea portrays cyberspace as a domain marked by acute crisis imagery. Based upon visual narrative foundations, the government subsequently invokes established normative frameworks across specific issue areas to bolster the credibility and authority of its cybersecurity policy. The norm-grafting process not only situates South Korea within the broader architecture of global governance standards but also consolidates the legal and normative basis underpinning domestic policy reform. Furthermore, the externality of canonical international norms helps alleviate both internal politics and external power pressures. The sustained elevation of cybersecurity on the national security agenda via crisis-oriented discourse, coupled with the legitimacy empowerment, lowers the frictional costs of strategic transformation. This dynamic facilitates a paradigmatic momentum in the evolution of contemporary South Korean cybersecurity strategy.

3.1. Hypersecuritisation in Cyberspace

Securitisation theory was developed by the scholarly community commonly known as the Copenhagen School in the

1990s. Since then, the theory has been subjected to extensive debate, refinement, and applied across military, political, societal, economic, and environment domains. It provides a rationale for illustrating how ordinary issues can be deliberately reframed as security-related matters, along with its reverse process – desecuritisation – whereby they are intentionally desecuritised and returned to the status of non-security [25].

Hypersecuritisation is an emerging theoretical concept, situated within security epistemology as a sub-concept addressing securitisation processes [26]. It was initially introduced by Barry Buzan as part of his configuration of security studies paradigms. The notion was later systematically operationalised by Lene Hansen in the field of digital security, and experientially applied by Helen Nissenbaum within the online privacy governance. These fundamental contributions have established hypersecuritisation as a critical analytical instrument for exploring cybersecurity affairs [27]. Hypersecuritisation offers a fundamental framework for understanding how cyberspace catastrophe imaginaries are constructed. It functions through mechanisms that instrumentally amplify the perceived severity and immediacy of security threats by deploying hypothetical narratives rooted in apocalyptic or doomsday scenarios, thereby inflating risks well beyond their actual likelihood [28]. In discursive practice, actors typically highlight the potentially devastating consequences of sudden cybersecurity incidents, particularly their capacity to paralyse core information systems integral to critical infrastructure, most notably in the financial and military sectors. Such dramatisation portrays cyber threats as possessing the capacity to precipitate mass systemic collapse across the prevailing political and socio-economic orders [29].

In comparison with other categorical concepts, *pan-securitisation* is driven by a widespread emphasis on horizontal tendencies, resulting in the incorporation of a wide array of non-security issues into the securitisation process [30]. Pan-securitisation not only blurs the boundary between security and non-security but also leads to an abnormal broadening of security agenda. By contrast, *over-securitisation* is manifested vertically through the deep reconstitution of specific issues within a hierarchical structure, such as infectious disease prevention and control in global public health [31]. By binding a single issue to particular actors within a premise securitisation schema, the issue is artificially elevated, functioning as power amplification.

While conceptually related to the aforementioned models, hypersecuritisation presents variations in its core characteristics.

First, hypersecuritisation advances the prioritisation of cybersecurity within policy agendas by discursively anchoring it to national security memorandums. It relies on analogical reasoning, whereby the potential consequences of cyberattacks are assessed, referencing the physical destruction caused by conventional armed conflict. The discourse of 'cyberwarfare' frames high-intensity conflicts as actions capable of generating material devastation, granting cyberspace a strategic significance equivalent to traditional military-spatial domains [32]. By establishing a symbolic linkage between cyberattacks in virtual space and tangible physical damage, hypersecuritisation portrays cyber threats as existential in nature, depicting characteristics of classical warfare [33]. In doing so, it shapes the perception of domestic audience and reinforces the urgency of securitised responses. Second, hypersecuritisation underscores a lens for interpreting the evolving profile of cybersecurity by constructing the strategic role of cyber infrastructure as the 'security nexus'. It focusses on how a single cybersecurity rift can trigger cascading effects that jeopardise multiple security referent objects [34]. Drawing on the offence-defence dynamics among cyberspace actors, there exists a structural resemblance to physical terrorism: malicious actors possess an inherent asymmetrical advantage, enabling them to conduct high-impact operations with minimal entry barriers. Although technological iterations have strengthened defensive capacities, they have exacerbated hyperconnectivity, giving rise to novel vulnerabilities [35]. This contradictory interplay renders the postures among cyberspace actors highly fluid and imparts non-linearity to security outcomes. Third, the rapid proliferation of emerging technologies like high-performance computing and artificial intelligence (AI) highlight the underdevelopment of universal norms governing cyberspace behaviour [36]. This regulatory gap has produced a lack of institutional mechanisms and precedents for coping actual incidents, leaving considerable ambiguity in crisis responsiveness. Ad hoc crisis management thus becomes the default feedback option fostering expectations among stakeholders for the progressive strengthening of cybersecurity measures. In the absence of binding norms, the emergency responses of individual states may serve as de facto models for others with limited cybersecurity experience, providing a fragmented basis for the domestically rationalised narrative of cyberspace hypersecuritisation.

Hansen and Nissenbaum [27] further argue that hypersecuritisation in cyberspace has spawn to distinct 'everyday security practice' and the technification. The former entails mobilising the public to engage in cybersecurity efforts and embedding hypersecuritised

imaginaries into digital practices of daily life, thereby garnering societal endorsement for securitisation discourses and the corresponding countermeasures. The latter pertains to the predominance of technical actors; whereby cyber professionals become the dominant agents fortifying the credibility of security narratives through the application of cyber-technology and the deployment of technological expertise. Technification frames cybersecurity as a domain ostensibly contingent upon hierarchical and specialised technical knowledge, and the supposition by the presumption of political and normative neutrality [37]. This article contends that the securitisation unfolding at the dimension of everyday-security-practices and technification reinforces security actor's motivation and accelerates the broader trajectory of securitisation. Through mechanisms of discursive internalisation, it enhances audience receptivity, thereby (re-)facilitating the diffusion and entrenchment of hypersecuritisation.

When examining the evolution of South Korea's cybersecurity strategy, it reveals that a cluster of early, high-visibility incidents – initiated from the 2009 DDoS attack that crashed major financial websites, followed by the 2013 'DarkSeoul' operation targeting critical institutions, and the 2014 cyber intrusion affecting hydro and nuclear power facilities – collectively functioned as pivotal catalysts propelling the country's progressive hypersecuritisation of cyberspace, a trajectory that is amenable to empirical substantiation.

3.2. Norm-Grafting: The Politics of Legitimacy

Scholars have observed that security appeals function as potent instruments of political mobilisation, contributing to the process of legitimisation. In practice, legitimacy manifests multilevel roles. Domestically, it undergirds a state's capacity to cultivate political identification among its citizens. Internationally, legitimacy shapes strategic responsiveness of states in transnational interactions, particularly in their diplomatic engagement with major powers. By incorporating normative dimensions, this article introduces the analytical concept of norm-grafting to interpret the tactics states employ in pursuit of comprehensive legitimacy. It further elucidates the contextual judgements and systematic considerations underlying strategic choices.

'Grafting' is originally a horticultural technique that denotes surgical joining of tissues from two distinct plants to form their coalescence into a single physiological unit. The process involves uniting a *scion* (the aerial portion) with a *rootstock* (the root system), thereby

enabling integration of vascular systems and combination of advantageous traits, such as fruit quality, disease resistance, and stress tolerance [38]. Political science scholars pioneered the application of grafting as a conceptual metaphor, employing it to interrogate the dialectics of transnational order formation as manifested in institutional praxis [39]. In this usage, grafting underscores the fusion and recombination of concepts and practices. As elaborated, grafting constitutes a dynamic process distinguished by repeatability, adaptability, and the capacity for selective absorption, transformation, and substitution of pre-existing paradigms. This generates complex outcomes wherein normative systems, cognitive frameworks, policy architectures, and implementation modalities intermingle, co-evolve, and undergo continuous innovation. Complementing this perspective, Mejri et al. [40] contend that successful grafting requires effective absorption and integration of grafted knowledge systems and relational networks into the cognitive framework of the grafting actor. Crucially, the grafted knowledge must be intelligible to and accepted by relevant stakeholders, encompassing cultural cognition, institutional norms, and specialised expertise originating from the '*graftee*' – external actors capable of transmitting experiential knowledge or network-based resources.

Drawing upon the botanical origin, the metaphor of grafting in social science entails not only the examination of heterogeneous ideas and institutional templates that serve as the grafting foundation (analogous to the rootstock) but crucially, the analysis of inter-subjective relations and power configurations that shape the grafting process (paralleling the ecological environment in plant grafting). Grafting represents the materialisation of normative politics. It does not occur in a vacuum but unfolds within a dynamic arena of contestation between dominant and emergent norms. The process reveals the pluralistic nature of international norms, underscoring the dominant and subordinate position of certain actors within the global order, along with their inherent potential for agentive manifestation [41]. To make this translational move explicit, the following matrix (Table 1) delineates the core logics, mechanisms, and objectives of grafting in biological origin, compared with its normative application in social science, elucidating how the notions of compatibility and integration traverse these contexts to underwrite legitimacy-seeking strategies.

A broader theoretical understanding is particularly salient for analysing how normatively dependent actors navigate the global state dynamics. Focussing on middle-power state actors exemplified by

Table 1. Comparative Framework of Norm-Grafting: From Biology to Normative Politics.

Dimension	Botanical/grafting	Social-scientific/norm-grafting
Ontology of units	Scion + rootstock	External norms + domestic frameworks
Causal logic	Compatibility → Vascular integration → Stable phenotype	Norm fit → Institutional absorption → Legitimisation → Routinised practices
Mechanisms	Cambium Alignment → Callus → Xylem-phloem link	Selection → Translation → Recombination-internalisation
Driving objectives	Yield, vigor, disease resistance	Comprehensive legitimacy, policy effectiveness, international recognition
Power and asymmetry	Implicit in cultivation choices	Major power agendas, global agenda-setting, resource dependency

Source: Author's elaboration.

South Korea, this article adopts the process-relational interpretation of grafting outlined above – highlighting both structural constraints and agential creativity – to advance the concept of norm-grafting, describing scenarios of a state with relatively limited discursive power, seeks to expropriate the authoritative content embedded in international norms through selective adaptation and reinterpretation, thereby converting imported normative authority into exportable governance templates. From this operationalisable premise, the state strives to bolster the legitimacy of strategic policy transitions – mitigating domestic controversies while evading international scrutiny or intervention. Within the grafting metaphor, norm-grafting can manifest in both state-led discursive constructions (the 'scion' of new normative claims) and its concrete policy practices (the 'rootstock' of the pre-existing institutional frameworks) [42]. South Korea exhibits a proficiency in deploying norm-grafting. By leveraging established institutionalised normative resources, Seoul strengthens the legitimacy of its own policy initiatives. This approach proves particularly consequential in cybersecurity governance, where norm-grafting assumes critical importance during phases of significant policy realignment by fulfilling the key functions.

First, norm-grafting facilitates a dual process of legitimisation: the internal reconstruction of threat perception and the external consolidation of policy support. In the cognitive sphere, under hypersecuritisation – where threats are presumed to be highly destructive and policies lack established precedents, norm-grafting functions by elucidating the applicability of the existing norms to novel challenges (e.g. applying data protection norms to the domain of

AI security). This defines the nature of emerging threats and furnishes legitimate strategies, alleviating ontological insecurity associated with unknown risks while reducing resistance towards transformation. At global level, the selection of norms is constrained by structural factors. Universality refers to the invocation of internationally recognised norms (such as the Cybercrime Convention), which not only signals a state's commitment to upholding the existing order, but also expands its policy space – actions framed as efforts to preserve order are more readily legitimised [43]. Selectivity unveils the tendency of states to graft norms advanced by ideologically aligned powerful actors (such as South Korea's adherence to the US-led 'Norms of Responsible State Behavior in Cyberspace'), thereby constructing shared identity narratives and gaining international tolerance for policy adjustments [44].

Second, given that international cybersecurity norms remain in evolutionary, norm-grafting addresses the challenge of shaping normative trajectories amid the uncertainty of incomplete rule codification. At the core of norm-grafting lies the strategic appropriation of authoritative norms. Through cooperative engagements, states clarify the substantive content of norms, accumulate rule-making power, and counterbalance rivalries in the international system. Simultaneously, by participating in norm formation, they expand interpretive and operational latitude within the normative structure. These dynamics foster favourable environments for subsequent, ambitious policy recalibrations, ultimately forming a self-reinforcing norm-grafting close-loop.

3.3. An Integrated Analytical Framework

The notion of hypersecuritisation and norm-grafting constitute strategic paradigms congregated defining the evolution of South Korea's cybersecurity strategy. Hypersecuritisation encodes the uncertainty surrounding cybersecurity landscape, framing the cross-domain, unprecedented nature of threats, and amplifying the sense of urgency among targeted audiences. Principal agents – sub-state actors, such as political elites, administrative institutions, academic communities, and mass media – translate specialised technical concerns into tangible public anxieties via routine discursive practices. This mechanism reflects the dominant pathway through which hypersecuritisation unfolds in South Korea's cyberspace. By contrast, norm-grafting emphasises the legitimation of strategic transformation through the interpretation, bridging, and mutually constructed external normative frameworks. South Korea has actively shaped societal acceptance of 'extraordinary measures'

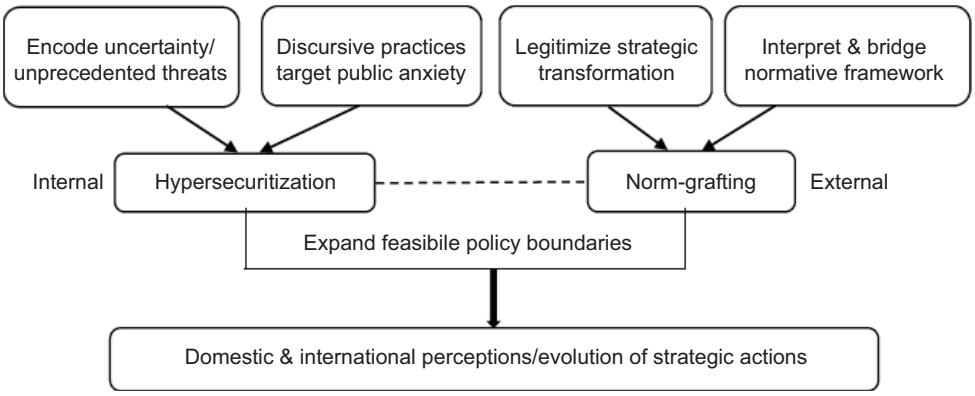

Figure 1. Systematic model of hypersecuritisation–norm-grafting dynamics. *Source*: Author's illustration.

within cybersecurity domain. Normatively, grafting facilitates the shift from a defensive inclination to a proactive and relatively offensive strategic attitude. Politically, it incrementally broadens the boundaries of feasible cybersecurity policy change, expanding the scope of operational space. This section develops an analytical framework that systematically incorporates hypersecuritisation and norm-grafting as key theoretical variables to logicalise the dynamics of South Korea's cybersecurity strategy (Figure 1). By exploring the synergistic effects of the functions, this approach underscores the collaborative impact on domestic and international perceptions of cybersecurity transformation – an understanding critical for informing the future trajectory of the country's policy actions.

4. Pathways and Policy Logic of South Korea's Cybersecurity Transformation

Since the 2010s, South Korea's foreign and security policies have undergone a consequential recalibration. In the realm of middle-power diplomacy, Seoul has pursued strategies linking Lee Myung-bak's New Asia Initiative, Park Geun-hye's Eurasia Initiative, and the co-founding of the middle-power governance grouping – MIKTA – to deepen global governance engagement [45]. On security, from the 2011 National Cyber Security Master Plan to the 2022 National Security Strategy, the country codified strengthened deterrence and proactive response to counter growing cyberattacks and safeguard societal information infrastructures. Consequently, cybersecurity agendas have articulated as a pivotal policy lever through which traditional middle powers exercise strategic agency and normative leadership. By coupling

hypersecuritisation to foreground the gravity and urgency of cyber threats with norm-grafting to consolidate the legitimacy of the evolving strategic rim, South Korea has not only facilitated domestic policy transition but also furnished enabling conditions for the outward projection and diffusion of its governance approaches.

4.1. Hypersecuritisation: The Construction of Security Hermeneutics

The hypersecuritisation discourse of South Korea's cybersecurity is manifested in the symbolic and institutional elevation of cyberspace to an empowered status equivalent to the traditional physical domains of defence. Such elevation creates the political space necessary to confer cybersecurity with governance capacity echelon and normative applicability comparable with conventional security issues. In the early stage of strategic transformation, the Ministry of National Defense focussed on developing cyber counterstrike capabilities, designating cyberspace as a future 'battlefield', [46] and incorporating cyber warfare into the military system and joint operational framework to enhance deterrence against North Korea. The 2014 National Defense White Paper stated that the North commanded approximately 6000 cyber warfare personnel [11], a figure far higher than previous assessments highlighting the magnitude of cyber threat. Correspondingly, during the initial incident cluster, official statements and media-facing narratives recurrently highlighted systemic disruption and the vulnerability of critical institutions, reinforcing a crisis imaginary through which cybersecurity could be prioritised within the security agenda. This discursive elevation, in turn, widened the feasible space for institutional consolidation and policy codification – visible in the subsequent strengthening of interagency cyber governance coordination and the production of countermeasure roadmaps and strategic planning documents. Notably, the 2009 National Cyber Crisis Comprehensive Countermeasures and the National Cybersecurity Master Plan formulated in the aftermath of the Nonghyup Bank attack, became South Korea's roadmaps for cyber defence. The former introduced integrated initiatives, such as DDoS 'cyber shelters', while the latter articulated the long-term approach to clarify the responsibilities and coordination of involved government agencies [47]. Nevertheless, both remained limited in mandate and fell short of a comprehensive strategic vision. Policy efforts have continued to evolve in tandem with the changing cyber threats. Since 2021, the annual National Cybersecurity White Paper has reflected a maturation, specifically elaborating governance, incident response, industry development, data protection, and international cooperation [48].

The elevation of security capacity echelons also signifies the geopolitical extension in confronting challenges posed by North Korea, China, and anarchic hackers. Notably, North Korea has been repeatedly accused of advanced persistent threat (APT) operations against South Korean institutions, heightening societal awareness of state-level cyber warfare [49]. In response, the government has emphasised the strategic vantage point of national cybersecurity, clearly delineated the governance responsibilities of relevant units, including military, diplomacy, and intelligence, promoting both functional differentiation and interdepartmental collaboration – an approach emblematic of hypersecuritisation. In the period of Lee Myung-bak administration, the 'micro-government' reform agenda – prompted by institutional consolidation – culminated in the establishment of the Korea Internet and Security Agency (KISA) under the Ministry of Science and ICT (MSICT) through the merger of the National Internet Development Agency and the IT International Cooperation Agency. Concurrently, the Ministry of National Defense established the Cyber Command [46]. In 2015, the National Security Office (NSO) created the post of Secretary to the President for Cybersecurity to coordinate inter-ministerial cybersecurity decision-making under presidential authority [50]. Within the aforementioned architecture, the Blue House (Korean presidential office) emerged as the central node of cybersecurity governance: the Chief of Future Strategy oversaw day-to-day activities, the NSO directed management of crisis events, and the National Intelligence Service (NIS) – the principal intelligence agency reporting directly to the president – handled information and security affairs related to national security. Collectively, these institutions addressed the country's increasingly complex cyber threats [51], as shown in Figure 2.

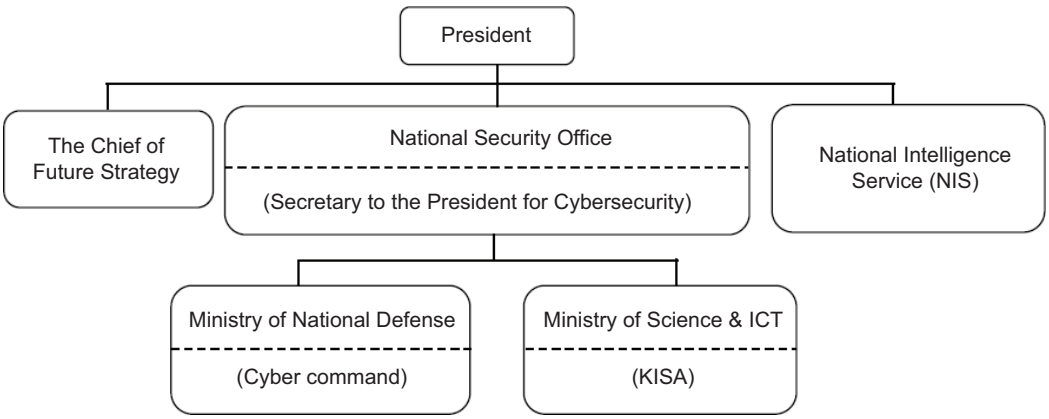

Figure 2. Structural configuration of cybersecurity governance in South Korea. *Source*: [24, 50, 61].

Finally, political elites have adeptly employed major social events as discursive leverage fulcrums to heighten the salience of cybersecurity, implementing the everyday -security -practices of hypersecuritisation. Following the 'Olympic Destroyer' malware attack during the PyeongChang Winter Olympics, the president convened an interagency crisis meeting and expedited the introduction of the subsequent National Cybersecurity Strategy. The incident also illustrates, as North Korea has been widely perceived as the suspect in cyberattacks against critical infrastructure, South Korean public opinion increasingly frames such attacks as acts of 'war', accompanies by calls for retaliation in both cyber and traditional security domains [52]. Since 2020, North Korea's continued intrusions and cryptocurrency thefts – including the Lazarus' attack on the Ronin Network – has deepened societal awareness of cybersecurity [53]. By 2024, the release of the Second National Cybersecurity Strategy and the National Cybersecurity Basic Plan marked a decisive turn towards proactive cyber defence, reflecting a forward-leaning, threat-pre-emptive orientation.

4.2. Norm-Grafting: The Mechanisms of Legitimacy Justification

Amid the intensifying hypersecuritisation discourse surrounding the regional and global cybersecurity climate, South Korea employs the sequential norm-grafting strategies drawing from domestic and international normative frameworks across temporal spans, to legitimise its policy transformations.

Phase I – Absorption and adaption: The foundational phase of norm-grafting rooted in establishing the contextual basis for norm absorption and the ensuing adaption, configuring structural and relational prerequisites for effective grafting. In South Korea's incipient norm absorption process, the superpower has been the principal driving force guiding the enhancement of South Korea's cybersecurity capabilities to sustain broader US geostrategic interests in its Asia-Pacific alliance network. Aligned with security imperatives, the United States has consistently urged accelerated cybersecurity infrastructure development and the implementation of associated measures. Within global normative ecosystems, soft law instruments leading by the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn 1.0) and *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* have become widely referenced standards with the Euro-American sphere exhibiting pronounced interpretive dominance [54]. Expansive readings of *Article 2(4)* (prohibition on the use of force) and *Article 51* (right

of self-defence) of the UN Charter have extended traditional jus ad bellum norms into cyberspace, incorporating a pre-emptive logic that justifies unilateral cyber-defence actions [55]. Expectations from global allies serve as a clear setting shaping South Korea's normative selections. For norm adaptation, South Korea affirms the applicability of the existing international law to cyberspace governance, particularly self-defence provisions under the UN Charter and the US–ROK Mutual Defense Treaty, reflecting the extended logic of a reinforced cybersecurity gradient. In parallel, domestic stakeholders have actively endorsed evolving cybersecurity posture through legislative deliberations and academic discourse production amid ongoing digital norm migration [56].

Despite enduring upheavals, the US–ROK alliance has neither collapsed nor faced existential crisis. It has demonstrated remarkable adaptability to the evolving regional landscape, transitioning from a patron-client, threat-based model to a comprehensive, reciprocal alliance anchored in shared interests and multifaceted agendas [57]. Recent geopolitics, including the Russia–Ukraine war and the Israel–Palestine conflict, has heightened South Korean perceptions of a deteriorating global order, eroded the peacetime assumptions, and stimulated calls for a more assertive role within the alliance. Long-term polling further indicates enduring public support: over 90% affirm the alliance's necessity and nearly 90% express optimism regarding the great power presence on the Peninsula [58]. The absorption and adaptation of cybersecurity norms consolidate South Korea's role as a strategic pivot within the security alliance while enhancing its stature as a global middle power and a regional power by leveraging Western-dominated discourse [59]. Scholars note that a weaker ally can 'insure' its alliance by attending to the stronger partner's security agendas [60], thereby adding legitimacy to specific policies the partner holds.

Phase II – Accommodation and engraftment: The subsequent stage of norm-grafting involves the assimilation and operational integration of norms. South Korea exemplifies a nuanced trajectory, where norm accommodation and engraftment are shaped by its authoritarian legacy and democratic institutionalisation. During the authoritarian period of the 20th century, large-scale intelligence operations under military government executing in the absence of oversight, culminated in governance crises and widespread human rights violations. The Korean Central Intelligence Agency (KCIA), established following the May 16 coup in 1961 as the predecessor of the National Intelligence Service [61], functioned as an

instrument of state coercion, creating an information-controlled, surveillance-repression apparatus that provoked profound societal backlash. This historical trauma crystallised into a deep-seated distrust of unchecked state power and generated enduring normative sensitivity towards the domestic expansion of security authority in the cyber domain, and an impetus for the institutionalisation of stringent intelligence scrutiny and regulatory mechanisms in the 1980s. Following democratisation, state–citizen relations have required striking a careful balance between security and freedom in cyberspace. Policymakers thus became attentive not only to threat mitigation but also to the political and legal risks of legitimising intrusive surveillance practices or emergency powers through escalatory security framings.

In the advent of information age, while Western states increasingly prioritise offensive cyber capabilities [62], South Korea has adhered a distinctly conservative approach. The existing legislation explicitly impedes the military from developing offensive cyber weapons and imposes limitations on the permissible scope of proactive cybersecurity measures, reflecting a domestically rooted preference for legal restraint and oversight that conditions how external cyber norms are adopted and operationalised, signalling a selective adaptation of external legal paradigms that remain anchored in internal political realities. Norm accommodation has been pursued through deliberate ambiguity, incremental reform, and consensus-driven policy discourse – collating foreign concepts and domestic institutional constraints into legal revisions. Confronted with cybersecurity risks shaped by subjective perceptions and objective vulnerabilities, South Korea refrains from wholesale adoption of offensive doctrines. Instead, it filters international norms through the prism of historical experience and constitutional principles, maintaining vagueness in the characterisation of cyber incidents. These elements are deliberately contextualised and localised, consistent with the strategy of norm accommodation [63]. Such ambiguity embodies a contingent interpretation of whether cyberattacks amount to a 'use of force', softening contentious normative implications by blurring the technical specifics, advancing innovative yet domestically palatable security concepts and pre-emptively containing domestic securitisation dynamics by mitigating political friction and societal resistance [64]. This cautious stance is exemplified by the responses to high-profile cyberattacks attributed to the North – including the 'July 7 DDoS attacks' in 2009, the 2011 Nonghyup Bank incident, and operations linked to state-sponsored hacker groups such as the Lazarus Group – where South Korean issued public condemnations

but avoided directly framing them as acts of war or invoking military responses. Importantly, such restrained rhetoric can be read as a discursive governance instrument: it acknowledges external threats while avoiding escalatory labels that might broaden domestic mandates for exceptional measures, thereby sustaining the democratised equilibrium between freedom and security. In this respect, the restrained rhetoric also underscores a preference for addressing cyber conflicts through diplomatic or criminal justice channels, rather than military avenues. Despite ongoing debate over whether cyberattacks fall under the UN self-defence clause, South Korea has yet to claim that any incident constitutes an armed attack warranting military response, reflecting the strategic ambiguity and non-consensus within international legal regime regarding the threshold for such determinations.

In 2019, the Moon Jae-in administration released the first National Cybersecurity Strategy. Emphasising deterrence, systemic resilience, and international cooperation in cyberspace, the strategy adopted a predominantly defence-oriented posture. Stemming from the pro-North posture of the administration, the document, for the first time, refrained from designating North Korea as an enemy, instead advocating the diversification of foreign policy beyond a single state focus [46]. This marked a departure from the previous attributive posture that had exclusively targeted the North, redirecting the emphasis towards strengthening the overall domestic capabilities in responding to cyberattacks. It simultaneously mirrors the Moon administration's overarching political attitude towards North Korea. Notably, the strategy maintained a non-committal stance regarding circumstances under which cyberattacks might trigger military obligations, although the concept of proactive defence was acknowledged. Conversely, in 2024, the Yoon Suk-yeol administration unveiled the second National Cybersecurity Strategy, signalling the discernible shift in cybersecurity norm engraftment – from a defensive logic towards an offensive orientation. It explicitly delineates threat actors and affirms commitment to adopting active stance countering malicious cyber activities. The government also reiterates South Korea's responsibility as a global pivotal state to fulfil obligations and enhance international cooperation as a 'responsible user of cyberspace [65]'. The outlined strategic tasks place emphasis on fortifying offensive cyber capabilities. Nonetheless, this emerging norm engraftment phase reveals preferences for pragmatism, flexibility and institutional caution, avoiding rigid legal commitments that might bind future policy maneuvering, minimising escalation risks in cybersecurity tensions while retaining diplomatic latitude.

In the conventional literature, middle powers are understood with recurring traits and by their moderate capabilities, which incline them towards preserving the existing order. They are sufficiently endowed to hold considerable stakes in the international system, yet lack the power to absorb systemic turmoil independently [66]. Consequently, they often emerge as natural advocates of institutionalisation, as formal rules enhance predictability and introduce mechanisms of accountability [67]. In sum, while accommodation entails selective adaptation of external norms, engraftment involves deeper institutionalisation and subjective alignment. This hybrid process highlights the intricate nature of norm-grafting, particularly for middle powers such as South Korea, as they navigate the reconciliation of global normative pressures with entrenched domestic socio-political legacies in the field of cybersecurity governance.

Phase III – Re-architecting and norm projection: At present, cyberspace remains without universally accepted norms governing state behaviour and lacks a fully established regulatory regime. As international society seeks greater stability and predictability, competing normative claims emerge from actors with diverse strategic interests and ideological orientations. On one side, a broadly 'Western' normative package that privileges an open, global, and interoperable internet and the multi-stakeholder model of cyberspace governance, emphasising principles such as due diligence, transparency, and proportionate responses to malicious cyber activities. The opposing side is the alternative framework associated with authoritarian discourses of 'cyber/digital sovereignty', which foregrounds state primacy in domestic cyberspace governance, non-interference, and the legitimacy of extensive state regulatory authority over cross-border data flows, critical information infrastructure, and internet content [68]. For states, norm rearchitecting denotes the deliberate reinterpretation, modification, and recombination of the existing norms to accommodate shifting national interests and geopolitical realities. Norm re-architecting functions on interrelated fronts. Externally, it enables states to embed preferred normative expectations into emerging regimes, thereby exerting moral and legal constraints on others while consolidating their discursive standing in the global arena. Internally, norm rearchitecting serves as a mechanism of interpretive authority by aligning with the prevailing international frameworks while selectively integrating localised values and priorities. Once institutionalised, such authority projects into domestic sphere, providing justification and legitimacy for policy recalibration.

South Korea's cybersecurity strategy increasingly demonstrates a model of norm re-architecting. Rather than focussing solely on global performance in security-related digital technologies, Seoul prioritises cooperation with the US-led coalition while proactively engaging in the norm construction governing cyberspace. This orientation reflects its ambition to secure a competitive edge in the global contest over norm-setting authority. Simultaneously, it leverages integration into Western normative frameworks as a catalyst for recalibrating and evolving its cybersecurity strategy. The approach advances interrelated objectives: first, reshaping national identity by positioning South Korea as a norm-constructive middle-power and responsible stakeholder in global digital governance regime [69]. Second, elevating the country's international stature in the global hierarchy of cybersecurity by augmenting discursive power – strategically complementing and resonating with advancement in sectors such as 5G/6G and semiconductors [70].

On the other hand, the nascent character of the international normative schema governing cyberspace leaves considerable scope for proactive norm construction, ultimately culminating in the final phase of norm-grafting – norm projection – analogous not only to the vigorous flourishing of a plant in the wake of successful grafting, but also to the spread of its propagated traits beyond the original site of cultivation. South Korea's engagement in global governance is often framed through the connotation of 'peace public diplomacy' [71] and its broader middle-power strategy. Within this lens, the country has adopted the re-architecting approach aimed at reinforcing the Western discursive hegemony while advancing its own normative interests by promoting normative coordination and institutional alignment. These efforts are most visible in the pattern of norm projection across regional and interregional landscapes. In 2015, South Korea established the Global Cybersecurity Center for Development (GCCD) to enhance expertise and facilitate knowledge-sharing. By 2020, the network encompassed over 59 governmental and non-governmental institutions from 45 countries. Additionally, the government financed the 'Combatting Cybercrime: Tools and Capacity Building for Emerging Economies' project of the World Bank [72].

In another vein, as a core middle-power actor, globally, South Korea has advanced cyber diplomacy with other key middle powers. In 2021, South Korea and Australia announced the establishment of a Comprehensive Strategic Partnership (CSP), and signed the Memorandum of Understanding (MoU) on Cyber and Critical Technology Cooperation (CACT) in the same year. The MoU defined

cyber and critical technologies as 'current and emerging technologies with the capacity to significantly enhance, or pose risks to, the two countries' prosperity, social cohesion, and national security', [73] while underscoring the vision of 'an open, secure, stable, accessible, and peaceful cyberspace' aimed at fostering prosperity, safeguarding national security, and promoting international order. This development highlights the centrality of 'shared values' in shaping bilateral approaches to cybersecurity governance. Regionally, beyond the alliance with the United States, South Korea positions itself as an infrastructural and normative hub within the evolving Indo-Pacific cybersecurity architecture [74]. As transboundary cyber threats – from ransomware attacks to state-backed disinformation – intensify, the imperative for regulatory harmonisation and operational coordination has grown. In response, South Korea's Indo-Pacific strategy institutionalises its commitment to strengthening cyber capacities across the Association of Southeast Asian Nations (ASEAN) member states [75]. Leveraging the robust digital economy and adherence to democratic norms, South Korea acts as a strategic bridge between advanced industrial democracies and developing countries in shaping regional cybersecurity governance. Norm projection is central to this role, enabling South Korea to disseminate cybersecurity values, institutional preferences, and virtual governance models throughout Southeast Asia. Initiatives such as the Korea–ASEAN Defense Cooperation Framework and the participation in the ASEAN Regional Forum (ARF) Inter-Sessional Meeting on ICT Security exemplify this practice. These engagements advance regional capacity-building, norm development, and cyber intelligence-sharing while projecting South Korea's cybersecurity principles into multilateral frameworks. Through vehicles such as the ASEAN–Korea Cooperation Fund (AKCF), Seoul has invested in digital development initiatives emphasising cyber hygiene and infrastructure resilience [76]. Collectively, these efforts contribute to the regionalisation of strategic cybersecurity governance and reconfigure South Korea's identity from a reactive security actor to a proactive norm entrepreneur and architect of the Indo-Pacific's emerging cyber order.

Compared with the primary analytical frameworks of hypersecuritisation and norm-grafting developed in this article, the notion of security communities represents a comparatively mature construct in the realm of international politics. As Adler and Barnett [77] argue, security communities foreground the roles of power and knowledge in reshaping the environment of interstate interaction: power enables leading states to assume leadership and attract broader participation, while the circulation of shared

knowledge fosters stable and predictable expectations regarding state behaviour. Relative to the concluding phase of norm-grafting, as global and regional actors increasingly converge in the technical and knowledgeable approaches to cyberspace capacity-building through grafting processes of re-architecting and projection, their cooperative efforts against cyber threats tend to yield more tangible effects, thereby establishing the foundational conditions for the emergence of 'cybersecurity communities'.

5. Implications and Conclusion

This article employs concepts of hypersecuritisation and norm-grafting to systematically examine their generative logic within the evolving spectrum of South Korea's cybersecurity strategies. Its academic novelty lies in applying hypersecuritisation theory to explain the formation and metamorphosis of cybersecurity strategic configuration; while utilising the botanical concept of norm-grafting to dissect the gradual legitimisation process underpinning the country's shift towards a more offensive-oriented security posture in cyberspace. Responding to the dynamic cyberspace environment, South Korea has amplified societal perception of cybersecurity threats by presupposing worst-case scenarios. At policy level, the country has aligned the developmental trajectory of international cybersecurity norms, adopting a progressive norm-grafting strategy that facilitates the incremental optimisation of legislation and policies. From the perspective of realism in international politics, the convergence of these elements reflects the inherent complexities of cybersecurity strategy transformation. It is noteworthy that an offensive-oriented cybersecurity strategy remains a politically contentious issue. In contrast, constrained by multiple limitations, South Korea's strategic efforts will likely to hinge on constructing the hypersecuritised narrative of cyberspace to reinforce the structural legitimacy of policy shift, mitigate domestic and international criticism, and sustain the long-term institutionalisation and development.

Furthermore, the rationales of hypersecuritisation and norm-grafting have shown signs of diffusion into adjacent fields. For instance, in light of North Korea's persistent cyber threats, there is a growing societal perception in South Korea that national security faces severe and prolonged menace [78], accompanied by rising public support for enhancing defence capabilities and the US–ROK alliance. Irrespective of shifts in the domestic political configuration, the expanding trend is likely to prompt significant adjustments

in South Korea's overall national security strategy. Accordingly, concerning how South Korea advances and consolidates this trajectory through hypersecuritisation discourse construction and norm-grafting policy actions, as well as evaluating its impact on cybersecurity norm practices, provides a viable alternative governance paradigm for other states – particularly state clusters of middle powers as a meaningful reference – at both regional and global levels. Moreover, the case study reveals a comparative orientation, suggesting that further refinement and extension of hypersecuritisation and norm-grafting theories could facilitate macro-level analysis of how different countries position themselves on the global cybersecurity landscape. These insights hold considerable relevance for fostering efforts to advance cyberspace security, resilience, and sustainability.

References

[1] Y.D. Kim, J.S. Kim, K.H. Lee, "Major issues of the national cyber security system in South Korea, and its future direction," *The Korean Journal of Defense Analysis*, vol. 25, no. 4, pp. 435–455, 2013, doi: 10.22883/kjda.2013.25.4.001.

[2] S. Khalifeh, "The evolution of warfare from conventional to a digital battlefield: An analysis of cyber technology and artificial intelligence in the Lebanese-Israel conflicts," *Defense and Security Studies*, vol. 6, no. 1, pp. 91–102, 2025, doi: 10.37868/dss.v6.id285.

[3] M. Ernst, S. Lee, "Countering cyber asymmetry on the Korean Peninsula: South Korea's defense against cyber attacks from authoritarian states," *Journal for Intelligence, Propaganda and Security Studie*s, vol. 15, no. 1, pp. 165–179, 2021.

[4] N. Shafqat, A. Masood, "Comparative analysis of various national cyber security strategies," *International Journal of Computer Science and Information Security*, vol. 14, no. 1, pp. 129–136, 2016.

[5] N. Chang, "Cybersecurity threats, counter strategies and South Korea's cyber strategy," *National Security and Strategy*, vol. 19, no.2, pp. 1–36, 2019. [Online]. Available: http://www.riia.re.kr/upload/bbs/BBSA05/202010/F20201027548753.pdf. [Accessed: Oct. 30, 2025].

[6] G. Boulet, M. Reiterer, R.P. Pardo, *Cybersecurity policy in the EU and South Korea from consultation to action: Theoretical and comparative perspectives*. Cham: Palgrave Macmillan, 2022.

[7] K. Socquet-Clerc, S. Khoo, Fitriani, M.A. Gomez, N.V. Lam, *Cybersecurity governance in Southeast Asia*, Thematic SSG Brief, Geneva Centre for Security Sector Governance, 2023. [Online]. Available: https://www.dcaf.ch/sites/default/files/publications/documents/Cybersecurity_Governance_in_Southeast_Asia_Thematic_Brief.pdf. [Accessed: Mar. 30, 2024].

[8] J.E. Platte, "Defending forward on the Korean Peninsula," *The Cyber Defense Review*, vol. 5, no. 1, pp. 75–92, 2020.

[9] M.B. Manantan, S. Kwon, *Strengthening ROK-US critical technologies cooperation: Progress and path forward*, The Pacific Forum, 2023. [Online]. Available: https://pacforum.org/wp-content/uploads/2023/01/Pacific-Forum-George-Mason-Uni-ROK-Publication-July-2023_Pages.pdf. [Accessed: Mar. 2, 2026].

[10] J.E. Platte, "Bilateral alliances in an interconnected cyber world: cyber deterrence and operational control in the US Indo-Pacific Strategy," *Asian Perspective*, vol. 47, no. 1, pp. 75–99, 2023, doi: 10.1353/apr.2023.0003.

[11] N. Kshetri, "Cyber warfare in the Korean Peninsula: Asymmetries and strategic responses," *East Asia*, vol. 31, no. 3, pp. 183–201, 2014, doi: 10.1007/s12140-014-9215-1.

[12] J. Park, N. Rowe, M. Cisneros, "South Korea's options in responding to North Korean cyberattacks," *Journal of Information Warfare*, vol. 15, no. 4, pp. 86–99, 2016.

[13] H. Boo, K. Kang, "An assessment of North Korean cyber threats and the Republic of Korea's policy responses: An update," *Defense Strategy & Assessment Journal*, vol. 9, no. 1, pp. 79–98, 2019.

[14] S. Bae, Y. You, K. Kim, S.J. Kim, "Cyberattack severity assessment (CASA) and national response matrix (NRM) in Korea," *The Journal of East Asian Affairs*, vol. 34, no. 2, pp. 67–98, 2021.

[15] A. Chapnick, "The Canadian middle power myth," *International Journal: Canada's Journal of Global Policy Analysis*, vol. 55, no. 2, pp. 188–206, 2000, doi: 10.1177/002070200005500202.

[16] R. Mason, "Small-state aspirations to middle powerhood: The cases of Qatar and the UAE," in *Unfulfilled Aspirations: Middle Power Politics in the Middle East*, A. Saouli, Ed. Oxford: Oxford University Press, 2020, pp. 157–182, doi: 10.1093/oso/9780197521885.003.0009.

[17] S. Kim, *Policy recommendation for South Korea's middle power diplomacy: Cyber security*, EAI MPDI Policy Recommendation Working Paper, 2015.

[18] R.P. Pardo, T. Kim, M. Ernst, K. Sung, R. Villa, *Beyond traditional security: South Korea's positioning towards the cyber, energy, maritime and trade security domains*, KF-VUB Korea Chair Report, 2020.

[19] U. Heo, "The US-ROK alliance: Security implications of the South Korea-US free trade agreement," *Pacific Focus*, vol. 23, no. 3, pp. 365–381, 2008, doi: 10.1111/j.1976-5118.2008.00018.x.

[20] A. Asaki, "The U.S.-ROK alliance and the ROK's choices: Considerations on extended deterrence and nuclear armament," *NIDS Commentary*, no. 358, pp. 1–11, 2024, [Online]. Available: https://www.nids.mod.go.jp/english/publication/commentary/pdf/commentary358e.pdf. [Accessed: Feb. 12, 2025].

[21] S.A. Snyder, "The U.S.-South Korea alliance and space cooperation," *Asian Security*, vol. 21, no. 1, pp. 30–41, 2025, doi: 10.1080/14799855.2025.2483165.

[22] K.B. Park, S. Chae, H. Lee, "Korea's cybersecurity regulations and enforcement related to security incidents," *International Cybersecurity Law Review*, vol. 2, no. 1, pp. 47–55, 2021, doi: 10.1365/s43439-021-00028-5.

[23] S. Kim, "Roles and limitations of middle powers in shaping global cyber governance," *The International Spectator*, vol. 57, no. 3, pp. 31–47, 2022, doi: 10.1080/03932729.2022.2097807.

[24] S. Paz, L. Tejerina, D. Kang, *National Cybersecurity Law, Governance, and Infrastructure in the Republic of Korea*. Washington, DC: Inter-American Development Bank (IDB), 2024, doi: 10.18235/0012876.

[25] D. Aydindag, "Copenhagen school and securitization of cyberspace in Turkey," *Propósitos y Representaciones*, vol. 9, no. 1, Art. no. e850, 2021, doi: 10.20511/pyr2021.v9nSPE1.850.

[26] M. Andžāns, "Small powers, geopolitical crisis and hypersecuritisation: Latvia and the effects of Russia's second war in Ukraine," *Central European Journal of International and Security Studies*, vol. 17, no. 2, pp. 138–162, 2023, doi: 10.51870/RNCC4980.

[27] L. Hansen, H. Nissenbaum, "Digital disaster, cyber security, and the Copenhagen school," *International Studies Quarterly*, vol. 53, no. 4, pp. 1155–1175, 2009, doi: 10.1111/j.1468-2478.2009.00572.x.

[28] M.A. Gomez, C. Whyte, "Breaking the myth of cyber doom: Securitization and normalization of novel threats," *International Studies Quarterly*, vol. 65, no. 4, pp. 1137–1150, 2021, doi: 10.1093/isq/sqab034.

[29] S. Backman, T. Stevens, "Cyber risk logics and their implications for cybersecurity," *International Affairs*, vol. 100, no. 6, pp. 2441–2460, 2024, doi: 10.1093/ia/iiae236.

[30] Z. Liu, "The 'pan-securitization' of the EU's connectivity policy and China–EU cooperation," in *The Belt and Road Initiative: Past, Present, Future*, X. Gao, K. Gouliamos, Z. Liu, C. Kassimeris, Eds. Cham: Palgrave Macmillan, 2025, pp. 259–278. doi: 10.1007/978-981-96-1128-7.

[31] C. Wenham, "The oversecuritization of global health: Changing the terms of debate," *International Affairs*, vol. 95, no. 5, pp. 1093–1110, 2019, doi: 10.1093/ia/iiz170.

[32] J. Nye Jr., "Nuclear lessons for cyber security?" *Strategic Studies Quarterly*, vol. 5, no. 4, pp. 18–38, 2011. [Online]. Available: http://nrs.harvard.edu/urn-3:HUL.InstRepos:8052146 [Accessed: Mar. 23, 2026].

[33] R. Miller, D. Kuehl, I. Lachow, "Cyber war: Issues in attack and defense," *Joint Force Quarterly*, vol. 61, no. 2, pp. 18–23, 2011.

[34] R.J. Deibert, "Circuits of power: Security in the internet environment," in *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, J.N. Rosenau, J.P. Singh, Eds. Albany, NY: State University of New York, 2002, pp. 115–142, doi: 10.1353/book4485.

[35] M. Lacy, D. Prince, "Securitization and the global politics of cybersecurity," *Global Discourse*, vol. 8, no. 1, pp. 100–115, 2018, doi: 10.1080/23269995.2017.1415082.

[36] International Telecommunication Union, *Global Cybersecurity Index 2024*, 5th Edition, Geneva: ITU Publications, 2024. [Online]. Available: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024. [Accessed: Mar. 9, 2026].

[37] M.D. Cavelty, F.J. Egloff, "Hyper-securitization, everyday security practice and technification: Cyber-security logics in Switzerland," *Swiss Political Science Review*, vol. 27, no. 1, pp. 139–149, 2021, doi: 10.1111/spsr.12433.

[38] J. Lee, M. Oda, "Grafting of herbaceous vegetable and ornamental crops," *Horticultural Reviews*, vol. 28, 2010, doi: 10.1002/9780470650851.ch2.

[39] A. Acharya, "How ideas spread: Whose norms matter? Norm localization and institutional change in Asian regionalism," *International Organization*, vol. 58, no. 2, pp. 239–275, 2004, doi: 10.1017/S0020818304582024.

[40] K. Mejri, J.A. MacVaugh, D. Tsagdis, "Knowledge configurations of small- and medium-sized knowledge-intensive firms in a developing economy: A knowledge-based view of business-to-business internationalization," *Industrial Marketing Management*, vol. 71, pp. 160–170, 2018, doi: 10.1016/j.indmarman.2017.12.018.

[41] A. Simons, L. Rethel, "Subordinated agency and the grafting of sustainable finance regulations in Southeast Asia," *International Affairs*, vol. 101, no. 5, pp. 1679–1699, 2025, doi: 10.1093/ia/iiaf058.

[42] J. Lai, L. Rethel, K. Steiner, "Conceptualizing dynamic challenges to global financial diffusion: Islamic finance and the grafting of Sukuk," *Review of International Political Economy*, vol. 24, no. 6, pp. 958–979, 2017, doi: 10.1080/09692290.2017.1373689.

[43] P. Popovic, "Redefining the status quo state: Collective support, order-maintenance, and self-restraint," *International Politics*, 2024, doi: 10.1057/s41311-024-00635-z.

[44] S.E. Goddard, *When Right Makes Might: Rising Powers and World Order*. Ithaca, NY: Cornell University Press, 2018.

[45] G. Baba, B. Engin, "MIKTA: A functioning product of 'new' middle power-ism?," *Review of International Law & Politics*, vol. 11, no. 42, pp. 1–40, 2015.

[46] M. Pradhan, *Cyber insecurity in South Korea: Decoding cybersecurity vulnerabilities*, SSPC Issue Brief, 2024. [Online]. Available: https://sspconline.org/sites/default/files/2024-10/IB_SSPC-Pradhan-Sept-2024.pdf. [Accessed: Dec. 31, 2025].

[47] P. Roshan, "The evolving cyber landscape: Capabilities and cyber diplomatic efforts of Korean Peninsula," *Journal of Regional Studies Review*, vol. 4, no. 1, pp. 1–14, 2025, doi: 10.62843/jrsr/2025.4a045.

[48] J. Jung, V. Wang, Y. Kim, "South Korean cyber security threats, governance measures, and implications for SMEs," *Korean Journal of Industry Security*, vol. 10, no. 1, pp. 81–109, 2020, doi: 10.33388/kais.2020.10.1.081.

[49] M. Chung, J. Lim, H. Kwon, "A study on North Korea's cyber attacks and countermeasures," *Journal of Information Technology Services*, vol. 15, no. 1, pp. 67–79, 2016, doi: 10.9716/KITS.2016.15.1.067.

[50] S.J. Kim, S. Bae, "Korean policies of cybersecurity and data resilience," in *The Korean Way with Data: How the World's Most Wired Country Is Forging a Third Way*, E.A. Feigenbaum, M.R. Nelson, Eds. Washington, DC: Carnegie Endowment for International Peace, 2021, pp. 39–60.

[51] H. Ebert, L. Groenendaal,. *Cyber Resilience and Diplomacy in the Republic of Korea: Prospects for EU Cooperation*, EU Cyber Direct, 2020. [Online]. Available: https://eucyberdirect.eu/research/cyber-resilience-and-diplomacy-in-the-republic-of-korea. [Accessed: Dec. 12, 2025].

[52] K. Park, S. Park, J.I. James, "A Case Study of the 2016 Korean Cyber Command Compromise," 2017, doi: 10.48550/arXiv.1711.04500.

[53] K. Zellers, "Hacked! North Korea's billion-dollar crypto heisting scheme," *The Penn State Journal of Law & International* Affairs, vol. 12, no. 2, pp. 261–302, 2024, [Online]. Available: https://insight.dickinsonlaw.psu.edu/jlia/vol12/iss2/10. [Accessed: Apr. 21, 2026].

[54] E.T. Jensen, "The Tallinn manual 2.0: Highlights and insights," *Georgetown Journal of International Law*, vol. 48, pp. 736–778, 2017. [Online]. Available: https://ssrn.com/abstract=2932110. [Accessed: Jan. 25, 2025].

[55] M.C. Waxman, "Cyber-attacks and the use of force: Back to the future of Article 2(4)," *Yale Journal of International Law*, vol. 36, pp. 421–459, 2011. [Online]. Available: https://scholarship.law.columbia.edu/faculty_scholarship/1653. [Accessed: Jan. 17, 2026].

[56] J. Jun, S. Kim, "US-South Korea cyber cooperation: Towards the higher-hanging fruits," *Korea Policy*, vol. 2, no. 2, pp. 150–171, 2024.

[57] T. Xu, "U.S.-ROK alliance: Looking toward the future," in *SAIS U.S.-Korea Yearbook 2007*, The U.S.-Korea Institute at the Paul H. Nitze School of Advanced International Studies (SAIS), Johns Hopkins University, 2007, pp. 19–29, [Online]. Available: https://usakoreainstitute.org/wp-content/uploads/2010/05/YB07-Chapt2.pdf. [Accessed: Mar. 2, 2026].

[58] K. Friedhoff, *While positive toward US alliance, South Koreans want to counter Trump's demands on host-nation support*, Chicago Council on Global Affairs, 2019. [Online]. Available: https://globalaffairs.org/sites/default/files/2020-11/191214_korean_attitudes_on_host_nation_support_final_.pdf. [Accessed: Dec. 18, 2024].

[59] S. Kim, "Cyber security and middle power diplomacy: A network perspective," *The Korean Journal of International Studies*, vol. 12, no. 2, pp. 323–352, 2014, doi: 10.14731/kjis.2014.12.12.2.323.

[60] J.J. Park, E. Tan, "South Korea's investment in the U.S.-ROK alliance," *Asia Policy*, vol. 17, no. 4, pp. 101–122, 2022, doi: 10.1353/ASP.2022.0060.

[61] S. Cho, *National Cybersecurity Organisation: Republic of Korea*, National Cybersecurity Governance Series. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2022. [Online]. Available: https://afyonluoglu.org/PublicWebFiles/NATO/2022-NCS-Korea.pdf. [Accessed: Oct. 3, 2023].

[62] A. Tumkevič, "Uncertain security community: Building western cyber-security order," *Journal of Information Warfare*, vol. 17, no. 1, pp. 74–86, 2018.

[63] I.Y. Min, "The rise and fall of nuclear phase-out in South Korea: German model and the dynamics of policy learning," *The Pacific Review*, vol. 39, no. 1, pp. 208–230, 2026, doi: 10.1080/09512748.2025.2554364.

[64] M.C. Libicki, "The strategic uses of ambiguity in cyberspace," *Military and Strategic Affairs*, vol. 3, no. 3, pp. 3–10, 2011.

[65] S.J. Kim, "ROK's new national cybersecurity strategy and its implications," *Institute for National Security Strategy (INSS) Issue Brief*, vol. 106, no. 3, pp. 1–7, 2024. [Online]. Available: https://www.inss.re.kr/upload/bbs/BBSA05/202404/F20240425131646465.pdf. [Accessed: Jan. 16, 2026].

[66] R. Cox, "Middlepowermanship, Japan, and future world order," in *Approaches to World Order*, R. Cox, T. Sinclair, Eds. Cambridge: Cambridge University Press, 1996, pp. 241–243, doi: 10.1017/CBO9780511607905.

[67] A. Hurrell, "Some reflections on the role of intermediate powers," *Paths to Power: Foreign Policy Strategies of Intermediate States*, no. 244, pp. 1–11, 2000.

[68] N. Katagiri, "Why international law and norms do little in preventing non-state cyber attacks," *Journal of Cybersecurity*, vol. 7, no. 1, Art. no. tyab009, 2021, doi: 10.1093/cybsec/tyab009.

[69] T. Murphy, S. Nagy, "Middle power cyber security cooperation in the Indo-Pacific: An analysis through the lens of Neo-middle power diplomacy," *Journal of Intelligence, Conflict, and Warfare*, vol. 7, no. 1, pp. 1–24, 2024, doi: 10.21810/jicw.v7i1.6454.

[70] C.M. Lee, *Building a New U.S.-Korea Technology Alliance: Strategies and Policies in an Entangled World*. Washington, DC: Carnegie Endowment for International Peace, 2024.

[71] Y.Y. Cho, "Public diplomacy and South Korea's strategies," *The Korean Journal of International Studies*, vol. 10, no. 2, pp. 275–296, 2012.

[72] World Bank, United Nations, *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*. Washington, D.C.: World Bank Group, 2017. [Online]. Available: http://documents.worldbank.org/curated/en/355401535144740611. [Accessed: Apr. 11, 2026].

[73] J. Lim, "Australia-Korea cyber diplomacy – Advancing bilateral cooperation on cyber and critical technologies," *Yonsei Journal of International Studies*, 2022. [Online]. Available: https://theyonseijournal.com/wp-content/uploads/2022/07/YJIS-2022-spring_summer-online-Australia-Korea-Cyber-Diplomacy.pdf. [Accessed: Feb. 17, 2026].

[74] D. Cho, "Cyber resilience in South Korea," *Asia Policy*, vol. 20, no. 2, pp. 46–59, 2025, doi: 10.1353/asp.2025.a960042.

[75] W. Kharisma, A.M. Mantong, "Becoming middle power: Challenges and opportunities of ASEAN-ROK security cooperation," in *Navigating Uncharted Waters: Security Cooperation between ROK and ASEAN*, A.W. Mantong, W. Kharisma, Eds. Washington, DC: Centre for Strategic and International Studies (CSIS), 2022, pp. 169–180.

[76] ASEAN–ROK Cooperation Fund, *AKCF Annual Report 2022*, 2022. [Online]. Available: https://www.aseanrokfund.com/lib/upload/files/resources/AKCF_Annual_Report_20221.pdf. [Accessed: Aug. 7, 2024].

[77] E. Adler, M. Barnett, *Security Communities*. Cambridge: Cambridge University Press, 1998, doi: 10.1017/CBO9780511598661.

[78] H. Yun, "Reassessing North Korea's evolving cyber threat and South Korea's countermeasures," *North Korean Review*, vol. 21, no. 1, pp. 70–91, 2025, https://www.jstor.org/stable/27393827. [Accessed: May. 23, 2026].

[79] K.H. Yeh, "Middle powers in the space development: A comparative analysis of South Korea and Indonesia," *Balkan Social Science Review*, vol. 21, pp. 143–167, 2023, doi: 10.46763/BSSR2321143y.