Journal of Political Science and International Relations Studies
ISSN: 3078-7319
DOI: https://doi.org/10.61784/jpsr3020

INTERNATIONAL SECURITY GOVERNANCE IN AN ERA OF DEGLOBALIZATION: RISK DIFFUSION AND INSTITUTIONAL RESPONSES UNDER GREAT POWER COMPETITION

QianAn Wang
Department of Global Processes, Lomonosov Moscow State University, Moscow 119991, Russia.
Corresponding Email: wqajbc12345678@163.com

Abstract: Deglobalization pressures are increasingly reshaping the governance ecology of international security by tightening geopolitical blocs, politicizing interdependence, and fragmenting institutional authority across issue areas. This article conceptualizes international security governance in the deglobalization era as a problem of cross domain risk diffusion under conditions of intensified great power competition, where security threats and disruptions propagate through supply chains, finance, information infrastructure, and regional security complexes, while institutional responses struggle to maintain coherence, legitimacy, and enforceability. Building on risk governance and global security governance perspectives, the study develops an analytical framework that links three mechanisms of risk diffusion, namely interdependence channel transmission, domain coupling through technology and infrastructure, and strategic amplification through competitive statecraft, to three families of institutional response, namely multilateral orchestration, minilateral security cooperation, and hybrid governance arrangements. The argument is illustrated through comparative discussions of the Indo Pacific maritime cyber domain, crisis governance in global health emergencies, proliferation risks in the Middle East and North Africa, and emerging regional theatres such as the Arctic.
Keywords: Deglobalization; International security governance; Great power competition; Risk diffusion; Institutional response; Regional security

1 INTRODUCTION

Deglobalization is increasingly invoked to describe a reorientation of cross border economic and technological ties toward security centered logics, yet the more analytically consequential change lies in how risk travels through interdependence under intensified great power competition and how institutions struggle to respond with credible governance. Rather than a simple retreat from globalization, contemporary deglobalization dynamics are often characterized by selective decoupling, geopolitical rivalry over standards and infrastructures, and the securitization of trade and investment choices, which together reshape the operating environment of international security governance. This environment amplifies the strategic meaning of interdependence because supply chains, energy systems, and digital networks simultaneously constitute channels of prosperity and vectors of vulnerability, making risk diffusion a central feature of national and regional security agendas[1-3].

Within this context, international security governance can be understood as the attempt to manage cross domain risk diffusion while maintaining institutional legitimacy and enforcement capacity in a system that is increasingly fragmented and contested. Risk governance scholarship emphasizes that modern risk problems involve uncertainty, complexity, and contested values, so governance must encompass not only technical mitigation but also coordination, communication, and legitimacy producing procedures[4]. At the international level, these requirements are complicated by the distributive consequences of security choices and by the presence of strategic competition that incentivizes unilateral advantage seeking and forum shopping. The enforcement problem is therefore not peripheral but foundational, because the capacity of rules to shape behavior depends on credible monitoring and sanctioning arrangements that can withstand political contestation[5]. In practice, institutional fragmentation and uneven compliance often generate governance gaps precisely where risk diffusion is fastest, producing conditions in which national security strategies harden while regional security dilemmas intensify[6].

The article situates these dynamics within the renewed prominence of great power competition as a structuring condition for security order. Contemporary rivalry is frequently associated with acceleration in technology, information operations, and strategic narratives, which alters the pace of escalation and the scope of security agendas beyond traditional military domains[7]. The return of competitive power politics also creates power vacuums and contested zones where institutional authority is weak and external actors seek influence through security cooperation, proxy engagement, or economic leverage[8]. At the same time, competition is not only material but also ideological and interpretive, shaping how actors define threats and evaluate the legitimacy of institutional responses[9]. These shifts are particularly salient for regional security governance, because regional theatres often become the sites where systemic rivalry meets localized disputes, multiplying pathways for risk diffusion.

A major implication of deglobalization era rivalry is the coupling of maritime security with economic security and strategic access, especially in regions where sea lanes, ports, and undersea infrastructures connect military mobility with commercial resilience. The Indo Pacific exemplifies this coupling, where maritime cybersecurity vulnerabilities create pathways for disruption that can cascade from digital networks into shipping logistics and critical infrastructure operations[10]. The European theatre similarly highlights the strategic value of maritime access and overseas basing as instruments through which great powers manage presence, deterrence, and crisis response[11]. These dynamics suggest that maritime security governance must be analyzed not only through conventional military balances but also through the governance of cyber risk, infrastructure protection, and rules for access under competitive conditions[12].

Cybersecurity more broadly has become a governance frontier because it diffuses risks across sectors, blurs the boundaries between peacetime competition and crisis, and raises persistent challenges of attribution and escalation control. Efforts to expand cyber mission spaces and to scale security cooperation can enhance defensive capacity among partners, yet they may also deepen bloc segmentation and reduce incentives for inclusive norm building[13]. Leadership and organizational capacity in cyber governance are therefore increasingly treated as strategic assets, shaping how states coordinate internally and externally in an environment where operational tempo and threat surfaces expand[14]. From a governance perspective, the crucial question is how to build institutional interoperability and crisis management mechanisms when competition encourages secrecy, rapid innovation, and the politicization of technical standards[5].

Deglobalization also intensifies the strategic salience of non traditional security risks that propagate through societal systems and generate secondary effects on political stability, legitimacy, and regional order. Global health emergencies demonstrate how risk diffusion combines biological threats with governance challenges in public communication, resource allocation, and cross border coordination, all of which can become politicized amid competitive narratives[15]. Hybrid responses in crisis settings further show that governance frequently depends on combinations of state authority, international coordination, and localized implementation, especially where institutional capacity is uneven[16]. Climate related security governance illustrates an additional dimension of fragmentation, where institutional and ideational disagreements over securitization, responsibility, and appropriate policy instruments complicate collective action despite the transboundary nature of climate risks[10].

Regional security complexes in the Middle East and adjacent regions reveal how great power competition amplifies proliferation and escalation risks while complicating institutional responses. Proliferation concerns in MENA are shaped by regional rivalries and external alignments, making risk governance inseparable from the strategic calculations of major powers and regional actors[17]. The Persian Gulf security complex similarly demonstrates how rapprochement and rivalry coexist under competitive external pressures, producing shifting threat perceptions and governance opportunities that remain fragile[18]. The intersection of geoeconomic interests, security commitments, and institutional contestation is also visible in cases where external actors navigate security risks alongside economic corridors and influence strategies, as illustrated by China’s engagement with Afghanistan under conditions of competition[19].

Emerging theatres such as the Arctic further underscore how deglobalization does not reduce geopolitical contestation but can relocate and diversify it across new geographies and issue linkages. The Arctic is increasingly portrayed as a domain where strategic access, resource competition, and military posture interact with governance gaps and environmental constraints, making it a salient case for understanding how risk diffusion and institutional response evolve at the margins of established security architectures[20]. Strategic planning in this theatre also highlights the institutional tension between national security strategies and broader cooperative governance needs, particularly when competition encourages positional bargaining over rules and presence[21]. In parallel, deep sea resources and rare earth related dynamics in East Asia show how maritime conflict management, technological change, and resource security can become tightly coupled, creating new pathways for risk diffusion across economic and security domains[22].

Against this backdrop, the article advances a central argument: international security governance in the deglobalization era is best analyzed as a problem of cross domain risk diffusion under great power competition, where institutional responses are constrained by fragmentation, enforcement deficits, and competing visions of order. Competing conceptions of durable security order, including visions associated with China and other major actors, shape expectations about institutional design, legitimacy, and the balance between sovereignty and multilateral coordination[23]. At the global level, the United Nations Security Council remains a focal institution for multilateral security governance, yet its capacity is conditioned by the strategic environment and by the bargaining patterns of major powers[24]. At the regional level, organizations such as ASEAN face persistent challenges in maintaining centrality and cohesion amid external competition, illustrating how regional governance can be both necessary and structurally constrained[25].

The study’s contribution is therefore twofold. Conceptually, it integrates risk governance with global security governance to specify how interdependence channels, technology driven domain coupling, and strategic amplification jointly produce risk diffusion, and how multilateral, minilateral, and hybrid governance arrangements respond with varying degrees of effectiveness[4]. Empirically and analytically, it foregrounds national and regional security by emphasizing theatres where risk diffusion is most acute and institutional responses are most contested, including the Indo Pacific maritime cyber domain, MENA proliferation dynamics, and emerging arenas such as the Arctic[8,20]. This framing positions deglobalization not as a deterministic decline of governance but as a reconfiguration that demands institutionally plural yet interoperable security governance architectures capable of managing diffusion, enforcing commitments, and reducing escalation risks under competitive conditions[26].

2 DEGLOBALIZATION AND THE SECURITY GOVERNANCE PROBLEM

Deglobalization in security governance should be treated less as a collapse of international connectivity and more as a transformation in the political meaning and management of interdependence. In this view, the defining shift is that cross border ties in production, finance, technology, and infrastructure are increasingly assessed through vulnerability and leverage, rather than efficiency and mutual gain. The resulting governance problem is not that states become isolated, but that they remain structurally connected while actively redesigning connections to reduce exposure, enhance autonomy, and create bargaining advantages. This reconfiguration is consistent with arguments that the language of deglobalization can obscure the continued depth of transnational corporate and economic linkages, even as geopolitical rivalries reorganize the incentives that previously supported relatively open regimes of exchange[1]. The security implications of this transformation are especially visible in domains where interdependence is both indispensable and securitized, such as supply chains and economic statecraft under competitive conditions[2]. When national security is conceptualized as resilience against coercion and disruption, governance shifts toward risk management across networks rather than mere threat balancing across borders[3].

A central consequence is that risk diffusion becomes faster, more multidirectional, and harder to contain within single issue regimes. Governance institutions face rising complexity because shocks in one domain quickly propagate through shared infrastructures and interlinked policy spaces, including energy markets, food systems, maritime logistics, and digital platforms. In East Asia and other interdependence dense regions, economic security is not only a policy objective but also a governance constraint, because the same networks that generate prosperity can transmit instability and political pressure[11]. Trade and welfare disputes further interact with power competition, turning economic relations into arenas where distributional conflicts are interpreted as strategic contests and therefore subject to securitized policy responses[27]. In this environment, deglobalization intensifies the governance challenge by coupling the management of external risks with internal political expectations of control, autonomy, and protection, which can reduce tolerance for multilateral compromise.

The security governance problem is also institutional, because fragmentation across venues and mandates increases precisely when cross domain coordination becomes most necessary. Even where organizations exist, their authority is often partial and contested, while their enforcement tools may be weak relative to the speed of risk diffusion. The enforcement dimension is critical because rules do not produce security outcomes merely by existing; they require monitoring, compliance incentives, and credible sanctioning, all of which are difficult to sustain amid geopolitical rivalry[5]. Deglobalization conditions amplify these difficulties because major powers have stronger incentives to interpret rules instrumentally and to relocate governance to preferred forums. This creates governance gaps and overlapping authorities that can allow strategic actors to exploit ambiguity. The dynamics of diffusion in complex international society further suggest that power distribution and governance authority may shift in non linear ways, producing outcomes that are difficult to anticipate and therefore hard to govern through static institutional designs[6].

Great power competition deepens the problem by turning institutional arenas into sites of strategic signaling and contestation, rather than primarily cooperative problem solving. Competition can accelerate the pace of interaction across military, technological, and informational domains, reducing the time available for crisis management and increasing the risk that misperception or overreaction will spread across domains[7]. It can also produce power vacuums or contested zones where governance is thin, authority is disputed, and external influence becomes a tool of rivalry, thereby increasing instability risks at the regional level[8]. Ideational competition matters as well, because alternative worldviews shape how actors interpret threats, attribute responsibility, and decide whether multilateral procedures are legitimate or merely constraining[9]. Under these conditions, institutional effectiveness depends not only on formal design but also on whether key actors view the institution as compatible with their strategic objectives.

Deglobalization also shifts the center of gravity from global governance to regional security governance, because many of the most consequential diffusion pathways operate through regionally concentrated infrastructures, chokepoints, and security complexes. Regional organizations may be expected to act as stabilizers, yet they face intensified pressures to accommodate external rivalry while managing internal diversity. ASEAN illustrates this tension because it seeks to preserve centrality and autonomy, but it operates in a strategic environment where major power competition creates incentives for states to hedge, align selectively, or bypass regional mechanisms[25]. The governance challenge is compounded when non traditional security issues become entangled with geopolitics, as the evolving EU ASEAN relationship suggests in the context of China's rise and changing conceptions of non traditional security cooperation[28]. Where regional institutions cannot fully resolve competition, they often serve as arenas for managing exposure and reducing escalation risk rather than as sites of decisive enforcement.

Maritime security shows how deglobalization transforms governance by securitizing strategic access and linking it to economic resilience. Strategic access is no longer only a military question but also a governance problem of protecting sea lines of communication, undersea infrastructures, and port ecosystems that sustain national economic security. European debates over maritime security and overseas basing highlight how competition shapes access strategies and creates pressure for states to maintain presence and readiness, often through dispersed infrastructures and networked basing arrangements[11]. Similar dynamics are emphasized in discussions of European maritime security as a strategic access question under competition, which underscores how governance must integrate operational planning with broader institutional arrangements for cooperation and crisis management[12]. When access is securitized, institutional cooperation becomes more fragile because transparency and coordination can be perceived as vulnerabilities, even though the absence of coordination raises escalation and disruption risks.

The cyber domain intensifies these challenges because it amplifies diffusion and blurs the boundary between routine competition and crisis. Maritime cybersecurity vulnerabilities in the Indo Pacific illustrate how digital disruption can cascade into logistics failures, infrastructure downtime, and political pressures, while contested threat perceptions limit the willingness to share information and harmonize standards[10]. At the same time, coalitional approaches to expanding cyber mission space and security cooperation reflect an institutional response that prioritizes speed and interoperability among partners, while potentially increasing bloc differentiation and governance fragmentation[22]. Cyber leadership and organizational capacity are therefore treated as strategic resources, not merely administrative features, because they shape the ability to coordinate across agencies and allies under conditions of persistent contestation[14]. In deglobalization conditions, cyber governance becomes a core element of national and regional security governance because it influences both deterrence credibility and societal resilience.

Deglobalization also reinforces the linkage between crisis governance and strategic competition, particularly for global health and climate security. Health emergencies demonstrate that risk governance requires rapid coordination, resource mobilization, and public communication, yet the competitive context can politicize expertise and reduce trust, thereby weakening compliance and collective action. Disaster risk governance approaches highlight how national policy responses are shaped by governance structures and by the broader strategic environment, including the incentives to frame crisis responses in ways compatible with national security narratives[15]. Hybrid security governance in crisis contexts further suggests that effective response often depends on combining state authority with international coordination and local implementation capacity, especially where state capacity is uneven[16]. Climate security governance adds an additional layer because fragmentation is not only institutional but also ideational, meaning that actors disagree about how climate risks should be framed and governed, which can inhibit coherent security responses even when risks are transboundary and cumulative[10].

Regional security complexes in MENA provide a concentrated illustration of how deglobalization, rivalry, and diffusion interact through proliferation risks and strategic alignment patterns. Proliferation risk governance is shaped by local rivalries and by the involvement of external powers, which can both deter and incentivize escalation depending on alliance commitments and crisis dynamics[8]. The Persian Gulf security complex further demonstrates how rapprochement and rivalry coexist under great power competition, producing shifting threat perceptions that complicate stable institutionalization[18]. Geoeconomic and security risk navigation in Afghanistan indicates how infrastructure and economic corridor considerations become intertwined with security commitments and influence strategies, thereby intensifying diffusion risks across governance domains[19]. In such theatres, governance failures can be disproportionately costly because regional instability can spill into global energy and trade systems, reinforcing the systemic character of deglobalization era insecurity.

Finally, deglobalization complicates security governance by enabling both plural institutional visions and intensified competition over ordering. Competing conceptions of durable security order shape expectations about multilateralism, sovereignty, and enforcement, which in turn affect the feasibility of shared governance arrangements[23]. At the global level, the United Nations Security Council remains a critical focal institution, yet its multilateral strategy and effectiveness are conditioned by the constraints of great power competition and bargaining dynamics among major powers[24]. At the same time, the emergence of new theatres such as the Arctic shows how competition can relocate to domains where governance frameworks are thinner and operational incentives for presence and resource positioning are stronger, increasing the demand for institutions that can manage both access and restraint[20]. Strategic planning for the Arctic similarly underscores how national strategies can coexist with governance gaps, raising the risk that theatre specific competition will generate broader systemic friction[21]. The security governance problem under deglobalization is therefore best understood as the challenge of maintaining credible, interoperable governance across domains and regions while managing enforcement deficits and strategic contestation.

3 THEORETICAL ANCHORS: RISK GOVERNANCE AND GLOBAL SECURITY GOVERNANCE

This article anchors its explanation of security governance under deglobalization in two complementary theoretical traditions: risk governance and global security governance. The first clarifies how complex threats diffuse through interconnected systems under uncertainty, while the second specifies how international institutions attempt to organize authority, compliance, and collective action in security domains. Together, these lenses help explain why risk diffusion accelerates in an era of strategic rivalry, and why institutional responses are frequently partial, fragmented, and contested. Deglobalization does not eliminate interdependence, but it changes the political meaning of interdependence by reframing cross border ties as exposure to disruption and coercion. This shift strengthens the case for treating national security as resilience and risk management rather than only territorial defense[1]. The resulting governance problem is that vulnerability is produced within networks that no single actor controls, so security outcomes depend on coordination across public and private actors, across sectors, and across levels of governance[29]. The same environment also heightens strategic incentives to contest institutional rules and to shape the ordering of international relations, which makes risk governance inseparable from questions of authority and legitimacy[30].

Risk governance provides a conceptual vocabulary for analyzing threats characterized by uncertainty, complexity, and ambiguity. In this approach, governance is not limited to technical risk assessment and mitigation; it includes how societies define risk, allocate responsibility, communicate uncertainty, and select policy instruments that are viewed as legitimate. This perspective is especially relevant for security governance in the deglobalization era because many salient risks are systemic and cascading, meaning they propagate through infrastructures and markets rather than through conventional military pathways[4]. Systemic propagation is reinforced when supply chains and logistics systems become subject to competitive statecraft and strategic disruption, producing security externalities that spill beyond any single jurisdiction[2]. Trade politics further complicate risk governance because welfare effects and distributive conflicts are often interpreted through strategic lenses during great power competition, which can turn economic policy into security policy and thereby broaden the scope of securitization[27].

From a risk governance perspective, contemporary security challenges are increasingly cross domain, with feedback loops among cyber, maritime, energy, and societal systems. Maritime cybersecurity illustrates how risks diffuse across technical and operational layers, translating vulnerabilities in digital systems into disruptions in shipping, port operations, and strategic mobility[10]. Climate security governance illustrates another diffusion dynamic: environmental stressors generate indirect effects on livelihoods, migration pressures, and political stability, yet governance responses often fragment across institutions and competing ideas about what counts as security[10]. In the Pacific, the coupling of climate change and geopolitical competition intensifies the challenge because governance must address long horizon environmental risks while also navigating short horizon strategic rivalry[31]. Risk governance is therefore analytically useful because it foregrounds the mechanisms that translate hazards into political and security outcomes through exposure, vulnerability, and institutional capacity.

The utility of risk governance becomes clearer when applied to crisis episodes that reveal the institutional conditions of effective response. Disaster risk governance approaches highlight how policy responses depend on governance design and on the capacity to coordinate across agencies and levels of authority in real time[15]. Hybrid security governance in health crises further demonstrates that the locus of effective action often lies in institutional hybrids that combine state authority, international coordination, and local implementation networks, particularly where formal capacity is uneven[16]. These insights matter for national and regional security governance because deglobalization conditions increase pressure for rapid, sovereign centered action, even though many crises require cross border coordination to prevent escalation and diffusion. Risk governance thus provides a theoretical basis for evaluating whether institutional arrangements are capable of managing uncertainty, complexity, and distributional conflict while maintaining public legitimacy.

Global security governance complements risk governance by focusing on institutions, rules, and enforcement mechanisms through which security order is produced and contested. A key premise is that security governance is not only about cooperation but also about organizing authority over the use of force, the management of crises, and the regulation of security related behaviors across states and non state actors. The enforcement problem is central because even well designed rules are ineffective without credible mechanisms for monitoring, compliance, and sanctioning[5]. Under great power competition, enforcement becomes harder because major actors can resist or reinterpret constraints, leverage veto points, and shift governance to alternative forums. The diffusion of power in complex international society further implies that authority may disperse across multiple actors and venues, increasing the likelihood of overlapping mandates and strategic contestation[6]. Where institutions cannot deliver enforcement, governance often shifts toward informal coalitions, minilateral arrangements, or unilateral strategies that can reduce coordination burdens but may also deepen fragmentation.

The deglobalization era intensifies these governance dilemmas because the meaning of multilateralism itself becomes contested. The United Nations Security Council remains a focal arena for global security governance, yet its ability to act depends on the strategic environment and on the bargaining strategies of major powers[24]. Competing visions of international order also shape how states evaluate multilateral institutions and whether they prioritize sovereignty, hierarchy, or rule based constraints in security governance[23]. The revival of competitive power politics creates incentives to treat institutions as instruments of influence rather than as neutral coordinators, which can weaken legitimacy and reduce willingness to accept costly commitments. Ideational contestation is therefore not a peripheral factor but a structural feature of governance in great power competition, shaping threat framing and the perceived fairness of institutional procedures[9].

To bridge risk governance and global security governance, the article conceptualizes international security governance as the governance of diffusion. Diffusion refers to the movement of risks, shocks, and strategic effects across borders and across domains through shared infrastructures and interdependent systems. In this framing, governance effectiveness depends on whether institutions can interrupt harmful cascades, reduce exposure, and create credible commitment mechanisms under conditions of rivalry. The age of acceleration intensifies diffusion because technology and information operations increase the speed of interaction, reduce decision time, and expand the number of actors able to generate cross border effects[7]. Power vacuums further intensify diffusion by creating contested spaces where governance is weak and external actors compete for influence through security assistance, proxy dynamics, or strategic infrastructure[8]. These dynamics indicate that governance problems should not be reduced to regime design alone, but should include the capacity to manage time pressure, uncertainty, and escalating interdependence.

Regional security governance provides a practical arena in which the interaction of these theoretical anchors becomes visible. ASEAN's struggle to accommodate great power competition illustrates how regional institutions attempt to preserve autonomy and centrality while managing divergent member preferences and external pressures[25]. The EU's role as a multilateral security actor after Lisbon suggests that external governance instruments can support security objectives, yet such roles remain bounded by political cohesion and by the broader strategic environment. (The EU as a Multilateral Security Actor After Lisbon: Conceptual and Empirical Perspectives, 2013). The EU ASEAN relationship further illustrates how non traditional security concepts can provide a cooperation platform, but also how rising power dynamics reshape the scope and meaning of such cooperation[9]. These regional experiences underscore a general theoretical point: institutions may function less as enforcement machines and more as arenas for managing exposure, coordinating limited cooperation, and providing legitimacy for selective actions.

The risk governance lens also illuminates why certain security domains become focal points of diffusion and governance contestation. Maritime security and strategic access in Europe highlight how basing, presence, and sea lane protection become intertwined with institutional bargaining under competition[11]. Related arguments emphasize that strategic access is a governance problem because it requires coordination across allies, legal frameworks, and infrastructure protection policies under contested conditions[12]. Cybersecurity further intensifies the governance challenge because it expands the mission space and encourages security cooperation toolkits designed for interoperability, capacity building, and partner integration[26]. Such cooperation may increase resilience, but it can also contribute to bloc formation and institutional fragmentation if it is perceived as exclusionary or strategically directed[13]. Cyber leadership becomes a governance variable because the ability to coordinate across bureaucracies and alliances influences whether states can manage diffusion without escalating conflict[14].

Hard security risks remain central in the theoretical architecture because they interact with diffusion pathways and institutional constraints. Nuclear deterrence under disruptive technologies illustrates how strategic stability is challenged by new capabilities and by the need to integrate deterrence logic with governance mechanisms that reduce escalation risks[32]. Proliferation risks in MENA similarly show how regional dynamics interact with external competition, producing governance dilemmas where institutional responses must manage both strategic rivalry and localized security drivers[8]. Proxy war ethics introduces an additional governance dimension because partner selection, delegation, and norms of cooperation shape how states pursue influence and manage responsibility under competition[33]. These domains demonstrate that governance must address both intentional threats and systemic risks, integrating deterrence, ethics, and institutional oversight to manage diffusion.

Finally, the article's theoretical anchors extend to emerging theatres and to the governance of strategic resources. The Arctic is increasingly framed as a theatre of competition where governance gaps, environmental constraints, and strategic access interact, creating incentives for presence and positional bargaining that can generate broader systemic friction[20]. Arctic strategy debates further highlight how national planning can advance security objectives while leaving institutional coordination underdeveloped, thereby increasing the risk of misperception and escalation[21]. Deep sea resources and rare earth related dynamics in East Asia show how resource security intersects with maritime conflict management and technological change, generating diffusion pathways that link commercial competition with strategic posturing[22]. Energy governance remains an additional anchor because climate change and energy transitions reshape security priorities and create governance demands that interact with rivalry and institutional fragmentation[34]. These developments support the article's central theoretical claim: risk governance and global security governance jointly explain why deglobalization produces a security governance problem characterized by diffusion, fragmentation, and contested authority.

4 AN ANALYTICAL FRAMEWORK: FROM RISK DIFFUSION TO INSTITUTIONAL RESPONSE

This chapter proposes an analytical framework that connects risk diffusion to institutional response under deglobalization and great power competition. The core premise is that security governance is increasingly shaped by how risks travel through interdependence and how institutions filter, translate, and sometimes amplify those risks through rules, enforcement practices, and political bargaining. The framework treats deglobalization not as a simple decline in cross border exchange, but as a reconfiguration of interdependence through security centered logics that prioritize resilience, control over critical infrastructures, and strategic leverage[1]. This reconfiguration reshapes the context in which global and regional security governance operates, because it increases both the strategic value of connectivity and the political salience of vulnerabilities embedded in networks[11]. In this setting, risk diffusion becomes a practical problem of national and regional security, while institutional response becomes a problem of legitimacy and compliance in an increasingly fragmented order[6].

The first component of the framework specifies the sources and channels of risk diffusion. Following risk governance reasoning, diffusion is not merely the spread of a single hazard but the propagation of disruptions through coupled systems characterized by uncertainty and complexity[4]. Under deglobalization, supply chains become securitized and exposed to strategic interference, which increases the likelihood that localized shocks cascade across sectors and borders[2]. Economic competition further complicates diffusion because policy interventions in trade, investment, and technology standards may be justified as security measures while producing strategic externalities for other actors, thereby widening the range of disputes treated as security matters[27]. The framework therefore models diffusion as networked movement across infrastructures, markets, and information environments rather than as a purely territorial process.

The second component clarifies the domains in which diffusion is most likely to generate security consequences. The framework identifies domain coupling as a decisive condition, where risks in one domain translate into vulnerabilities in another due to shared infrastructures, dependencies, or governance overlaps. Maritime cybersecurity in the Indo Pacific illustrates this logic because digital vulnerabilities can disrupt shipping logistics and port operations, which in turn affect economic security and strategic mobility[10]. European maritime security and strategic access reveal a comparable coupling mechanism, where overseas basing, sea lane protection, and access management link deterrence with the governance of infrastructure and transit[11]. Related analysis of strategic access emphasizes that the contestation of maritime corridors and infrastructures can transform commercial connectivity into a security liability under competition[12]. Domain coupling thus functions as a bridging mechanism that translates technical vulnerabilities into national security exposure.

The third component centers on strategic amplification, which captures how great power competition increases the scale and speed of diffusion by changing incentives, threat perceptions, and operational tempo. The age of acceleration strengthens strategic amplification because technological change and information operations compress decision time and broaden the scope of contestation across domains[7]. Power vacuums and contested zones further intensify amplification by creating spaces where institutional authority is weak and external actors compete through security cooperation, proxy engagement, or coercive statecraft[8]. Ideological competition reinforces amplification because rival interpretations of threat and legitimacy affect whether institutional responses are viewed as neutral governance or as instruments of influence[9]. Within the framework, amplification is the political and strategic process that turns diffusion into a governance crisis by elevating risks into the realm of security priorities and escalation dynamics.

The fourth component specifies the institutional response repertoire. Institutional responses are not treated as a single mode of multilateral cooperation but as a spectrum ranging from global multilateralism to minilateral toolkits and hybrid governance. At the global level, multilateral institutions remain reference points for legitimacy and coordination, yet their performance is conditioned by rivalry and bargaining among major powers[24]. Competing visions of order shape how actors evaluate institutional design, including the acceptable balance between sovereignty, enforcement, and collective constraint[23]. At the regional level, institutional cohesion becomes a limiting factor, as seen in ASEAN's difficulties in sustaining centrality when external competition widens internal preference divergence[25]. For the EU, external governance and security actorness can broaden the toolset for response, but effectiveness depends on political unity and on the alignment of instruments with strategic realities. (The EU as a Multilateral Security Actor After Lisbon: Conceptual and Empirical Perspectives, 2013). The framework therefore conceptualizes institutional response as plural, layered, and often incomplete.

The fifth component addresses enforcement capacity as the pivot between institutional design and behavioral outcomes. In global security governance, enforcement is not an optional supplement but a foundational condition for credibility[5]. Deglobalization conditions can weaken enforcement because states are more likely to prioritize unilateral advantage, to contest monitoring arrangements, and to shift issues into forums that align with their preferences[30]. In such environments, institutional response may be expressed through partial compliance, selective implementation, and fragmented regimes that perform coordination functions without producing robust constraint[10]. The framework therefore treats enforcement deficits as a structural driver of governance gaps, especially in domains where diffusion is rapid and where attribution or verification is difficult, such as cyber and information operations.

To connect diffusion and response, the framework introduces a sequence of governance translation steps. First, diffusion produces exposure, meaning that actors perceive vulnerability due to dependencies and network position. Second, exposure becomes securitized, meaning that political actors frame the vulnerability as a security issue demanding exceptional priorities and resources. Third, securitized exposure triggers venue selection, in which states choose among global institutions, regional organizations, coalitions, and bilateral arrangements to pursue preferred responses. Fourth, chosen venues produce policy outputs, including standards, capacity building, sanctions, or operational cooperation. Fifth, outputs produce effects that depend on enforcement, legitimacy, and the strategic environment, which can either dampen diffusion or generate feedback loops that intensify rivalry. This sequence is consistent with the risk governance emphasis on the social processing of risk and the importance of legitimacy producing procedures[4]. It also aligns with the security governance emphasis on authority, compliance, and political contestation[5].

The framework's value can be illustrated across major security theatres that combine diffusion and contested response. In the Indo Pacific, small and middle powers navigate security dilemmas shaped by great power rivalry while attempting to protect maritime connectivity and critical infrastructures[35]. Cyber mission expansion and security cooperation initiatives may strengthen partner capacity, yet they can also reinforce bloc segmentation if institutional interoperability is pursued primarily within rival camps rather than across them[13]. Cyber leadership and organizational capacity become part of institutional response because they determine whether coordination is feasible across agencies and alliances under high tempo conditions[14]. In the Middle East, proliferation and escalation risks are intertwined with external alignments, which makes institutional response vulnerable to strategic bargaining and to competing threat perceptions[8]. The Persian Gulf security complex shows how rapprochement and rivalry coexist, creating fragile governance openings that may narrow when external competition intensifies[18]. These theatres illustrate the framework's claim that institutional response is conditioned by strategic amplification and enforcement constraints.

Non traditional security crises further demonstrate why hybrid governance is often necessary. Public health emergencies show that policy responses depend on risk governance design, cross sector coordination, and the ability to maintain legitimacy under uncertainty[15]. The Ebola response in Sierra Leone illustrates how hybrid security governance emerges when formal state capacity is insufficient, requiring combinations of international coordination and localized implementation to manage diffusion[16]. Climate security governance shows a parallel pattern of fragmentation, where institutional disagreements and competing ideas about securitization and responsibility complicate coherent response despite transboundary diffusion[10]. The framework therefore interprets hybrid governance as a pragmatic response to diffusion when neither purely national action nor fully multilateral coordination can deliver timely capacity and legitimacy.

Emerging theatres extend the framework's applicability to spaces where governance is under institutionalized. The Arctic is increasingly framed as a competitive arena where strategic access and resource concerns intersect with environmental constraints and governance gaps[20]. National strategies in this theatre indicate how institutional response may be shaped by positional bargaining, which risks generating security spirals in the absence of robust cooperative mechanisms[21]. Deep sea resource dynamics in East Asia show how resource security becomes entangled with maritime conflict management and technological competition, producing diffusion pathways that link commercial rivalry with strategic postures[22]. Energy governance under globalization and climate change adds an additional layer, because energy transitions and climate pressures interact with geopolitical competition to reshape security governance agendas[34]. These cases highlight that diffusion and response cannot be separated from geography, resource politics, and infrastructure dependence.

The framework ultimately proposes evaluative criteria for comparing institutional responses. First, damping capacity refers to whether responses reduce cascade potential by hardening critical nodes, diversifying dependencies, and improving crisis management. Second, interoperability refers to whether responses enable coordination across actors and domains without producing excessive fragmentation. Third, legitimacy refers to whether governance outputs are seen as procedurally fair and substantively appropriate by affected actors, which influences compliance. Fourth, enforcement credibility refers to whether monitoring and sanctioning arrangements can withstand contestation and strategic circumvention. These criteria integrate risk governance concerns about uncertainty management and legitimacy with security governance concerns about authority and compliance[4]. They also align with the claim that cooperation toolkits can be useful but may deepen fragmentation if they prioritize alignment over inclusivity and verification[26]. In the deglobalization era, the analytical challenge is therefore to identify which combinations of multilateral, regional, minilateral, and hybrid arrangements can achieve damping, interoperability, legitimacy, and enforcement under great power competition.

5 CONCLUSION

This article set out to clarify how international security governance is being reconfigured in an era commonly described as deglobalization, and to argue that the analytically decisive shift lies less in the aggregate contraction of cross border ties than in the changing pathways through which risk diffuses across tightly coupled domains under intensified great power competition. Rather than treating globalization and deglobalization as binary states, the analysis has emphasized the security consequences of selective decoupling, strategic competition over infrastructures and standards, and the securitization of economic and technological interdependence. In this setting, interdependence functions simultaneously as a channel of wealth creation and a vector of vulnerability, with supply chains, energy systems, maritime corridors, and digital networks enabling both resilience and disruption. The result is an operating environment in which national and regional security agendas increasingly converge on the management of cross domain spillovers, and in which governance effectiveness depends on the ability to reduce cascade risks without triggering escalatory dynamics that further fragment institutional order.

The article has advanced a central claim that security governance in this era should be analyzed through the linkage between risk diffusion and institutional response. Risk diffusion captures how shocks travel through networked interdependence and domain coupling, while institutional response captures how governance arrangements interpret, prioritize, and act upon those risks through rules, capabilities, and enforcement mechanisms. This linkage matters because deglobalization era competition tends to accelerate diffusion by politicizing technical systems and compressing decision time, while simultaneously constraining response by weakening trust, increasing forum shopping, and incentivizing unilateral advantage seeking. The conceptual integration of risk governance and global security governance therefore provides a more precise vocabulary for understanding why governance gaps often emerge where diffusion is fastest. It also clarifies why institutions that appear stable in formal design may become operationally fragile when enforcement capacity, legitimacy, and interoperability are stressed by rivalry.

A key conclusion is that domain coupling has become a defining condition of contemporary security governance. Maritime security cannot be understood solely as naval balance or territorial dispute management when cyber vulnerabilities, undersea infrastructures, port logistics, and commercial routing decisions can translate rapidly into strategic exposure. Similarly, cybersecurity is no longer an isolated technical field but a governance frontier that shapes crisis stability and alliance management, given persistent attribution challenges and the blurred boundary between peacetime competition and escalation. The analysis also suggests that non traditional security risks, including global health and climate related security pressures, are not peripheral to national and regional security in the deglobalization context because their diffusion interacts with political legitimacy and strategic narratives. These dynamics widen the substantive scope of security governance while intensifying the problem of institutional coordination across domains that are often governed by separate regimes and competing normative logics.

A second conclusion is that institutional responses are increasingly plural and layered, yet not necessarily coherent. The empirical illustrations across theatres highlight that governance does not unfold exclusively through universal multilateralism, nor does it collapse into pure unilateralism. Instead, states and organizations rely on a mixed architecture that includes global institutions, regional organizations, minilateral coalitions, and hybrid governance arrangements that combine international coordination with localized implementation. This pluralization can be adaptive because it allows tailored responses to specific risks and capacity constraints. At the same time, pluralization can deepen fragmentation if interoperability is limited to intra bloc coordination or if institutional outputs are designed primarily for strategic signaling rather than for risk reduction. The implication is that institutional diversity is not inherently stabilizing or destabilizing. Its effects depend on whether governance layers can exchange information, align procedures, and maintain crisis management channels that reduce misperception and escalation incentives.

A third conclusion concerns enforcement and credibility. The analysis has treated enforcement deficits as a structural problem rather than an implementation detail because the capacity of governance rules to shape behavior is inseparable from monitoring, verification, and sanctioning arrangements that can withstand political contestation. Deglobalization era rivalry increases the temptation to reinterpret rules opportunistically, to contest oversight as sovereignty intrusion, and to shift disputes into favorable venues. Enforcement weaknesses are particularly consequential in domains where verification is difficult, such as cyber operations, influence activities, and certain forms of infrastructure disruption. The practical governance consequence is that institutions may remain symbolically central while becoming operationally selective, producing uneven compliance and persistent gray zones where risk diffusion accelerates. This finding reinforces the importance of designing governance mechanisms that balance transparency with security needs, and that embed enforcement in procedures that are viewed as legitimate by a wide range of actors.

A further conclusion is that national and regional security concerns must be addressed simultaneously, because risk diffusion links local vulnerabilities to systemic competition. Regional theatres are not merely arenas where great powers project influence. They are also the spaces where competing governance models intersect with local disputes, where small and middle powers face constraints on strategic autonomy, and where escalation risks are shaped by a combination of external rivalry and internal security dilemmas. This is evident in maritime theatres where strategic access and economic resilience converge, in regions where proliferation and escalation dynamics interact with great power alignment, and in emerging arenas such as the Arctic where governance institutions are less consolidated. The article's framework indicates that regional security governance is most effective when it reduces cascade risks and provides credible crisis management channels while avoiding rigid bloc logic that amplifies insecurity. Where regional institutions cannot sustain cohesion, the governance challenge becomes one of managing competitive alignment while preserving minimal cooperation for shared risks.

The analytical framework proposed in this study has emphasized a sequence from exposure to securitization, from venue selection to policy output, and from output to effects mediated by enforcement, legitimacy, and strategic context. This sequence is intended to support future empirical research by providing a structured way to compare institutional responses across domains and theatres. In particular, the evaluative criteria of damping capacity, interoperability, legitimacy, and enforcement credibility offer a basis for assessing whether specific governance arrangements reduce cascade potential or unintentionally intensify rivalry. Future studies can operationalize these criteria through comparative case analysis of crisis episodes, institutional design changes, and the interaction between national security strategies and regional governance mechanisms. Methodologically, this approach can bridge qualitative institutional analysis with network oriented representations of interdependence, enabling more precise claims about when and how governance interventions dampen diffusion.

The study also has implications for policy and institutional design. The most immediate implication is that managing deglobalization era insecurity requires governance architectures that are institutionally plural yet interoperable. Plurality is unavoidable given political contestation and divergent threat perceptions. Interoperability is essential because risks propagate across boundaries regardless of institutional fragmentation. Effective governance therefore depends on shared crisis communication protocols, minimum standards for infrastructure protection, and coordination mechanisms that function even when strategic trust is limited. A second implication is that governance should prioritize preventing cascade failures in critical nodes, including ports, undersea cables, logistics platforms, and energy infrastructures, because these nodes connect economic functioning to strategic stability. A third implication is that institutions should pay greater attention to legitimacy producing procedures, including transparency, consultation, and accountability mechanisms appropriate to security contexts, because legitimacy shapes compliance and reduces the incentives for opportunistic defection. These design priorities do not eliminate competition, but they can mitigate the tendency of competition to convert interdependence into systemic vulnerability.

Finally, the article underscores that deglobalization does not imply the disappearance of multilateralism. It implies a contested multilateralism in which institutions must operate under conditions of intensified bargaining, rival ordering projects, and uneven willingness to accept constraints. Global bodies remain important for legitimacy and agenda setting, while regional institutions remain essential for contextualized governance and crisis management. The central challenge is to prevent governance fragmentation from becoming self reinforcing, where each new governance gap is treated as evidence that only unilateral or bloc based solutions are viable. By reframing international security governance as the management of cross domain risk diffusion under great power competition, the article has argued for an analytical and practical focus on the mechanisms that generate cascades and the institutional features that can dampen them. In this perspective, security governance effectiveness is less about restoring an idealized universal order and more about building durable capacities for coordination, enforcement, and crisis stability across a plural institutional landscape that reflects the realities of contemporary competition.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Linsi L, Gristwood E. The myth of deglobalization: Multinational corporations in an era of growing geopolitical rivalries. Politics and Governance, 2024, 12. https://doi.org/10.17645/pag.8092.

[2] Heto P P-K. Global supply chains and great power competition. In: East Asia, 2021: 115–132. https://doi.org/10.1017/9781108985468.009.

[3] Slawotsky J. Conceptualizing national security in the era of great power competition. East Asia, 2024, 42(3): 279–307. https://doi.org/10.1007/s12140-024-09434-y.

[4] Renn O, Klinke A. Risk governance: Concept and application to institutional risk management. In: Better Business Regulation in a Risk Society, 2012: 17–36. https://doi.org/10.1007/978-1-4614-4406-0_2.

[5] Chan K, Wouters J. Enforcement in global security governance. In: Accountability, Governance and Democracy, 2015. https://doi.org/10.4337/9781781952627.00015.

[6] Wissenbach U. International society and the diffusion of power in complexity. In: Rethinking Governance in Europe and Northeast Asia, 2019: 11–27. https://doi.org/10.4324/9780429317125-2.

[7] Gray C S, Wirtz J J. The age of acceleration and the rise of great power competition. In: War, Peace and International Relations, 2023: 310–325. https://doi.org/10.4324/9781003336358-25.

[8] Coker C. Power vacuums and the return of great power competition. International Security, 2018: 13–14. https://doi.org/10.31175/p.2018.01.03.

[9] Watts S, Beauchamp-Mustafaga N, Harris B, et al. Alternative worldviews: Understanding potential trajectories of great-power ideological competition. 2020. https://doi.org/10.7249/rr2982.

[10] Floyd R. Global climate security governance: A case of institutional and ideational fragmentation. Conflict, Security & Development, 2015, 15(2): 119–146. https://doi.org/10.1080/14678802.2015.1034452.

[11] Yeo A, Kardon I. European maritime security and strategic access in an age of great power competition. In: Great Power Competition and Overseas Bases, 2024: 137–156. https://doi.org/10.5771/9780815740711-137.

[12] Gresh G F. European maritime security and strategic access in an age of great power competition. In: Great Power Competition and Overseas Bases, 2024: 137–156. https://doi.org/10.5040/9780815752868.ch-009.

[13] Rosario A, Shives T, Canan M. Expanding the cyber mission space with the expansion of security cooperation in the era of great power competition. International Conference on Cyber Warfare and Security, 2025, 20(1): 427–436. https://doi.org/10.34190/iccws.20.1.3388.

[14] Potts G. Cyber leadership in the era of the great power competition. In: The Great Power Competition, 2022, 3: 263–279. https://doi.org/10.1007/978-3-031-04586-8_13.

[15] Warner R. Disaster risk governance as a guide to Canadian policy responses to a global health emergency. In: Canada and Great Power Competition, 2022: 147–167. https://doi.org/10.1007/978-3-031-04368-0_7.

[16] Gbla O. Hybrid security governance responses to crises: The case of the Ebola response in Sierra Leone. Stability: International Journal of Security and Development, 2018, 7(1). https://doi.org/10.5334/sta.612.

[17] Grajewski N, Menton J D. MENA at the threshold? Proliferation risks and great power competition. Texas National Security Review, 2025, 8(4): 95–103. https://doi.org/10.1353/tns.00017.

[18] Ullah A, Xinlei L. Navigating the Persian Gulf security complex: Saudi–Iran rapprochement in an era of great power competition. East Asia, 2024, 41(3): 273–300. https://doi.org/10.1007/s12140-024-09430-2.

[19] Samad O. China and Afghanistan: Navigating geoeconomic and security risks amid great power competition. In: Volume 6, 2024: 291–314. https://doi.org/10.1007/978-3-031-70767-4_14.

[20] Mahmood M. The Arctic: A new theater of great power competition. ACADEMIA International Journal for Social Sciences, 2025, 4(3): 583–599. https://doi.org/10.63056/acad.004.03.0397.

[21] Bhandari S. The frozen frontier: U.S. Arctic strategy in the era of great power competition. 2025. https://doi.org/10.2139/ssrn.5374239.

[22] Muth C J. Limited semi-infinity: Japan's deep-sea resources against the backdrop of China's rare earth. In: Navigating East Asian Maritime Conflicts, 2024: 257–291. https://doi.org/10.1007/978-3-031-51989-5_11.

[23] Puranen M, Chen J Y-W. Chinese vision for a durable security order in an era of great power competition. In: Competing Visions for International Order, 2025: 40–51. https://doi.org/10.4324/9781003562306-4.

[24] Yang L. The UN Security Council's strategy for multilateralism in the context of great power competition. Studies in Social Science & Humanities, 2025, 4(3): 40–48. https://doi.org/10.63593/sssh.2709-7862.2025.05.007.

[25] Beeson M. Decentered? ASEAN's struggle to accommodate great power competition. International Studies Quarterly, 2022, 2(1). https://doi.org/10.1093/isagsq/ksab044.

[26] Wise M. The security cooperation toolkit and the future of great power competition. Orbis, 2024, 68(4): 589–606. https://doi.org/10.1016/j.orbis.2024.09.006.

[27] Yuyan, Z., & Guangtao, X. Trade, power, and welfare: An international economic political analysis of great power competition. Social Sciences in China, 2024, 45(3): 57–75. https://doi.org/10.1080/02529203.2024.2403261.

[28] Maier-Knapp, N. The non-traditional security concept and the EU–ASEAN relationship against the backdrop of China's rise. The Pacific Review, 2015, 29(3): 411–430. https://doi.org/10.1080/09512748.2015.1038579.

[29] Economic security in an era of globalization: Definition and provision. In: Globalisation and economic security in East Asia, 2012: 40–56. https://doi.org/10.4324/9780203086155-12.

[30] Cooley, A. International ordering and great power competition. In: Great power competition and overseas bases, 2024: 103–120. https://doi.org/10.5040/9780815752868.ch-007.

[31] Siekiera, J. Climate change in the Pacific Ocean: Security and great power competition. In: 21st century as the Pacific century, 2023: 96–110. https://doi.org/10.31338/uw.9788323563136.

[32] Steff, R. Nuclear deterrence in a new age of disruptive technologies and great power competition. In: Deterrence, 2020: 57–75. https://doi.org/10.1007/978-3-030-29367-3_4.

[33] Pfaff, C. A. Proxy war ethics: The norms of partnering in great power competition. Springer Nature Switzerland, 2024. https://doi.org/10.1007/978-3-031-50458-7.

[34] Camilleri, J. A. Energy governance in the era of globalization and climate change. In: Globalization and climate change, 2012: 255–274. https://doi.org/10.1057/9780230355361_15.

[35] Walia, S. The role of Australia and the Pacific Islands in the Indo-Pacific region amidst the great power competition. In: 21st century as the Pacific century, 2023: 144–154. https://doi.org/10.31338/uw.9788323563136.pp.144-154.