GAP BETWEEN CONVENTIONAL AND NON-CONVENTIONAL THREATS: UNDERSTANDING AND ADDRESSING MODERN SECURITY CHALLENGES

Brig. (R) Dr. ZEESHAN FAISAL KHAN
Former Editor "Hilal Magazine "
Inter-Services Public Relations Directorate.
zee34ian@gmail.com

ABSTRACT
In today's rapidly evolving global landscape, distinguishing between conventional and non-conventional security threats is crucial for ensuring both national and international stability. While conventional threats are state-centric, military-focused, and largely predictable, non-conventional threats such as terrorism, cyberattacks, pandemics, and climate change are diverse, unpredictable, and often transcend national boundaries. This paper delves into the historical progression of security threats, showcasing the transition from traditional military conflicts to more complex and multifaceted challenges. It explores the influence of both state and non-state actors, the role of globalization, and the growing impact of multinational corporations and global regulatory organizations. Highlighting the necessity for comprehensive and collaborative strategies, this study underscores the importance of advanced risk management, efficient resource utilization, and international partnerships to address the intricacies of modern security dynamics effectively.

KEYWORDS
Security Threats, Conventional and Non-Conventional, State Actors, Non-State Actors, Cyber Threats.

INTRODUCTION

Understanding the evolving nature of security threats has become crucial in an era marked by rapid technological advancements and global

interconnectedness. The dichotomy between conventional and non-conventional threats provides a framework for analyzing the complex challenges that nations and international organizations face in maintaining security and stability. Conventional threats typically refer to military challenges other nation-states pose, such as wars, invasions, or military standoffs. They involve state actors employing traditional methods of warfare, such as ground troops, naval forces, and airpower. These threats are often characterized by their visibility, predictability, and the use of formal military assets (Raffaele Marchetti 2018). Examples include interstate wars, invasions, or military occupations. Conventional threats are generally addressed through military preparedness, defense alliances, and diplomatic negotiations.

In contrast, non-conventional threats encompass a wide range of challenges that do not fit the traditional mold of warfare. These threats are diverse, including terrorism, cyber-attacks, economic instability, pandemics, climate change, and more. They often originate from non-state actors or natural phenomena, making them less predictable and more difficult to trace. Non-conventional threats transcend national borders and require a multidimensional approach for resolution, involving intelligence, counter-terrorism measures, cyber security, economic policies, and international cooperation (Ivana Luknar, 2021).

The Historical Context of Security Threats

The history of security threats is as old as civilization itself. Initially, threats were predominantly conventional, revolving around territorial conquests and power struggles between empires and states (H. G. Brauch, 2002). The two World Wars epitomized the height of conventional warfare with massive armies, navies, and air forces engaged in extensive battles. Korean War, Vietnam War, Falklands War, 1965 India-Pakistan war, 1967 Arab-Isreal war, Iran-Iraq War, Iraq-Kuwait War followed by Gulf War I (Desert Storm), Bosnian war (1992-1995), Azerbaijan-Armenia War, and more recent Russian-Ukrainian War are the few examples of convention war.

Gulf War II (19 March 2003) is a different phenomenon it started as a conventional war without the approval of the UNSC by a coalition of different countries led by the US and the UK invaded Iraq, the invasion led to the collapse of the Saddam Hussain's government (Britannica). United States President George W. Bush on May 1, 2003, declared "Mission Accomplished" but this started a new type of war, on Aug. 31, 2010, President Obama

announced the end of U.S. army combat missions in Iraq and the major armed forces personals were withdrawn (15 Dec 2011) there are a significant number of US forces still present on the ground in Iraq and are involves in the other type of war.

The Dichotomy Between Conventional and Non-Conventional Threats

The evolution from conventional to non-conventional threats reflects the changing dynamics of global power and the advent of new technologies (Jan Martin Rolenc, 2020). Today's security landscape demands a holistic approach that goes beyond traditional military strategies. It requires integrating intelligence, diplomacy, economic policies, technological solutions, and international collaboration. The threat of nuclear war and conventional military build-ups and conflicts were still prominent, introducing a new dimension of ideological and proxy conflicts, where both conventional and non-conventional tactics were employed.

Unlike conventional threats that have a more predictable pattern, relying on visible military assets and strategies. Non-conventional threats, by contrast, can be unpredictable and often emerge suddenly or from non-traditional sources, like non-state actors or natural phenomena, like climate change, has emerged as a security threat, with its potential to cause resource conflicts, mass migration, and destabilized regions (N. Akhtar, Inamullah, 2023).

RESOURCES ALLOCATION AND HOLISTIC APPROACHES TO SECURITY

To counter conventional threats, military preparedness, alliances, and the use of traditional diplomacy are required, as these threats often have a direct and immediate impact, typically confined to the military or political domain, but non-conventional threats require a broader range of tools, including intelligence gathering, counter-terrorism measures, cyber security strategies, economic policies, and international cooperation on issues like climate change and pandemics. Traditional defense budgets and resources are often oriented toward conventional threats and are usually covered through defense and foreign ministry spending, while non-conventional threats require different resource allocations, focusing on technology, intelligence, and other non-military areas, as non-conventional threats require a more integrated approach, involving

domestic policies, international collaboration, and often non-governmental actors.

In the rapidly evolving dynamics of global security, the distinction between conventional and non-conventional threats is paramount for formulating effective strategies and policies in today's complex and interconnected world. Conventional threats, typically state-centric and involving traditional military forces, are characterized by a structured nature and predictable outcomes (Muhammad Imran, Et. al, 2021). Non-conventional threats, however, are diverse and elusive, involving non-state entities like terrorist groups, cyber criminals, or even multinational corporations. This distinction is critical in understanding the full spectrum of modern security challenges, as the landscape is no longer dominated by conventional warfare alone. Non-conventional threats, often arising from globalization, technological advancements, and climate change, require nuanced approaches, including international cooperation, advanced technology, and diverse public policies.

Understanding the nature of these threats is crucial for appropriate resource allocation and effective response measures. While military spending may address conventional threats, non-conventional threats like cyber-attacks or pandemics necessitate investment in technology, healthcare infrastructure, and international collaboration (Solomon Ilevbare, Gayle Mcpherson 2022). The unpredictable nature of non-conventional threats demands sophisticated surveillance, data analysis, and a proactive approach. Additionally, these threats often require global cooperation for effective mitigation, transcending national borders, and challenging traditional legal frameworks.

A comprehensive understanding of both conventional and non-conventional threats is essential for advanced risk assessment and management strategies. This includes analyzing geopolitical trends and military intelligence for conventional threats and harnessing expertise in information technology, health sciences, and international law for non-conventional threats. Such comprehensive knowledge enables the integration of various approaches to form cohesive response strategies. For example, addressing cyber threats requires a combination of technical expertise, legal knowledge, and international cooperation, while combating terrorism might involve intelligence operations and socio-economic policies. (Muhammad Riaz Shad 2019)

This advanced understanding underscores the importance of education and training in security, adapting to technological advancements, and fostering international cooperation. As threats evolve, so must the training and skill set of security personnel, encompassing military, cyber-security, emergency response, and crisis management. The need for comprehensive knowledge in today's security landscape is multifaceted, encompassing risk assessment, response strategies, resource allocation, and predictive measures. With the increasing prevalence of hybrid threats, combining conventional and non-conventional elements, a flexible and dynamic approach to security is necessitated (Mikael Weissmann, 2021). As the world grapples with a broad spectrum of threats, this comprehensive understanding becomes the cornerstone of effective security management, underlining the need for enhanced international cooperation and a shared understanding of these complex issues.

NON-STATE ACTORS AND THE SECURITY OF THE STATE

Non-state actors are the entities that participate in international relations or domestic affairs without being officially affiliated with any government. Unlike state actors, which are characterized by their sovereignty and are typically represented by governments, non-state actors can encompass a broad range of entities, each with its own structures, goals, and methods of influence (Muhittin Ataman, 2003). The term "non-state actor" is a broad umbrella that includes a diverse array of groups and organizations.

These actors can be divided into several categories based on their nature and objectives. One major category includes non-governmental organizations (NGOs), which are typically non-profit entities that operate independently of any government. NGOs and INGOs are often involved in humanitarian, environmental, educational, or advocacy work and can range from small, grassroots organizations to large, international entities. These organizations play a crucial role in global and local issues, often filling gaps left by governments and providing critical services or advocacy on behalf of vulnerable populations. Examples include the Red Crescent, Greenpeace, Amnesty International, Edhi, Alkhidmat Trust, and Akhuwat.

Another significant category of non-state actors is multinational corporations (MNCs). These are large companies that operate in multiple countries and often

have a significant impact on local economies, politics, and environments. MNCs can influence government policies through lobbying, economic leverage, and sometimes even through more direct forms of intervention (Violeta Iftinchi, H. Gheorghe 2018). Their operations and business practices can have profound implications for international trade, employment, and environmental standards.

Terrorist groups, insurgent movements, and rebel forces also fall under the umbrella of non-state actors. These groups typically use violence or the threat of violence to achieve their goals, which can range from political change to territorial control. Unlike NGOs and MNCs, these actors often operate outside of the legal and ethical frameworks that govern international relations. Their actions can have significant impacts on regional and international security, humanitarian situations, and the political landscape. (Aarish Ullah Khan, 2005)

Religious and cultural organizations constitute another form of non-state actors (James Tiburcio, 2010). These entities can wield significant influence over social norms, values, and behaviors. In some cases, religious groups can have considerable political influence, shaping government policies and public opinion. Cultural organizations, on the other hand, often play a role in preserving heritage and promoting cultural understanding, thus influencing societal dynamics and international perceptions.

Another growing category includes online communities and networks. In the digital age, these entities, which can range from activist networks to online forums, have become increasingly influential. They are known as civil societies and those who are active online are called influencers, they can mobilize public opinion, organize social movements, and even affect the outcomes of political processes through information dissemination and digital advocacy.

According to Englehart 2016, the impact of non-state actors on state security is a dynamic and evolving issue. States must continually adapt their strategies and policies to address the diverse challenges posed by these actors. The nature of these challenges also necessitates international cooperation and coordination, as non-state actors often operate across national boundaries, making unilateral state action less effective in addressing these security concerns.

Impacts and Threats from Non-State Actors

The most direct and apparent impact of non-state actors on state security comes from terrorist organizations and insurgent groups. These entities challenge state authority and security by employing violence and intimidation tactics. Terrorism, in particular, seeks to destabilize governments and societies, often targeting civilians to create an atmosphere of fear and uncertainty. Insurgent groups may engage in prolonged armed conflicts against state forces, as we saw in the Naxal-Maoist insurgency and Baloch Liberation Organization in the case of India and Pakistan respectively, aiming for political change or territorial control. The threats posed by these groups often necessitate significant state resources in counterterrorism and counterinsurgency operations, intelligence gathering, and homeland security measures.

In the digital age, non-state actors operating in cyberspace, such as hacker collectives or cyber-terrorist groups, pose a new kind of threat to state security. They can disrupt critical infrastructure, steal sensitive information, and influence public opinion through misinformation campaigns. We have seen that several federal and local governmental websites and companies' data were breached and hacked by these cyber terrorists, National Electric Gridline was also disturbed by these elements (Christiana Parreira, 2020). The anonymous and borderless nature of cyberspace complicates the ability of states to respond effectively to these threats (Michael N. Schmitt, Sean Watts).

THE INFLUENCE OF GLOBAL INSTITUTIONS, MNCs, AND NGOs ON STATE SECURITY

The use of commercial entities, such as Multinational Corporations (MNCs), and the influence of global institutions and regulators, like the International Monetary Fund (IMF), World Bank, Financial Action Task Force (FATF), and Nuclear Suppliers Group (NSG), have profound direct and indirect impacts on state security. These entities, through their economic and regulatory powers, can exert significant influence over national policies, economic stability, and even sovereignty. MNCs, with their vast resources and global reach, can exert considerable influence over economies and labor markets. Their decisions on investment, production, and employment can have significant implications for the economic health of states. The ability of MNCs to shift capital and resources across borders allows them to maneuver in ways that can challenge the

economic policies and priorities of individual states. In some scenarios, the economic clout of these corporations can rival or even surpass that of the states in which they operate, leading to a form of dependence where state decisions may be heavily influenced by the interests of these corporations. The power wielded by MNCs and global regulatory bodies can sometimes challenge the sovereignty of states. This challenge manifests in various ways, such as when states modify their internal policies and laws to attract foreign investment or comply with international regulations. The economic dependencies created by these adjustments can lead to a situation where states find themselves constrained in their policy-making, effectively ceding aspects of their sovereignty to external entities (In Song Kim Helen V. Milner, 2016)

Organizations like the International Monetary Fund (IMF), World Bank, Financial Action Task Force (FATF), and Nuclear Supply Group (NSG) play crucial roles in shaping global economic and security policies. The IMF and World Bank, for instance, provide financial assistance and guidance to countries but often attach stringent conditions to their support (Daryna Abbakumova, 2019). These conditions typically require significant economic reforms, which can lead to changes in national policies and priorities. The FATF and NSG, focused on financial crimes and nuclear proliferation respectively, exert influence by setting international standards and norms. Non-compliance with these standards can result in sanctions or other forms of international isolation, effectively arm-twisting states into alignment (Mariam Shah Salman Javed, 2023).

While these entities primarily influence economic policies, the ramifications for state security are significant. Economic instability can lead to social unrest, weakening the internal security of a state. Dependence on international financial institutions or MNCs can compromise a state's ability to independently address its security needs. Moreover, compliance with international regulatory standards, while often beneficial, can also force states to allocate resources in ways that may not align with their immediate security concerns or public welfare. (Martina Steinbockova, 2004)

NGOs often play a role in highlighting human rights abuses, environmental issues, and other matters that can be sensitive for states (Upasha Kumari, 2023). While they contribute positively to global governance and humanitarian efforts, their activities can sometimes be seen as a challenge to state authority,

especially when they expose state failures or misconduct. NGOs and INGOs sometimes push foreign agendas and create division in society by promoting their chosen groups and individuals (N. V. Burlinova, 2022).

CONCLUSION

ADAPTING TO GLOBAL SECURITY PARADIGMS

The influence of various non-state groups, particularly those driven by specific ideological, religious, or political agendas, on state security is substantial and multifaceted. By shaping societal values and norms, these groups can have a profound impact on domestic politics and policies, sometimes leading to radicalization and posing significant internal security challenges. Groups with strong ideological, religious, cultural, and ethnic beliefs can influence public opinion and societal norms. This influence can manifest in various ways, such as through education, media, social movements, or public discourse. When these groups successfully embed their values and perspectives into the fabric of society, they can indirectly influence the political agenda, leading to changes in policies and laws that reflect their beliefs and interests. The ability of these groups to mobilize public support or opposition can significantly impact domestic politics. Politicians and policymakers, seeking to align with or respond to public sentiments, may adopt positions or enact policies that cater to the interests of these influential groups. In some cases, these groups may propagate extremist ideologies that advocate for radical changes and are unacceptable to other groups and communities. These radicalized individuals or groups may resort to violence as a means to achieve their objectives, posing a direct threat to internal security and stability (Anselm Hager, Kunaal Sharma, 2016). Tahreek-e- Taliban Pakistan (TTP), Tehreek Labbaik Pakistan (TLP), Islamic State (ISIS), Vishva Hindu Parishad (VHP), Shlom Asiraich, Religious Zionist Party (Tukma) are a few examples.

Throughout history, the landscape of global security has been significantly shaped by the presence and actions of non-state actors. These entities, which range from pirates, rebel groups, religious cults, mercenaries, gangsters, warlords, terrorist organizations, insurgent groups, criminal networks, to non-governmental organizations (NGOs), possess varied motivations, capabilities, strategies, and goals. Their diversity in characteristics, design, and reach necessitates a deep understanding of their dynamics to strategize effective

responses. The impact of non-state actors on state security is profound, often exploiting vulnerabilities in state institutions and infrastructure to advance their objectives (Bashir, Et. Al, 2023). Their influence can be both direct and indirect, posing physical threats, undermining governance, and destabilizing the social and political fabric of states.

In the domain of international and domestic security, non-state actors have emerged as formidable forces, fundamentally altering traditional security paradigms (T. Jamil, M.T. Rashid, S. Minhas, 2023). Terrorist organizations and insurgent factions are particularly conspicuous in this regard. Employing tactics such as guerrilla warfare, bombings, and cyber-terrorism, they directly challenge state authority and seek to destabilize established political structures, often driven by political or ideological objectives. Their transnational nature complicates the ability of individual states to counteract their influence, requiring a shift towards international cooperation and the development of new security strategies.

Multinational corporations (MNCs), primarily economic entities, wield significant power that can indirectly impact state security. Their influence on global markets and policies creates economic dependencies for states, potentially leading to exploitation and interference in domestic policy decisions. In some cases, the economic power of MNCs rivals that of states, challenging state sovereignty, especially in smaller or economically vulnerable nations. (In Song Kim, Helen V. Milner,2019)

The digital domain has introduced new players in the form of cyber actors, including hacker collectives and state-sponsored cyber units (Broadhurst, Et. Al, 2014). This emerging threat is rapidly growing, as these actors possess the capability to disrupt critical infrastructure, steal sensitive information, and manipulate public opinion. Such activities pose severe risks to national security, economic stability, and democratic processes. Transnational criminal networks involved in illicit activities like drug trafficking, human trafficking, and arms smuggling undermine state authority and legal frameworks. Their operations contribute to widespread corruption, violence, and instability, further challenging state security.

The dynamics of non-state actors in the security landscape underscore the evolving nature of global threats. Traditional state-centric models of security are increasingly inadequate in addressing the complexities introduced by these

actors (Alam Saleh, 2011). As globalization progresses, the interconnectedness of these challenges becomes more apparent, necessitating adaptive and collaborative approaches to security. States must balance the need for robust security measures with the preservation of civil liberties and human rights, ensuring that responses do not inadvertently exacerbate the challenges they aim to address.

The influence of non-state actors on global security is a critical aspect of contemporary international relations. Their diverse nature and capacity to exploit state vulnerabilities present unique challenges. Understanding these entities, their motivations, and their methods is essential for developing effective security strategies. In response to the multifaceted threats posed by non-state actors, states have to adopt various strategies, including the deployment of military force, enhanced intelligence gathering, and fostering international cooperation. Effectively countering these threats requires a nuanced understanding of the motivations and grievances driving non-state actor activities. Moreover, analyzing the political, economic, and social impacts of countermeasures both in the short and long term is crucial. Collaboration between states, international organizations, and civil society is vital in developing comprehensive and sustainable countermeasures. The international community's collective response to these non-state actors will significantly shape the future of global security and stability.

REFERENCES

Aarish Ullah Khan, "The Terrorist Threat and the Policy Response in Pakistan", 2005.

Alam Saleh, "Broadening the Concept of Security: Identity and Societal Security", 2011

Anselm Hager, Kunaal Sharma, "The Determinants of Religious Radicalization: Evidence from Kenya", 2016

Brauch, “Security Threat, Challenges, Vulnerability and Risk” 2002

Britannica: https://www.britannica.com/event/Gulf-War

Christiana Parreira, "Power politics: Armed non-state actors and the capture of public electricity in post-invasion Baghdad", 2020

Daryna Abbakumova, "The Role of the World Bank and the IMF in the International Financial System and the Human Sphere", 2019

Dr Siraj Bashir, Jahanzeb Khan, Muhammad Danish, Walwala Bashir, "Governance and Development Challenges in Balochistan", 2023.

In Song Kim Helen V. Milner, "Multinational Corporations and their Influence Through Lobbying on Foreign Policy"

In Song Kim, Helen V.Milner, "Multinational Corporations and their Influence Through Lobbying on Foreign Policy" 2019

Ivana Luknar, "Cyberterrorism threat and the pandemic" 2021

James Tiburcio, "Human Security in Angola: The Role of Religious Non-state Actors" 2010.

Jan Martin Rolenc, "Technological Change and Innovation as Security Threats" 2020

Mariam Shah Salman Javed, "Chapter: A Critical Assessment of Pakistani Counter-Terrorism Financing Measures - Book 'Countering Terrorist and Criminal Financing: Theory and Practice", 2023

Martina Steinbockova, "Multinational Corporations and Nation States: Partners, Adversaries or Autonomous Actors?, 2004

Michael N. Schmitt, Sean Watts, “Beyond State-Centrism: International Law and Non-state Actors in Cyberspace” 2016

Mikael Weissmann, "Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone" 2021

Muhammad Imran et al, Non-Traditional Security Challenges 2021

Muhammad Riaz Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan"

Muhittin Ataman, “The Impact of Non-State Actors on World Politics: A Challenge to Nation- States” 2003

N. Akhtar, Inamullah, "Climate Change: Rising Security (Non-Traditional) Threat to Pakistan" 2023.

N. V. Burlinova, "The Role of NGOs in International Relations and Public Diplomacy," 2022

Neil A. Englehart, "Non-state Armed Groups as a Threat to Global Security: What Threat, Whose Security?" 2016

Raffaele Marchetti, “The Role of Non-state Actors in the Future of Global Governance and Int’l Security” 2018

Roderic G. Broadhurst, Peter Grabosky, Mamoun Alazab, Steve Chon, "Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime", 2014.

Solomon Ilevbare, Gayle Mcpherson, "Understanding COVID-19: A Hybrid Threat and Its Impact on Sport Mega-Events. A Focus on Japan and the Tokyo 2020 Olympic Games" 2022

Tahir Jamil, Muhammad Tahir Rashid, Shaid Minhas, "Terrorism and Extremism as a Non- Traditional Security Threats in Post 9/11: Implications for Pakistan's Society and Politics", 2023

Upasha Kumari, "Exploring the Role of NGOs in Addressing Gender-Based Violence Against Women, "2023

Violeta Iftinchi, Hurduzeu Gheorghe "How Multinational Corporation Use Lobbying and Advocacy to Mitigate Political Risks" 2018