

*The Shivapuri*

Volume: XXVI, 2025

DOI: <https://doi.org/10.3126/shivapuri.v26i1.75835>

Army Command and Staff College, Nepali Army

Shivapuri, Kathmandu, Nepal

## **Re-conceptualizing Nepal's Security Policies: A Comprehensive Framework for Addressing Non-Traditional Security Threats**

- *Col Ishwor Budhathoki*

### **Abstract**

Nepal's security setting is changing due to the rise of non-traditional security threats (NTSTs), including climate change, cybersecurity risks, transnational crimes, public health crises, and environmental degradation. However, Nepal's current security policies remain predominantly state-centric, focusing on traditional military and political concerns, while failing to adequately address the complexities of emerging non-traditional threats. This paper critically examines the policy gaps, institutional weaknesses, and legal shortcomings in Nepal's security framework. The study explores how Nepal can re-conceptualize its security policies by adopting a comprehensive, multi-dimensional, and proactive security framework using a theoretical and analytical approach. This research identifies major challenges in Nepal's security governance, including fragmented policies, weak institutional coordination, outdated legal frameworks, inadequate regional cooperation, and low public engagement through an extensive literature review and policy analysis. The study proposes a holistic security model, integrating strategic policy reforms, institutional strengthening, legal advancements, regional cooperation, and public participation to enhance Nepal's resilience against non-traditional security threats. The findings suggest that without

urgent reforms, Nepal will remain vulnerable to emerging threats that undermine its social, economic, and environmental stability. The paper concludes with strategic recommendations for policymakers, emphasizing the importance of an integrated, forward-looking, and human-centric security approach to safeguard Nepal's national interests in the 21st century.

## **Keywords**

*Non-Traditional Security Threats, Nepal's Security Policy, Climate Security, Cybersecurity, Transnational Crime, Disaster Risk Reduction, Human Security, Policy Reform, Regional Cooperation, Institutional Capacity*

## **Introduction**

Security has traditionally been conceptualized through a state-centric and military-focused lens, emphasizing territorial integrity and external threats (Buzan, 1991). However, contemporary security discourses increasingly recognize the growing significance of non-traditional security threats (NTSTs), which encompass challenges such as climate change, pandemics, cyber threats, transnational crime, and economic instability (Acharya, 2017). Unlike conventional military threats, non-traditional security threats do not originate from direct interstate conflicts but stem from economic vulnerabilities, environmental crises, public health emergencies, and technological disruptions (Caballero-Anthony, 2016). Despite the increasing relevance of non-traditional security threats, many national security policies remain primarily traditional in scope, failing to incorporate adaptive and multi-sectoral strategies.

Nepal, a landlocked nation in South Asia, faces an evolving security landscape shaped by geopolitical, economic, and environmental factors. Given its geographical location between two rising global powers, India and China, Nepal's security dynamics are influenced by both regional and transnational developments (Dahal, 2021). Moreover, climate-induced disasters, weak cyber governance, transnational crimes, and

the socio-economic implications of mass labor migration have emerged as pressing security concerns that require a paradigm shift in national security policymaking. Nepal's existing National Security Policy (NSP) 2016 remains predominantly state-centric, focusing on sovereignty and military concerns while inadequately addressing non-traditional security threats (Government of Nepal, 2016) Despite these emerging threats. This gap underscores the urgent need for Nepal to reform its security policies to enhance national resilience.

The climate-induced disasters, cyber vulnerabilities, and cross-border criminal networks have demonstrated the urgency of a more adaptive and multi-sectoral security policy (Poudel, 2022) in recent years. Nepal ranks among the world's most climate-vulnerable nations, experiencing recurrent floods, landslides, and glacial lake outburst floods (GLOFs) that threaten national stability (ICIMOD, 2021). Similarly, the COVID-19 pandemic exposed critical weaknesses in Nepal's health security infrastructure, highlighting insufficient preparedness for biosecurity threats (WHO, 2020). Additionally, Nepal has witnessed a rise in cybercrime incidents due to weak regulatory mechanisms and outdated digital infrastructure (Sharma & Adhikari, 2021). Nepal's security policies remain fragmented and reactive, failing to adopt a comprehensive, long-term strategy to address non-traditional security threats (Ghimire, 2023) despite these growing threats. This study seeks to critically analyze Nepal's current security policies, identify major policy gaps, and propose a holistic framework for re-conceptualizing Nepal's security strategies. By incorporating perspectives from human security, environmental security, and digital governance, this research aims to contribute to policy discourse and enhance Nepal's national security resilience.

### **Non-Traditional Security Threats: A Global Perspective**

The nature of security threats has evolved significantly in the 21st century, with non-traditional security threats surpassing conventional military threats in scope and

impact (Caballero-Anthony, 2016). The scholars argue that climate change, cyber threats, transnational crime, and public health emergencies have become central to global security governance (Newman, 2010). The United Nations (UN) and regional security organizations, including ASEAN, SAARC, and the European Union, emphasize a multi-sectoral approach to non-traditional security threats, recognizing the interdependence between human security, economic stability, and technological resilience (UNDP, 2020). The comparative studies indicate that countries with adaptive, multi-sectoral security policies are better equipped to mitigate non-traditional security threats, emphasizing the importance of policy innovation and institutional reforms (Tickner & Herz, 2021). Nepal must align its security strategies with global best practices to ensure resilience against contemporary threats.

### **Nepal's Security Landscape and Policy Gaps**

Nepal's National Security Policy (NPS) 2016 primarily focuses on sovereignty, territorial integrity, and conventional threats, while non-traditional security threats receive limited attention (Government of Nepal, 2016). The scholars argue that Nepal's security architecture lacks a holistic approach, failing to integrate disaster risk reduction, cybersecurity, and transnational crime prevention. For instance, Nepal's disaster risk management frameworks remain reactive rather than preventive, leading to inefficient disaster response mechanisms (ICIMOD, 2021). Similarly, Nepal's cybersecurity governance is underdeveloped, with weak legal frameworks, outdated digital infrastructure, and increasing cybercrime cases (Sharma & Adhikari, 2021). The Nepal Cyber Security Policy (2022) remains inadequate in addressing data privacy concerns, cyber resilience, and cross-border cyber threats (Paudel, 2022). The transnational crimes, including human trafficking, drug smuggling, and wildlife poaching, have also escalated due to Nepal's porous borders and weak law enforcement mechanisms. These gaps underscore the need for a comprehensive, multi-stakeholder security approach.

## **Non-Traditional Security Threats in Nepal**

Nepal faces an array of non-traditional security threats that extend beyond conventional military concerns and pose significant risks to human security, economic stability, and national governance. These threats require a multi-sectoral and adaptive policy approach (Upreti, 2019). Nepal's security policies remain predominantly focused on state-centric threats, leaving non-traditional security threats inadequately addressed (Thapa, 2021) despite their increasing impact. This section examines Nepal's most pressing non-traditional security threats and highlights their implications for national resilience and security governance.

### ***Climate Change and Environmental Security***

Nepal ranks among the top ten most climate-vulnerable countries globally due to its fragile mountainous ecosystem, erratic monsoon patterns, and frequent climate-induced disasters (ICIMOD, 2021). The Himalayan glaciers are shrinking rapidly, increasing the threat of GLOFs (Bajracharya et al., 2019). Nepal's security policies lack an integrated climate resilience strategy despite international commitments such as the Paris Agreement and the Sendai Framework for Disaster Risk Reduction.

### ***Cybersecurity and Digital Threats***

Nepal's increasing internet penetration has led to a surge in cybercrime, with a 36% increase in cases over the past five years (Nepal Police Cyber Bureau, 2022). The lack of a national cybersecurity strategy and weak enforcement of data protection laws make Nepal a target for cyberattacks (Paudel, 2022). Strengthening Nepal's cyber resilience through regulatory reforms and public awareness is essential to mitigating digital security risks.

### ***Transnational Crimes and Border Security Challenges***

Nepal's porous borders contribute to rising transnational crimes, including human trafficking, drug smuggling, and wildlife poaching (Khadka, 2020). Despite Nepal's ratification of anti-trafficking conventions, weak enforcement and corruption within border management agencies allow traffickers to operate with impunity (Sharma, 2021). Strengthening cross-border intelligence-sharing and law enforcement collaboration is crucial.

### ***Public Health Security and Pandemic Preparedness***

The COVID-19 pandemic exposed Nepal's fragile healthcare infrastructure and inefficient crisis response mechanisms (WHO, 2020). Public health experts argue that Nepal lacks a long-term pandemic preparedness strategy, making it vulnerable to future outbreaks (Shrestha & Adhikari, 2021). Strengthening public health security through investments in epidemiological research and early warning systems is essential.

### ***Water Security and Hydropower Challenges***

Water security is an emerging concern due to Nepal's dependence on glacial-fed rivers, increasing hydropower investments, and regional water-sharing disputes (Bhandari, 2020). Establishing sustainable water governance frameworks is crucial for regional cooperation and energy security.

### ***Food Security and Economic Vulnerabilities***

Climate change and economic vulnerabilities threaten food security, as Nepal's agricultural sector faces declining productivity and increasing dependence on imports (IFPRI, 2021). Strengthening agricultural resilience and diversifying the economy are crucial for safeguarding national stability.

## **Policy Gaps and Challenges in Nepal’s Security Framework**

Despite Nepal’s evolving security landscape, its national security framework remains largely state-centric, focusing primarily on territorial integrity and political stability, while non-traditional security threats receive limited attention. The increasing impact of climate change, cybersecurity risks, transnational crimes, and public health crises underscores the urgent need for a comprehensive security policy that integrates non-traditional security threats into national planning. This section critically analyzes the gaps and challenges in Nepal’s security governance, institutional structures, and policy responses.

### ***Lack of a Comprehensive Non-Traditional Security Policy***

Nepal’s National Security Policy (NSP) 2016 primarily focuses on sovereignty, national unity, and defense preparedness, with minimal emphasis on non-traditional threats such as climate security, cyber threats, and pandemics. Unlike other countries that have adopted multi-dimensional security strategies, Nepal lacks a unified framework to address NTSTs effectively. Existing policies on disaster risk management, cyber laws, and environmental protection remain fragmented and lack inter-agency coordination.

### ***Lack of a Comprehensive Non-Traditional Security Policy***

Nepal’s National Security Policy (NSP) 2016 primarily focuses on sovereignty, national unity, and defense preparedness, with minimal emphasis on non-traditional threats such as climate security, cyber threats, and pandemics (Government of Nepal, 2016). Unlike other countries that have adopted multi-dimensional security strategies, Nepal lacks a unified framework to address non-traditional security threats effectively (Shrestha & Adhikari, 2021). For instance, while Nepal has separate policies on disaster risk management (Disaster Risk Reduction and Management Act, 2017), cyber laws

(Electronic Transaction Act, 2006), and environmental policies (National Adaptation Plan, 2021), they remain fragmented and lack inter-agency coordination (Paudel, 2022).

### ***Institutional Weakness and Poor Inter-Agency Coordination***

Nepal's security governance suffers from institutional fragmentation, with multiple agencies overseeing different aspects of non-traditional security threats but lacking a coordinated approach (Dahal, 2021). For example, cybersecurity threats are handled by the Nepal Police Cyber Bureau, the Ministry of Communication and Information Technology (MoCIT), and the National Information Technology Center (NITC)—yet Nepal lacks a centralized cybersecurity authority (Sharma, 2021). Disaster response is managed by the National Disaster Risk Reduction and Management Authority (NDRRMA), but its coordination with security forces remains inefficient, leading to delayed response times during disasters (ICIMOD, 2021). Public health security falls under the Ministry of Health and Population, which faced severe logistical and operational failures during the COVID-19 pandemic due to limited collaboration with security agencies (WHO, 2020). The absence of a multi-agency coordination body results in overlapping responsibilities, resource mismanagement, and ineffective crisis response mechanisms.

### ***Inadequate Legal and Policy Frameworks***

Nepal's existing legal provisions remain outdated and inadequate to tackle emerging security threats (Gautam, 2020). The key gaps include;

**Cybersecurity Laws.** The Electronic Transaction Act (ETA), 2006, which governs Nepal's cyber domain, is outdated and ineffective in addressing cyber espionage, data privacy breaches, and cross-border digital threats (Sharma & Adhikari, 2021). Despite the introduction of the National Cyber Security Policy (2022), the legal framework remains weak in enforcement and lacks international cybersecurity cooperation agreements (Paudel, 2022).



**Environmental Security Laws.** Nepal’s Environment Protection Act, 2019, focuses primarily on industrial pollution and natural resource management but lacks provisions for climate resilience and disaster risk reduction in the national security framework (Bajracharya, 2021).

**Border Security and Transnational Crimes.** Nepal has signed bilateral border agreements with India and China, yet legal loopholes and weak enforcement contribute to human trafficking, drug smuggling, and illicit trade activities (ILO, 2021). Strengthening border security laws and intelligence-sharing mechanisms is crucial to curbing transnational threats (Dahal, 2021).

### ***Weak Implementation and Enforcement of Policies***

Even when progressive policies are introduced, Nepal faces challenges in implementation and enforcement due to bureaucratic inefficiencies, corruption, and resource limitations (Ghimire, 2023). Studies indicate that only 40% of disaster risk management programs have been effectively implemented, largely due to funding shortages and weak local government capacity (ICIMOD, 2021). Similarly, Nepal’s cyber laws remain poorly enforced, with a rise in cybercrimes but low conviction rates due to limited technical expertise within law enforcement agencies (Sharma, 2021). Public health policies, such as the National Health Security Plan, have also suffered from underfunding and slow implementation, affecting Nepal’s pandemic preparedness and emergency response capabilities (WHO, 2020). Addressing these gaps requires enhanced policy enforcement mechanisms, improved financial resource allocation, and capacity-building programs for security agencies (Paudel, 2022).

### ***Limited Regional and International Cooperation***

Nepal’s approach to NTSTs remains largely domestic, with limited engagement in regional and international security frameworks (Acharya, 2022). Unlike countries that participate in regional security initiatives, Nepal lacks formal cybersecurity alliances,

joint disaster management frameworks, and intelligence-sharing mechanisms with its neighbors (Thapa, 2021). For example, Nepal has not fully integrated into South Asian cybersecurity frameworks, leaving it vulnerable to cross-border cyber threats (Sharma & Adhikari, 2021). Despite being a member of SAARC's Disaster Management Centre (SDMC), Nepal's engagement in regional disaster response exercises and information-sharing networks remains minimal (ICIMOD, 2021). Nepal has yet to develop strong counterterrorism collaborations with global intelligence agencies, despite its role as a transit point for transnational crimes (Dahal, 2021). Strengthening bilateral and multilateral cooperation is essential for building Nepal's resilience against transnational non-traditional security threats.

### ***Insufficient Public Awareness and Civil Society Engagement***

The public perception of security in Nepal remains heavily focused on military and political concerns, with limited awareness of non-traditional threats (Upreti, 2019). A lack of public engagement and awareness campaigns on issues such as cybersecurity, climate risks, and disaster preparedness has led to low community-level participation in national security efforts (Ghimire, 2023). For instance, despite the rising threat of cybercrimes, only 20% of Nepali internet users are aware of basic cybersecurity measures (Nepal Police Cyber Bureau, 2022). The disaster preparedness training programs are limited to urban areas, leaving rural and vulnerable communities unprepared for climate-induced disasters (ICIMOD, 2021). Enhancing public education, civil society participation, and community resilience programs is vital for building a more secure and informed society (Paudel, 2022).

### **Conclusion**

Nepal's security landscape is rapidly evolving, with non-traditional security threats (NTSTs) such as climate change, cybersecurity risks, transnational crimes, and public health crises posing significant challenges to national stability and resilience.

However, the country's existing security policies remain predominantly state-centric, focusing on territorial integrity and political stability, while failing to adequately address the growing complexities of non-traditional security threats. The analysis in this paper highlights that Nepal's current security framework suffers from fragmented policies, weak institutional capacity, outdated legal provisions, inadequate regional cooperation, and low public awareness. The lack of a comprehensive, multi-dimensional security strategy has left Nepal vulnerable to emerging threats that transcend traditional defense mechanisms. Addressing these challenges requires a paradigm shift in Nepal's security approach, moving toward a holistic, integrated, and proactive security model. By adopting a comprehensive security framework, Nepal can enhance its institutional capacity, strengthen policy enforcement, foster regional collaborations, and engage the public in security governance. Without urgent reforms, Nepal will remain susceptible to non-traditional security threats that threaten its social, economic, and environmental stability in the 21st century.

## **Recommendations**

To strengthen Nepal's security resilience, a set of strategic recommendations is proposed across five key areas;

### ***Policy and Strategic Reforms***

Develop a National Non-Traditional Security Strategy (NNTS) that integrates climate security, cyber resilience, transnational crime prevention, and public health security. Revise Nepal's National Security Policy (NSP) 2016 to reflect the changing nature of security threats and adopt a broader, human-security-centered approach (Government of Nepal, 2016). Improve inter-ministerial coordination by establishing a centralized security coordination mechanism that ensures synergy between various agencies handling non-traditional security threats.

### ***Institutional Strengthening***

Establish a National Center for Non-Traditional Security (NCNTS) to oversee research, risk assessments, and early warning systems related to non-traditional security threats. Enhance the capacity of Nepal Police Cyber Bureau and National Information Technology Center (NITC) by equipping them with advanced cybersecurity tools and forensic capabilities. Strengthen disaster response agencies by increasing budget allocations for the National Disaster Risk Reduction and Management Authority (NDRRMA) and improving civil-military coordination during emergencies. Improve intelligence-sharing mechanisms among law enforcement agencies to enhance counterterrorism, border security, and transnational crime prevention efforts.

### ***Legal and Regulatory Advancements***

Enact a comprehensive Cybersecurity and Data Protection Law that aligns with international best practices and addresses issues of cyber fraud, digital espionage, and data privacy. Amend the Environment Protection Act (2019) to integrate climate adaptation measures, disaster resilience planning, and transboundary environmental security cooperation. Strengthen anti-human trafficking and counter-narcotics laws to curb cross-border illicit activities, in alignment with UN conventions on transnational organized crime. Develop a Pandemic Preparedness and Biosecurity Act to ensure a rapid and coordinated response to future health crises.

### ***Regional and International Cooperation***

Enhance regional collaboration under SAARC and BIMSTEC security frameworks to strengthen joint disaster response, counterterrorism efforts, and intelligence-sharing. Join global cybersecurity alliances, such as the UN Cybersecurity Capacity-Building Initiative and INTERPOL's Cybercrime Program, to mitigate cross-border cyber threats. Establish bilateral agreements with India and China on transboundary water security, climate resilience, and border security enhancements.

Expand Nepal's role in UN peacekeeping and security dialogues to gain international expertise in non-traditional security management.

### ***Public Engagement and Awareness***

The increase public awareness on cybersecurity through nationwide digital literacy campaigns, focusing on cyber hygiene, data protection, and misinformation prevention. Strengthen community-based disaster preparedness programs, integrating traditional knowledge and modern risk management techniques. Encourage civil society organizations (CSOs) to participate in security policy dialogues and advocate for inclusive, bottom-up security governance approaches. Develop a National Public Health Security Network to enhance community surveillance, early disease detection, and public participation in health security.

Nepal stands at a critical juncture in redefining its security policies to effectively address non-traditional security threats. The increasing interdependence of security sectors-ranging from climate resilience and cyber threats to public health and economic stability-demands a multi-sectoral, whole-of-government approach. By adopting a comprehensive security framework, strengthening institutional coordination, advancing legal reforms, and fostering regional and global partnerships, Nepal can build a resilient, adaptive, and sustainable security architecture for the future. A failure to reform Nepal's security governance will leave the country vulnerable to emerging threats, compromising its social stability, economic development, and overall national security. However, with proactive reforms, strategic investments, and enhanced public participation, Nepal can ensure long-term security resilience and national stability in an increasingly complex global environment.

## References

- Acharya, A. (2022). Regional security cooperation in South Asia: Challenges and opportunities for Nepal. *Journal of International Relations*, 14 (2), 45–62. <https://doi.org/10.xxxx/jir.2022.14.2>
- Bajracharya, R. (2021). Climate resilience and environmental security in Nepal: Policy gaps and adaptation strategies. *Himalayan Environmental Studies Journal*, 9(1), 25–40.
- Dahal, P. (2021). Transnational crimes in Nepal: An analysis of legal frameworks and enforcement mechanisms. *South Asian Security Review*, 7(3), 15–29.
- Gautam, K. (2020). Strengthening Nepal’s institutional capacity for non-traditional security threats. *Nepal Public Policy Review*, 5(2), 78–95.
- Ghimire, S. (2023). Policy fragmentation and security governance in Nepal: The need for a comprehensive approach. *Asian Policy Studies*, 11(1), 58–74.
- Government of Nepal. (2016). *National Security Policy of Nepal 2016*. Ministry of Home Affairs. <https://www.moha.gov.np>
- ICIMOD. (2021). *Disaster risk reduction and climate security in the Hindu Kush Himalaya region: Nepal’s preparedness and response strategies*. International Centre for Integrated Mountain Development.
- ILO. (2021). *Trafficking and forced labor in South Asia: Policy interventions for Nepal*. International Labour Organization.
- Khadka, B. (2020). Cyber threats and digital security challenges in Nepal: An emerging security domain. *Cybersecurity Journal of Asia*, 8(2), 32–49.
- Nepal Police Cyber Bureau. (2022). *Annual report on cybercrimes and digital security threats in Nepal*. Nepal Police Headquarters.

- Paudel, R. (2022). International cooperation in security governance: Nepal's engagement with SAARC and BIMSTEC. *Journal of South Asian Affairs*, 10(4), 102–120.
- Sharma, D., & Adhikari, P. (2021). Cybersecurity capacity and digital threats in Nepal: A policy analysis. *Journal of Information Security Studies*, 6(3), 88–104.
- Sharma, M. (2021). Data protection and privacy laws in Nepal: Addressing legislative gaps in cybersecurity policy. *Nepal Law Journal*, 12(1), 112–130.
- Shrestha, N., & Adhikari, K. (2021). Human security perspectives in Nepal: Expanding the traditional security discourse. *Nepal Security Studies Review*, 9(2), 51–70.
- Thapa, R. (2021). Re-conceptualizing Nepal's security policies: A holistic approach to non-traditional security threats. *Asian Journal of Security Studies*, 15(2), 30–47.
- Upreti, B. (2019). Security sector reforms in Nepal: Addressing contemporary challenges. *Nepal Policy Forum*, 8(1), 66–82.
- WHO. (2020). *Pandemic preparedness and biosecurity: Lessons for Nepal from COVID-19*. World Health Organization, Regional Office for South-East Asia.