Unity Journal
Vol.6, 202-215, Feb 2025
https://doi.org/10.3126/unityj.v6i1.75629
Prithvi Narayan Shah Research Center
Directorate General of Military Training, Nepali Army
Kathmandu, Nepal

ISSN - 2717-4751

Article history
Received: 08 Nov 2024
Accepted: 22 Jan 2025

Multi-Dimensional Strategy for Combating Non-Traditional Security Threats in Nepal

Ishwor Budhathoki[*]

Abstract

Nepal, strategically located at the crossroads of South Asia, confronts a complex array of non-traditional security threats that extend beyond conventional military concerns, thereby posing profound risks to national stability and sustainable development. This article undertakes a critical examination of these threats, ranging from environmental degradation and cybersecurity vulnerabilities to pandemics and transnational crime, arguing that traditional military-centric approaches are inadequate for effective mitigation. The central proposition contends that a multi-dimensional strategy, integrating human security, technological resilience, and regional cooperation, is indispensable for addressing these multifaceted challenges. The objectives are threefold: first, to systematically identify and categorize the principal non-traditional security threats facing Nepal; second, to critically assess the existing policy frameworks and institutional responses, identifying their limitations and gaps; and third, to propose a comprehensive and adaptive strategy for effectively addressing these threats. Employing a qualitative research methodology, extensive primary data was gathered through formal and informal interactions with subject matter experts, security analysts, and practitioners, as well as secondary data drawn from government publications, academic literature, and international best practices. The findings reveal gaps in coherence and implementation. This article underscores the necessity of adopting a holistic security paradigm that encompasses human security, technological resilience, and regional cooperation. The key recommendations include the establishment of a dedicated task force, the strengthening of public-private partnerships, and the integration of non-traditional security considerations into national security policies and frameworks.

Keywords: *Non-traditional security, environmental degradation, cybersecurity, pandemics, transnational crime*

[*] Colonel, Nepali Army
Email ID : ibudhathoki@gmail.com

Introduction

Nepal, a landlocked nation nestled between India and China, faces a complex array of non-traditional security threats that extend beyond conventional military concerns. These threats, which include environmental degradation, cybersecurity threats, pandemics, and transnational crime, pose significant risks to the country's stability and development (Shrestha & Adhikari, 2019). The environmental degradation, exacerbated by climate change, threatens agricultural productivity and food security, undermining rural livelihoods (Gautam & Karki, 2020). Cybersecurity threats have escalated with the rapid digitalization of Nepal's economy and society, exposing critical infrastructure and sensitive data to cyberattacks (Sharma & Singh, 2021). The pandemic, as starkly illustrated by COVID-19, has overwhelmed Nepal's public health system, revealing significant gaps in preparedness and response capabilities (Bhandari & Gyawali, 2020). Moreover, Nepal's strategic location and porous borders facilitate transnational crimes such as human trafficking, drug smuggling, and arms trafficking, further complicating the security landscape (Thapa, 2018). The traditional security approaches, which primarily focus on military and defense capabilities, are insufficient to address these multifaceted challenges. The non-traditional security threats are characterized by their complexity, interconnectedness, and ability to impact human security at a fundamental level (Buzan & Hansen, 2009). Human security, which emphasizes the protection of individuals from critical and pervasive threats, provides a more comprehensive framework for addressing these issues (UNDP, 1994). Therefore, a shift towards a multi-dimensional strategy that integrates human security, technological resilience, and regional cooperation is essential for effectively combating non-traditional security threats in Nepal. This article postulates that the current approach to security in Nepal necessitates a comprehensive and coordinated strategy for combating non-traditional security threats effectively. Such a strategy should prioritize human security, bolster technological resilience, and enhance regional cooperation to address the complexity of non-traditional security threats (Adhikari, 2021). By doing so, Nepal can build a robust security architecture capable of responding to contemporary challenges and ensuring sustainable development.

Statement of the Problem

Nepal is confronted with a rapidly evolving security environment characterized by non-traditional threats that extend beyond traditional military paradigms. These threats–including environmental degradation, cybersecurity threats, pandemics, and transnational crime–pose significant challenges to national stability and development (Adhikari, 2021). The traditional security frameworks, predominantly focused on defense and military capabilities, fail to adequately address these multifaceted and interconnected issues (Buzan, 2006). For example, the environmental degradation driven by climate change and unsustainable practices exacerbates food insecurity and threatens public health, critical dimensions of human security in Nepal (Gautam & Karki, 2020). Similarly, the rise of cyber threats due to rapid digitalization exposes Nepal's critical infrastructure to potential disruptions and data breaches, compromising national security (Sharma & Singh, 2021). Pandemics, such as the COVID-19 crisis, have exposed severe deficiencies in Nepal's health infrastructure and emergency response mechanisms, highlighting the need for comprehensive public health strategies (Bhandari & Gyawali, 2020).

Furthermore, Nepal's porous borders facilitate transnational crimes, such as human trafficking and drug smuggling, which undermine legal and social systems and require enhanced border management and regional cooperation (Thapa, 2018). The current security architecture needs to be further integrated to address these non-traditional threats, resulting in fragmented and often ineffective responses. There is a pressing need for a multi-dimensional strategy that encompasses human security, technological resilience, and regional cooperation to address these challenges effectively. The problem, therefore, is the inadequacy of existing frameworks to manage and mitigate non-traditional security threats in a coordinated and comprehensive manner (Buzan & Hansen, 2009).

Objectives

This research-based article aims to address the deficiencies in Nepal's current security frameworks by pursuing three key objectives. First, it seeks to systematically identify and categorize the non-traditional security threats facing Nepal, providing a clear understanding of their nature and impact. Second, the research evaluates existing policy frameworks and institutional responses to these threats, highlighting gaps, limitations, and areas for improvement. Finally, the study proposes a comprehensive and adaptive strategy that integrates human security principles, technological resilience, and regional cooperation to enhance Nepal’s capacity to manage and mitigate these complex challenges effectively.

Methodology

This research employs a qualitative methodology, integrating systematic document analysis and an extensive literature review to critically examine Nepal’s current strategies for addressing non-traditional security threats. The document analysis is central to the study, involving a thorough evaluation of key national security policies, environmental protection regulations, cybersecurity strategies, and pandemic response plans. These documents were selected based on their relevance to Nepal’s security concerns, authority, and recency, particularly those published after 2010 to reflect the latest policy shifts. The focus is on assessing the inclusivity, effectiveness, and adaptability of these frameworks in responding to emerging threats such as cyber-attacks, environmental degradation, transnational crime, and pandemics. The literature review further contextualizes these findings by drawing on a range of peer-reviewed academic journal articles, books, and reports from international organizations. It provides a theoretical foundation for understanding non-traditional security threats and highlights a gap in the literature regarding Nepal’s specific challenges. The key concepts, such as “non-traditional security threats,” “cybersecurity,” and “environmental degradation,” are clearly defined to ensure clarity and consistency throughout the study. This research aims to fill this gap by offering unique insights into Nepal’s policy responses. Data gathered through document analysis and literature review are analyzed through thematic analysis, with a systematic coding process to organize the data into relevant categories. The key themes, trends, and gaps are then identified, allowing for a nuanced understanding of the effectiveness of current measures that are in practice. To enhance the validity of the findings, triangulation is employed, cross-checking the results across multiple data sources to ensure consistency.

Additionally, peer review from experts in security studies and policy analysis is incorporated to validate the analysis and ensure the rigor of the research. Ethical considerations are paramount in this study, with adherence to transparency, proper citation practices, and confidentiality of sensitive information. This research is conducted with a commitment to ethical standards, ensuring that the findings contribute to advancing the global and regional understanding of non-traditional security threats while offering practical recommendations for policy development in Nepal to combat the non-traditional security threats.

Non-Traditional Security Threats in Nepal

Nepal's security landscape is increasingly defined by non-traditional security threats, which diverge from conventional military concerns and encompass a broader range of issues impacting human security and national stability. These threats include environmental degradation, cybersecurity threats, pandemics, and transnational crime, each posing unique challenges to the nation (Shrestha & Adhikari, 2019). The environmental degradation, driven by deforestation, land degradation, and climate change impacts, undermines agricultural productivity and exacerbates food insecurity, affecting millions of Nepali livelihoods (Gautam & Karki, 2020). The cybersecurity threats have surged with the country's growing digital infrastructure, exposing critical systems and sensitive data to cyberattacks, which can disrupt essential services and compromise national security (Sharma & Singh, 2021). The pandemics, such as the COVID-19 crisis, have revealed significant gaps in Nepal's public health infrastructure, stressing the need for robust health emergency responses and preparedness strategies (Bhandari & Gyawali, 2020). Additionally, Nepal's geo–political position facilitate transnational crimes, including human trafficking, drug smuggling, and arms trafficking, which undermine legal systems and social stability (Thapa, 2018). These non-traditional threats are characterized by their complexity and interconnectedness, necessitating a multi-dimensional approach to effectively address their multifaceted impacts (Buzan & Hansen, 2009). Understanding and mitigating these threats requires a comprehensive strategy that integrates human security, technological resilience, and enhanced regional cooperation to safeguard Nepal's socio-economic stability and overall security.

Environmental Degradation

Environmental degradation in Nepal represents a critical non-traditional security threat with profound implications for both the natural environment and human security. The rapid deforestation, exacerbated by legal and illegal logging activities, has led to significant loss of biodiversity and disruption of ecological balance (Gautam & Karki, 2020). The country’s mountainous terrain is particularly vulnerable to soil erosion and landslides, intensified by unsustainable land use practices and the impacts of climate change. These environmental issues contribute to decreased agricultural productivity, which directly affects food security and livelihoods for the majority of the population that relies on subsistence farming (Shrestha & Adhikari, 2019). Additionally, water resources in Nepal are under increasing pressure due to glacial melt, deforestation, and pollution, leading to reduced availability of clean drinking water and impacting public health (Adhikari, 2021). The degradation of natural resources also impacts the resilience of local communities to environmental shocks, such as floods and droughts, which are becoming more frequent and severe due to climate change (Gautam & Karki, 2020). Addressing environmental degradation requires a multi-faceted approach that integrates sustainable resource management, reforestation efforts, and climate adaptation strategies to enhance environmental resilience and safeguard human security (Buzan, 2006). Effective policy interventions, such as stricter enforcement of environmental regulations, promotion of sustainable agricultural practices, and community-based conservation programs, are essential for mitigating the adverse effects of environmental degradation and ensuring long-term environmental sustainability in Nepal.

Cybersecurity Threats

Cybersecurity threats in Nepal represent a significant and growing non-traditional security threat, highlighting the need for robust and adaptive defense mechanisms in an increasingly digital world. The rapid digitalization of Nepal's infrastructure, including critical sectors such as finance, health, and government services, has introduced new vectors for cyber threats, making the nation susceptible to a range of cyber-attacks including data breaches, ransomware, and denial-of-service attacks (Sharma & Singh, 2021). Appropriate cybersecurity policies should be formulated, and adequate technical capabilities enhanced. Similarly, making key systems susceptible to potential exploitation by malicious actors should be established. For instance, recent incidents involving breaches of sensitive information from financial institutions and government databases underscore the critical need for enhanced security measures and resilient infrastructure (Shrestha & Adhikari, 2019). Additionally, the growing sophistication of cyber threats necessitates a proactive approach to cyber defense, which includes regular system updates, robust encryption practices, and continuous monitoring of network activity (Bhandari & Gyawali, 2020). Despite these needs, Nepal faces challenges related to limited resources and technical expertise, which hinder the development of effective cybersecurity frameworks. It is essential for Nepal to invest in capacity building, foster collaboration with international cybersecurity organizations, and implement comprehensive cybersecurity strategies that align with global best practices (Buzan & Hansen, 2009). The specific measures could include developing a national cybersecurity policy, establishing a dedicated cybersecurity agency, and conducting regular cyber threat assessments. This approach will not only enhance Nepal's resilience against cyber threats but also safeguard its economic stability and public trust in digital systems.

Pandemics

Pandemics in Nepal exemplify a critical non-traditional security threat with far-reaching implications for public health and socio-economic stability. The COVID-19 pandemic highlighted significant vulnerabilities in Nepal's health infrastructure, exposing systemic weaknesses in epidemic preparedness and response capabilities (Bhandari & Gyawali, 2020). The country's health system, characterized by limited resources and inadequate public health facilities, could barealy be functional to cope with the unprecedented surge in cases, which exacerbated the strain on healthcare services, and thus, revealing gaps in emergency response protocols (Adhikari, 2021). Furthermore, the pandemic underscored the need for a robust public health surveillance system to detect and respond to emerging health issues swiftly and effectively (Shrestha & Adhikari, 2019). The socio-economic impacts of pandemics extend beyond immediate health concerns, influencing economic stability through disruptions to labor markets, trade, and public services, which further result in vulnerabilities in a developing economy like Nepal's (Gautam & Karki, 2020). Addressing these challenges requires a comprehensive strategy that includes strengthening health infrastructure, investing in pandemic preparedness, and fostering international cooperation for knowledge sharing and resource mobilization. The effective management of pandemics also necessitates enhancing public health education and communication to ensure informed responses and compliance with health guidelines (Buzan & Hansen, 2009). The recommendations include improving healthcare facilities, increasing funding for health research and emergency preparedness, and establishing partnerships with international health organizations. By implementing these measures, Nepal can build resilience against future health crises and safeguard public health and economic stability.

Transnational Crime

Transnational crime poses a significant and multifaceted security threat to Nepal, impacting national security and societal stability through its pervasive and cross-border nature. The country's strategic location and porous borders make it a conduit for various forms of transnational crime, including human trafficking, drug smuggling, and arms trafficking (Thapa, 2018). Human trafficking, in particular, is a grave concern, with Nepal serving as both a source and transit country for trafficking networks exploiting vulnerabilities among marginalized populations. This illegal trade undermines human rights and contributes to a range of social issues, including exploitation and forced labor (Shrestha & Adhikari, 2019). The drug smuggling routes traverse Nepal's borders, facilitating the flow of illicit substances that exacerbate public health issues and fuel organized crime. The proliferation of arms trafficking further destabilizes the region, providing criminal groups with the means to engage in violent activities and challenge state authority (Gautam & Karki, 2020). The complexity of transnational crime requires a coordinated response that includes enhancing border security, improving law enforcement capabilities, and fostering regional and international cooperation. Strengthening legal frameworks, increasing intelligence sharing, and collaborating with neighboring countries and international agencies are essential to disrupting criminal networks and addressing the root causes of transnational crime (Buzan & Hansen, 2009). The specific measures could include joint regional task forces, cross-border anti-trafficking initiatives, and international legal cooperation to address transnational crime effectively. Integrating efforts across various sectors, including security, justice, and social services, is crucial to mitigating the impact of transnational crime on Nepal's stability and development.

Evaluation of Existing Policy Frameworks and Institutional Responses

The evaluation of existing policy frameworks and institutional responses to non-traditional security threats in Nepal is essential for identifying gaps and enhancing the effectiveness of the country's security strategies. Nepal's policies, including national security policies, environmental regulations, cybersecurity strategies, and public health preparedness plans, have evolved to address various threats. However, their effectiveness is often hindered by implementation challenges, resource constraints, and fragmented coordination among institutions (Shrestha & Adhikari, 2019).

For instance, Nepal's environmental policies, such as the National Adaptation Programme of Action (NAPA) and the Climate Change Policy, are designed to tackle deforestation and climate change. Despite their intent, inconsistent enforcement due to insufficient monitoring and enforcement mechanisms undermines their impact (Gautam & Karki, 2020). Similarly, while the Cybersecurity Strategy outlines comprehensive measures, its implementation is limited by inadequate technical capacity and insufficient inter-agency collaboration (Sharma & Singh, 2021). The public health response, as evidenced during the COVID-19 pandemic, revealed significant gaps in pandemic preparedness and emergency response infrastructure, emphasizing the need for more robust and coordinated public health strategies (Bhandari & Gyawali, 2020). Additionally, responses to transnational crime suffer from jurisdictional overlaps and limited resources, affecting law enforcement and criminal justice effectiveness (Thapa, 2018).

To address these issues, a comprehensive review of policy frameworks and institutional responses is necessary. This includes improving policy coherence, enhancing resource allocation, and fostering greater inter-agency cooperation. These measures will offer critical insights for designing an integrated and effective strategy to combat non-traditional security threats in Nepal.

Policy Frameworks

The effectiveness of Nepal's policy frameworks in addressing non-traditional security threats is critical for national stability and development. Nepal has developed various policy documents aimed at mitigating these threats, yet their implementation often falls short due to institutional and resource constraints.

The National Security Policy 2016 of Nepal aims to address wider security concerns, including human security. However, its operationalization is hindered by a lack of clear directives and poor inter-agency coordination (Shrestha & Adhikari, 2019). The environmental policies, such as NAPA and the Climate Change Policy, address environmental degradation and climate resilience issues. Despite this, inadequate funding, limited technical expertise, and fragmented enforcement mechanisms significantly impact their effectiveness (Gautam & Karki, 2020).

In cybersecurity, the Cybersecurity Strategy introduced by the government of Nepal (GoN) outlines measures to protect critical infrastructure and data. However, rapid technological advancements and evolving cyber threats necessitate continuous updates and robust implementation strategies, which are currently lacking (Sharma & Singh, 2021). The public health frameworks, including the National Health Policy and the Public Health Act, have been crucial in managing health crises like the COVID-19 pandemic. Nevertheless, these frameworks reveal significant gaps in emergency preparedness, resource allocation, and healthcare infrastructure, highlighting the need for a more resilient health system (Bhandari & Gyawali, 2020).

Legal instruments such as the Human Trafficking and Transportation (Control) Act and the Narcotic Drugs Control Act demonstrate an understanding of the need for comprehensive legal frameworks to combat transnational crime. However, jurisdictional overlaps, corruption, and limited cross-border cooperation often impede effective enforcement (Thapa, 2018). Enhancing policy frameworks requires integrated approaches that promote collaboration among governmental and non-governmental entities, strengthen institutional capacities, ensure adequate funding, and foster transparency and accountability (Buzan & Hansen, 2009).

Institutional Capacities

Nepal's institutional capacities for addressing non-traditional security threats are crucial but to some extent constrained by structural and operational limitations. The effective management of these threats requires institutions with adequate resources, technical expertise, and coordinated efforts across sectors.

Currently, institutions responsible for environmental protection, cybersecurity, public health, and law enforcement face significant challenges. Environmental agencies, tasked with implementing climate adaptation and mitigation strategies, often lack sufficient funding and technical capabilities for effective regulation enforcement (Gautam & Karki, 2020). Similarly, cybersecurity institutions struggle to keep pace with evolving threats due to limited access to advanced technologies and skilled professionals (Shrestha & Adhikari, 2019). Public health institutions require enhanced infrastructure and better emergency preparedness to respond efficiently to health crises, as demonstrated during the COVID-19 pandemic (Bhandari & Gyawali, 2020). The law enforcement agencies combating transnational crime face jurisdictional complexities and need stronger cross-border cooperation to be effective (Thapa, 2018).

Strengthening institutional capacities involves increasing budgetary allocations, fostering continuous learning, promoting inter-agency collaboration, and leveraging international partnerships. By enhancing these capacities, Nepal can build a more resilient framework for effectively addressing and mitigating non-traditional security threats.

Proposed Multi-Dimensional Strategy

A multi-dimensional strategy for combating non-traditional security threats in Nepal requires an integrated approach that includes policy reform, capacity building, and enhanced collaboration. This strategy should focus on developing comprehensive and adaptive policies for threats such as environmental degradation, cybersecurity vulnerabilities, pandemics, and transnational crime (Shrestha & Adhikari, 2019).

For environmental challenges, the strategy should incorporate sustainable resource management, climate adaptation, and robust enforcement of environmental regulations (Gautam & Karki, 2020). In cybersecurity, implementing advanced technological solutions, continuous monitoring, and capacity-building programs are essential to protect critical infrastructure and sensitive data (Sharma & Singh, 2021). Strengthening public health infrastructure and emergency preparedness is crucial for managing health pandemics, which involves investing in healthcare facilities, training healthcare workers, and establishing efficient response mechanisms (Bhandari & Gyawali, 2020). Addressing transnational crime requires enhanced border security, regional and international cooperation, and improved legal frameworks to disrupt criminal networks (Thapa, 2018). This strategy should emphasize inter-agency collaboration and public-private partnerships, leveraging various stakeholders' strengths to create a unified and resilient response to security threats. By adopting this holistic approach, Nepal can build a more robust defense against non-traditional security threats, ensuring sustainable development and national stability (Buzan & Hansen, 2009).

Human Security Dimensions

Incorporating human security dimensions into the proposed multi-dimensional strategy is essential for addressing the broader impacts of non-traditional security threats on individuals and communities. Human security emphasizes protecting and empowering individuals, focusing on their safety, well-being, and freedom from fear and want (Buzan, 2006).

For environmental degradation, human security involves safeguarding communities from climate change and resource depletion, which can lead to displacement, increased poverty, and health risks (Gautam & Karki, 2020). In cybersecurity, protecting individual privacy and securing personal data are crucial, as cyber threats can undermine personal safety and economic stability (Sharma & Singh, 2021). The pandemics highlight the importance of human security, as effective public health interventions are necessary to protect individuals from disease and ensure equitable access to healthcare (Bhandari & Gyawali, 2020). Addressing transnational crime from a human security perspective involves combating human trafficking and ensuring the protection of vulnerable populations, as well as strengthening legal and social frameworks to prevent exploitation and violence (Thapa, 2018). Integrating human security dimensions into the strategy ensures that interventions not only mitigate threats effectively but also promote overall well-being and resilience, fostering a more inclusive and sustainable approach to security (Buzan & Hansen, 2009).

Technological Resilience

Enhancing technological resilience is crucial for managing and mitigating non-traditional security threats. Technological resilience refers to the capacity of systems, infrastructure, and organizations to withstand, adapt to, and recover from technological disruptions and cyber threats (Sharma & Singh, 2021).

For Nepal, this involves investing in robust cyber infrastructure to protect against cyber threats targeting critical systems and sensitive information. Implementing advanced security measures such as encryption, intrusion detection systems, and regular security audits can enhance the resilience of digital infrastructures (Bhandari & Gyawali, 2020). Additionally, developing disaster recovery plans and continuity strategies is essential to ensure essential services continue during and after technological disruptions. This includes establishing comprehensive backup systems and partnering with technology providers to secure data (Gautam & Karki, 2020). In environmental management, leveraging technology for real-time monitoring and early warning systems can improve Nepal’s response to natural disasters and environmental degradation (Shrestha & Adhikari, 2019). Building technological resilience involves adopting new technologies and fostering a culture of continuous improvement and adaptation to emerging challenges (Buzan & Hansen, 2009).

Regional Cooperation

Regional cooperation is pivotal in addressing non-traditional security threats in Nepal due to the transnational nature of challenges like environmental degradation, transnational crime, pandemics, and cybersecurity vulnerabilities. Effective regional collaboration enhances the ability to manage these threats through shared resources, collective expertise, and coordinated strategies.

Nepal's participation in regional organizations such as the South Asian Association for Regional Cooperation (SAARC) and the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) offers platforms for joint initiatives, policy harmonization, and strategic dialogue (Sharma & Upreti, 2019). These alliances facilitate the sharing of best practices, technological advancements, and intelligence crucial for addressing issues like human trafficking and drug smuggling (Thapa, 2018). The collaborative efforts in disaster risk management and climate change adaptation through SAARC's Disaster Management Centre can significantly enhance Nepal's resilience against environmental threats (Gautam & Karki, 2020). The regional cooperation during the COVID-19 pandemic highlighted the importance of coordinated public health responses, including resource sharing and mutual support for vaccine distribution (Bhandari & Gyawali, 2020).

Similarly, joint cybersecurity initiatives can improve regional cyber defenses through information sharing and coordinated responses (Sharma & Singh, 2021). The strengthening of diplomatic and economic ties with neighboring countries like India and China can further reinforce Nepal's strategic position and collective security framework. By actively engaging in and strengthening regional cooperation mechanisms, Nepal can enhance its capabilities to address non-traditional security threats, ensuring a more secure and stable region.

Prioritization and Implementation Roadmap

To make this strategy actionable, Nepal must establish a clear prioritization and implementation roadmap that enables targeted and efficient responses to non-traditional security threats. The first step is to develop a threat prioritization framework that evaluates challenges based on their immediacy, severity, resource requirements, and feasibility of intervention (Shrestha & Adhikari, 2019). This framework will guide decision-makers in focusing efforts on the most pressing and impactful threats. Additionally, piloting proposed solutions in high-risk or vulnerable areas is essential to test their effectiveness, gather insights, and refine strategies before scaling them nationwide (Bhandari & Gyawali, 2020). Strategic allocation of funding is equally critical, ensuring that immediate needs, such as emergency response capabilities, are addressed without compromising long-term investments in resilience, such as infrastructure development and capacity-building initiatives (Gautam & Karki, 2020). By adopting this holistic and adaptive approach, Nepal can strengthen its defense against non-traditional security threats while fostering sustainable development. This forward-looking strategy ensures that immediate vulnerabilities are managed effectively while laying the foundation for national stability and resilience in an increasingly complex and interconnected global environment (Buzan & Hansen, 2009).

Addressing Non-Traditional Security Threats in Nepal: Strategic Recommendations

Addressing the multifaceted non-traditional security threats in Nepal requires a strategic and comprehensive approach that builds on discussions of policy frameworks, institutional capacities, human security dimensions, technological resilience, and regional cooperation. The complexity of these threats necessitates a cohesive and well-coordinated strategy leveraging both national and regional resources. Despite the robust intent of current policy frameworks, their implementation often falls short due to fragmented efforts and limited resource allocation. The strengthening of institutional capacities is crucial to ensure the effective operationalization of these frameworks. Integrating human security dimensions into national security strategies ensures a holistic approach prioritizing individual well-being and protection. Enhancing technological resilience is vital to safeguard against cyber threats and maintain critical digital infrastructure. Regional cooperation plays a pivotal role in addressing transnational issues, fostering shared solutions, and strengthening collective security measures. The following recommendations outline specific strategies for achieving this integration and ensuring a comprehensive approach to national security;

Dedicated Task Force- Based Approach

The establishment of a Dedicated Task Force represents a critical component of the proposed multi-dimensional strategy for addressing non-traditional security threats in Nepal. Given the complex nature of threats ranging from environmental degradation and cyber vulnerabilities to health pandemics and transnational crime, a specialized task force can offer focused expertise, enhanced coordination, and streamlined response capabilities (Shrestha & Adhikari, 2019). This task force would act as a central coordinating body, integrating efforts across various sectors and agencies to ensure a unified approach to managing these threats (Buzan & Hansen, 2009).

For example, in the European Union, the European Union Agency for Cybersecurity (ENISA) has successfully coordinated efforts to address cyber threats through a specialized task force approach. Similarly, Nepal can benefit from consolidating expertise in environmental science, cybersecurity, public health, and law enforcement. The task force would develop and implement targeted strategies, allocate resources effectively, and foster inter-agency collaboration. By creating standardized protocols and response mechanisms, the task force can significantly enhance Nepal's capacity to preempt, respond to, and recover from non-traditional security threats (Gautam & Karki, 2020). Establishing such a task force aligns with best practices observed globally and promises to strengthen Nepal’s national security framework.

Public-Private Partnerships Approach

Public-Private Partnerships (PPPs) are instrumental in enhancing Nepal’s capacity to address non-traditional security threats effectively. These partnerships leverage the strengths and resources of both public and private sectors, fostering collaborative efforts that improve the management of complex challenges such as environmental degradation, cyber threats, health crises, and transnational crime (Bhandari & Gyawali, 2020).

For instance, in the United States, public-private partnerships in cybersecurity have led to the development of advanced threat detection systems and improved response strategies.

Similarly, Nepal can benefit from collaborations between government entities and private tech firms to develop cutting-edge cybersecurity solutions (Sharma & Singh, 2021). In public health, partnerships with private healthcare providers can enhance emergency response capabilities and healthcare infrastructure (Bhandari & Gyawali, 2020). Environmental initiatives, such as sustainable resource management projects, also benefit from private sector investment and innovation (Gautam & Karki, 2020). By fostering these collaborative relationships, Nepal can bridge gaps in expertise and resources, leading to more effective and sustainable responses to non-traditional security threats.

Integration into National Security Policies

Integrating non-traditional security threats into Nepal's national security policies is essential for crafting a cohesive and forward-looking security strategy. As global and regional dynamics increasingly expose countries to unconventional threats–such as environmental degradation, cybersecurity threats, pandemics, and transnational crime–there is a pressing need to incorporate these issues into the core national security framework (Buzan & Hansen, 2009).

For example, incorporating climate change into national security policies, as seen in Australia’s Climate Change and National Security framework, enhances resilience through proactive measures and adaptive strategies (Gautam & Karki, 2020). Similarly, integrating cybersecurity threats into national frameworks, as done in the UK’s National Cybersecurity Strategy, improves coordination and response mechanisms (Sharma & Singh, 2021). By embedding non-traditional threats into the national security agenda comprehensively, Nepal can develop more robust and holistic policies that address emerging challenges and safeguard overall stability and resilience.

Conclusion

Nepal requires a multi-dimensional strategy that combines policy innovation, institutional strengthening, and a nuanced understanding of human and technological resilience to address non-traditional security threats. This approach must effectively tackle diverse challenges, including environmental degradation, cyber threats, pandemics, and transnational crime–each of which poses distinctive risks to stability and development in Nepal. The government of Nepal must implement a robust policy framework integrating sustainable resource management and climate adaptation measures to address environmental degradation. In addition, ensuring effective enforcement and appropriate resource allocation is critical to mitigating risks and fostering long-term ecological sustainability. The escalating cybersecurity threats necessitate substantial investment in advanced technologies, resilient digital infrastructure, and enhanced cybersecurity awareness to safeguard critical systems. The lessons from recent pandemics emphasize the need for a resilient public health infrastructure, capable of swift response and equitable service delivery, ensuring the well-being of all citizens, particularly vulnerable populations. Furthermore, combatting transnational crime requires a coordinated strategy that includes enhanced border security, robust legal reforms, and active international cooperation to dismantle criminal networks and protect at-risk communities.

However, a thorough evaluation of existing policy frameworks reveals gaps in coherence and implementation. The Government of Nepal must prioritize refining policies, fostering inter-agency collaboration, and ensuring adequate funding for security initiatives to bridge these gaps. Strengthening institutional capacities is equally essential to improving operational efficiency and supporting a unified approach to tackling security threats. Incorporating a human security dimension ensures that strategies focus on individual well-being and community resilience, while investments in technological resilience will equip Nepal to adapt to disruptions and protect against emerging cyber threats. By integrating these elements into a cohesive and actionable framework, Nepal can enhance its ability to manage non-traditional security threats effectively. A comprehensive, prioritized strategy not only addresses immediate concerns but also underpins sustainable development and long-term stability. This forward-looking approach positions Nepal to navigate the complexities of the modern security landscape, ensuring a secure and resilient future for its people.

References

Adhikari, R. (2019). Institutional capacities and non-traditional security threats in Nepal. *Asian Security Review, 27*(1), 89-105.

Adhikari, S. (2021). Policy frameworks for non-traditional security threats in Nepal. *Nepal Policy Review, 8*(2), 134-150.

Adhikari, S., & Shrestha, P. (2020). Enhancing cybersecurity resilience in developing countries: Insights from Nepal. *International Journal of Cybersecurity and Digital Forensics, 9*(3), 45-61.

Acharya, K., & Ghimire, S. (2021). Pandemic preparedness and response in Nepal: Challenges and opportunities. *Journal of Public Health, 29*(3), 453-464.

Bhandari, D., & Gyawali, N. (2020). COVID-19 and Public health infrastructure in Nepal. *Health Policy and Planning, 35*(6), 686-693.

Bista, M. (2019). Integrating security policies in Nepal: A comprehensive approach. *Journal of South Asian Studies, 37*(4), 217-233.

Buzan, B. (2006). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies*. Cambridge University Press.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.). Sage Publications.

Dhakal, P. (2020). Enhancing cyber resilience in Nepal through public-private partnerships. *Cybersecurity Journal, 15*(1), 45-62.

Gautam, A., & Karki, R. (2020). Environmental degradation and its impact on food security in Nepal. *Journal of Environmental Management, 45*(3), 301-317.

Khanal, P. (2019). Transnational crime and border security in Nepal. *International Journal of Criminology, 22*(2), 133-148.

Poudel, S. (2019). Sustainable practices for combating deforestation in Nepal. *Forestry Journal, 34*(2), 187-202.

Rai, S. (2020). Institutional responses to cybersecurity threats in Nepal. *Information Security Review, 10*(4), 112-128.

Sharma, A., & Singh, B. (2021). Cybersecurity challenges in Nepal: A strategic overview. *Cyber Defense Review, 26*(2), 78-94.

Sharma, R., & Upreti, B. (2019). Regional cooperation and security in South Asia: Assessing the role of SAARC. *South Asian Survey, 26*(1), 1-17.

Shrestha, K. (2021). Policy coordination and non-traditional security in Nepal. *Nepal Security Review, 12*(1), 95-113.

Shrestha, P., & Adhikari, S. (2019). non-traditional security threats in Nepal: An emerging paradigm. *Nepal Journal of International Affairs, 15*(1), 55-73.

Thapa, R. (2018). Human trafficking and transnational crime in Nepal. *Journal of Human Rights, 14*(3), 201-217.

UNDP. (1994). *Human Development Report*. Oxford University Press.

United Nations Development Programme (UNDP). (1994). *Human Development Report 1994: New Dimensions of Human Security*. Oxford University Press.

-◆◆◆-