



**Non-Traditional Security Paradigm and Role of Intelligence:
Challenges of Transformation**

Muhammad Ajmal Abbasi¹

Abstract:

The triumphant elation of neo-liberal global order against the Marxist challenge after the cold war was soon replaced by a somber recognition that the world is still far from being a peaceful place. Post-cold war international environments had started revamping the global political order where the traditional notion of territorial security has been getting increasingly irrelevant. While conflicts in kinetic domain are persistent in some form, the broader concept of security highlights gravity of constantly evolving non-traditional threats. This emerging challenge, primarily categorized among the non-military threats, has caused a functional dilemma for the national security apparatus. Apparently, National Intelligence Community (NIC) is the most viable mechanism to anticipate, identify and forecast the non-traditional security threats. However, without undertaking necessary reforms, conventionally trained and organized NIC seems least prepared for the evolving challenges. It is, therefore, imperative that the intelligence agencies are adequately transformed and structured for the impending task.

Keywords: National Intelligence Community, Security, Conflicts, Conventional Threats, Non-traditional Security,

INTRODUCTION

Security paradigm was anticipated to decisively evolve after the culmination of cold war amid rising concerns with the devastating impact of global mayhem on humanity. The dawn of 21st century was expected to be the era of peace and prosperity with an apparent demise of bipolar as well as earlier multipolar global rivalries and violence. Capitalist triumphant was projected by many as a stabilizing factor, with the contending Marxist and Fascist economic ideologies finally giving in after one another. It was also widely projected that with the end of ideological conflicts among nations, the primacy of 'state' as the sole and legitimate referent of security, would undergo a paradigm shift. While the state continues to be the main referent of security in the contemporary era opposed to what many scholars perceived, the concept of security has evolved immensely from a 'narrow' to a much 'broader' framework. Broadening of this security framework with the emergence of several new domains, has introduced many unperceived challenges for the national security hierarchies all over the world. Consequently, 21st century has introduced diverse and unprecedented dimensions

¹ Affiliated with the National Institute of Intelligence and Security Studies (NISS), Islamabad, Pakistan. Email: ajmalabbasi23@yahoo.com.

of national security threats that are vastly different in construction compared to the traditional modes.

Contemporary security challenges have moved beyond the typically originated threats by the armies of other nation states, to the appearance of non-state actors, and hybrid intra-state conflicts (Srikanth, 2014: 60). During the current millennium, the risks of large scale armed conflict or inter-state wars have generally diminished and the international community is now increasingly threatened by the security challenges evolving from multifaceted local and transnational sources that are mainly non-military in nature (Caballero-Anthony & Cook, 2013: 1). Although, this contention claims declining prospects of major inter-state armed confrontations, however, ruling out kinetic threats altogether is out of question. Essentially, fading large scale military conflicts lead to various dimensions of asymmetric warfare that can also be classified among non-traditional or unconventional security threats. There is an ongoing debate over the modes, means and methodologies of non-traditional security threats, however, the consensus seems to be developing on the perspective that these challenges can be instigated by both, the natural or humanly constructed sources. The broader spectrum of all these issues is acknowledged as the threat to a nation's sovereignty, territorial integrity and safety of the societies as well as individuals (Anthony et al., 2006: 1).

It is now being largely accepted that the evolving contemporary challenges can potentially inflict highly detrimental effects by damaging the law and order dynamics of any state, thereby not only threatening the security of the targeted nation-state but the entire society also (Singh & Nunes, 2016: 9). Growing cognizance about the persistently rising significance of non-traditional security threats has led to the necessity of undertaking a wholesome review of the national security strategies. With shifting of focus from predominantly military threats where kinetic response has been the eventual option, emergence of security challenges from other domains warrants corresponding approaches. Consequently, the varying dimensions of contemporary security threats, classified mainly in the non-traditional spheres, have led to the belief that security can only be ensured from 'a balance of all instruments of foreign policy' (Snyder, 2012: 10). States would be required to prepare multi-dimensional responses for the equally detrimental but diversified security challenges emanating from both, conventional as well as unconventional sources, even simultaneously. Besides close coordination among all national security institutions of the state, 'whole of nation' response would be inevitable where each member of the society develops awareness about the evolving challenges.

According to another perspective, the nonconventional security concerns appear to be beyond the ambit of national security intelligence, which is essentially designed to focus on conventional threats. These non-traditional security dimensions logically fall in the jurisdiction of civil governments, and expected to be taken care of by the designated institutions of a state. Does it imply that the conventional intelligence agencies need to stay indifferent to these challenges and only concentrate on the traditional threats? Moreover, shall any involvement in probing or forecasting these emerging modes of security issues be regarded as the interference in the sphere of civil administration by the intelligence? And would it be possible to suggest that the non-traditional security challenges evolve in silos without impacting the entire spectrum of national security? In essence, it would be risky to even contemplate the attainability of conventional national

security without taking into consideration the influence of unconventional threats. This paper contends that despite the leading responsibility of civilian institutions, the role of national security intelligence cannot be disregarded against all these evolving domains of security challenges. Intelligence agencies can play a part in the identification and forewarning of every concern that can potentially undermine the national security quest of a state, irrespective of the threat being unconventional or conventional.

LITERATURE REVIEW

The subjects of non-traditional security and national security intelligence are among well-deliberated fields globally, especially among the scholars of the US and UK. However, both the paradigms despite being among popular research topics, have rarely been discussed collectively as one subject. Moreover, there are divergent views on non-traditional security as well; for some it is a non-military phenomenon aggravated by the nature, while few others view its many dimensions as the humanly orchestrated national security challenges. The debate is, nevertheless, unending, however, this paper focuses on all the dimensions of non-traditional security, which are detrimental to national security, whether instigated by the nature or deliberately crafted by the adversaries. Contrary to the US and West, the subject of intelligence is mostly viewed as a sensitive domain, especially in regions like South Asia and seldom deliberated publically.

Srikanth (2014), Caballero-Anthony & Cook (2013) as well as Singh & Nunes (2016) view non-traditional security threats as non-military in nature, involving non-state actors and hybrid intra-state conflicts and, thus, not only the challenge to nation-states but the entire society. For Anthony et al., (2006) these issues threaten national sovereignty, territorial integrity and the societies, while Snyder (2012) suggest 'a balance of all instruments of foreign policy' for countering such challenges. Krause & Williams (2002), Jarvis & Holland (2014), and Buzan et al., (1998) regard security as a contested subject, which is focused on survival and incorporates many more dimensions besides military, especially after the cold war. Chalk (2000), Booth (2007), Bilgin (2003), Anthony et al., (2006) and Aydın (2011) deliberate upon the shifting paradigm of security and suggest it has fallen in the lower end of conflict spectrum. Dalby (1995), Job (1992), Thomas (1987) and Swain (2012) highlight the internal drivers of evolving national security dynamics and, its effects on various spheres of nation states. Caballero-Anthony (2016), Craig (2007), Schilling (2002) has deliberated as to how conventionally leaned state-centric, military focus on the security paradigms is being replaced by non-traditional security factors such as political, economic, environmental, and information spheres.

Breckinridge (2019), Rathmell (2002), Moore et al., (2020), and Cavelty & Mauer (2009) emphasize the importance of comprehensive, and accurate information for policy formulation, influence of information revolution, evolving strategic dynamics, and intricacies of post-cold war challenges for the intelligence. Lahneman (2011), Sims (2022), Nicander (2011) and Quiggin (2007) underline the need of greater awareness among intelligence officials, significance of providing decision advantage, thinking ahead to anticipate the future and adapt, and the prospects of broader role in the evolving world. Berkowitz & Goodman (2000), Sims (2022), and HersHKovitz (2022) point out the impact of communication technology on the intelligence functions, especially the acquisition of information. Goldman (2024) stresses about the importance of communication art for the intelligence officials, while Omand (2014), Allen (2012) as well as De Graaff (2014) highlight rising

significance of analysis and developing capacity of situational awareness, explanation, prediction and strategic notice. Bury & Chertoff (2020), Bohm (2004), and Hatlebrekke (2019) identify critical thinking as the most vital attribute of intelligence officials in the post-cold war era. Foryst (2009) and Ireland (2017) suggest that intelligence organizations prefer to function in silos, whereas Lahneman (2011) and Nicander (2011) emphasize the inevitability of inter-agency cooperation. Biltgen & Ryan (2016) have highlighted various evolutionary phases of the American intelligence that is equally relevant to the intelligence setups of other nations as well.

RESEARCH METHODOLOGY

The descriptive research is being employed to explore the rising primacy of non-traditional security in the post-cold war arena, and how this shifting paradigm has necessitated transformation of national security intelligence. Descriptive research methodology is helpful for the assessment of ever evolving security challenges to a nation state, and continuous evaluation of these non-military threats. The paper also strives to evaluate the role of intelligence agencies during the no war situation by descriptive technique, the environments where natural as well as deliberately human constructed challenges would hold sway. Research work mainly relies upon the feedback on the subject extracted from pertinent books, research papers, as well as input from other available sources including the newspapers.

NATIONAL SECURITY: FROM CONVENTIONAL TO EVOLVING PARADIGM OF NON-TRADITIONAL DOMAIN

Security: Perceptions and Evolutions

Security is generally viewed as a contested term that has numerous connotations including those, which may not necessarily be linked or plausibly related with conventional understandings (Krause & Williams, 2002: 6). The contested view on security is essentially reflective of not only divided opinions on the concept, but also diversified interpretations stimulated by distinctive strategic environments. The historically persistent divergences on the subject, nevertheless cannot undermine a shared quest of surviving against all odds, in every environment and mitigating any potential risks. Perhaps the simplest definition of security is a condition wherein the ultimate desire of the 'survival of someone or something is not at risk' (Jarvis & Holland, 2014: 27). While national security and threat perceptions of a state have traditionally been dominated by the military aspect, however, this contention was never universally accepted. There has always been counter argument on, sometime, exaggerated notion of conventional security and many scholars actually looked beyond the military conflicts while debating the subject. Apparently, the mere survival cannot be the desired end-objective being pursued by nation states; rather national security would contemplate as to how and in what kind of environments to survive.

It is interesting how security is being perceived by various players, whether these are traditional states or the non-state actors, especially when taken in to account the aspired values, thresholds and interests. Krause & Williams (2002) suggest that the conventional understandings of security implies the existence of the threat including the possibility of the employment of military force; surveillance, may it be physical or technological for acquiring information, and the cautious demarcation of the spheres that have been subject to technological patrolling and control (p. 7). According to Buzan et al., (1998), security 'is about survival- It is when an issue is presented as

posing an existential threat to a designated referent object, traditionally, but not necessarily, the state, incorporating government, territory, and society' (p. 21). Here, the traditional understanding of the security concept is broadened with additional spheres other than the 'state' as referent objects that has legally as well as ethically, a validated right of survival. Buzan et al., (1998) further elaborate various referent objects including: 'the state (military security); national sovereignty or an ideology (political security); national economies (economic security); collective identities (societal security); species or habitats i.e. environmental security' (pp. 22-23).

The global arena during 20th century witnessed two immensely devastating, large scaled and violent Great Wars, while the decades thereafter infused the tantalizing agony of cold war turning in to an unprecedented nuclear conflict. Until the end of cold war, the global concern has naturally been on the perils of facing a 'never before' scenario, threatening even the extermination of human life due to the potential breakout of another world war, involving nukes. The end of cold war rivalry generated optimism regarding the prospects of an independent, and peacefully coexisting world, since the triumph of neo-liberalist global economic order promised mutual gains to all. It was perceived that after the cold war rivalry, the evolving global order would lead towards greater peace and alleviate potential threats to the international stability. However, contrarily, this initial euphoria quickly evaporated with the rising concerns about the security threats evolving towards 'lower end of the conflict spectrum,' and assuming greater prominence (Chalk, 2000: 1). Resultantly, the nation states are presently required to focus beyond the military power and external sources, and prepare to cope with a far broadened spectrum of evolving challenges in the contemporary world (Singh & Nunes, 2016: 3).

The opponents of established conception of security, based on the conventional narrative of interstate framework, now insist to abandon this traditional assumption, and advocate post-Cold War approaches, highlighting threats faced not only by the states, but the non-state actors also (Bilgin, 2003: 207). According to Booth (2007), security was, for a considerably long time, identified among the 'common-sense, pre-defined' terms that has been unproblematic, unless critically viewed (p. 96). Accordingly, in the views of many scholars, an exclusive focus on armed conflicts and interstate crises, implies that the security concerns of developing states are being largely neglected while theorizing the concept (Jarvis & Holland, 2014: 28). In the view of Booth (2007), the 'conventional convictions' were linked exclusively with the military terrain, especially during the Cold War era when the focus has been on military power as well as strategic relationships among the states (p. 96). It leads us to the notion of 'structural violence,' a term first coined by Johan Galtung (1971), which refers to mainly unintentional, but avoidable evils, that are without the obvious perpetrators, but cause sufferings 'beyond the direct physical violence' instigated by someone (Jarvis & Holland, 2014: 29).

Emergence of Non-traditional Security Challenges

National Security has traditionally been referred to as the military dimension of inter-state affairs; however, since the early 1990s, it is no more limited to a nation state and its survival from external threats, but also includes domains such as societies and human collectivities (Anthony et al., 2006: 1). The debate on national security is, therefore, facing a paradigm shift from conventional conception, which had mainly been dominated by the traditional inter-state conflicts. Whereas, the prospects of conventional security threats cannot be ruled out, focus is now centered more on

previously lesser emphasized non-traditional challenges. Resultantly, the identification and cataloging of security threats, has been under transformation from traditional to non-traditional domains. Present threat environments are, thus, characterized with the evolving but predominantly non-kinetic threats such as environmental degradation, organized crime, economic insecurities, illegal immigration etcetera (Aydın, 2011: v). In addition, aspects like infectious diseases, climatic degradation, narcotics, human trafficking, and transnational crimes, primarily regarded to be the non-military concerns, are also classified among the non-traditional security issues (Anthony et al., 2006: 1). Hence, environmental, social, and economic challenges as well as the evolution of cyber-warfare with the ongoing technological progression, have decisively transformed the future warfare.

Although historically, security challenges other than regular military threats have always existed, but did not necessarily emanate from conventional armed conflicts or the inter-state wars. The contemporary security issues are mainly the non-military threats, but can potentially threaten a nation's political as well as social integrity and the health sector, originating either from within or transcending the borders, and 'can-be termed as low-intensity conflicts' (Singh & Nunes, 2013: 67-68). These emerging security challenges are, thus, more diffuse as well as opaque, categorized as 'threats without enemies', and often exacerbated by an internal cause rather than the external source (Chalk, 2000: 2). Furthermore, security threats in the contemporary world do not, necessarily, emanate from external sources alone; the pre-existent domestic vulnerabilities can also be exploited by the adversaries, even without declaration of hostilities. Resultantly, conventional spatial strategies of national security, largely based on territorial integrity, are reckoned to be inadequate against these challenges, which may not explicitly be external, but likely to have emanated from domestic problems (Dalby, 1995: 186). Thus, the post-cold war debate on the concept of security, also largely focuses on the hazards of domestic insecurity that stimulates numerous exploitable vulnerabilities.

The challenges to national stability in the present world continue to evolve with highly-fluid strategic dynamics, notwithstanding, even the absence of distinctly pronounced global ideological divergences. With the line distinguishing war and peace blurring, unconventional security threats assuming much more prominence, and standard notions of sovereignty receding, the modes of conflict are becoming more intricate. Hence, historically accepted state-centric paradigms are losing the capacity of dealing with the evolving issues, which can be instigated within national borders but may have consequences transcending international boundaries as well as jurisdictions (Dalby, 1995: 186). The deliberately orchestrated non-traditional security threats against a state, presumably, reflect that the instigating power is avoiding an all-out conflict and prefers low intensity effort for desired outcome. Apparently, the aggressor maintains a low key involvement while inciting exploitable vulnerabilities in the targeted state and provokes discontent, violence, or even revolt. Most of the developing states are vulnerable to these threats, since they lack a socially cohesive society where several communal groups strive for their rights; unpopular ruling regimes lack legitimacy or represent the interests of a specific clique; and, state faces dearth of functionally effective and uncontroversial institutions (Job, 1992: 17-18).

Domestic Instability: Non-traditional Security Challenges of the Developing World

The literature on security mainly projects the contemplation of the advanced states on the subject, while mostly ignoring the challenges confronted by the underdeveloped world. The neglect or lack of emphasis on non-military dimensions of national security, affecting the underdeveloped states, had been visible even during cold war era. Thomas (1987) is of the view that the Third World states, being largely former colonies and with an inherent artificial constructs, face the challenges proliferating not only due to ethnic, religious and linguistic divergences but the fragile and divisive social, economic as well as political structures, thus making domestic security a major concern (p. 2). Moreover, developing or weak states primarily suffer for their incapacity in shaping the international environment favorably, and this lack of external control inhabits their ability of managing domestic economic, social as well as political domains (Thomas, 1987: 4). Consequently, for the developing states, security implies something more than simply managing to survive within an unfavorable status quo of prevalent global order (Jarvis & Holland, 2014: 28). It denotes an international system, wherein they have reasonable opportunities for state building with minimal of socio-economic and political disparities, evils that instigate domestic insecurity.

The internally driven sources of conflict or dissent, that stayed muted during the cold war era, are more pronounced among the de-colonized states, majority of whom emerged on global arena rather swiftly and without much groundwork. These internal divergences, which are reckoned to be highly conducive for non-traditional security challenges, result in a contested notion of national security among various segments of the society. Essentially, these contentious environments reflect a situation wherein, security environments for majority of the population are least conducive; the state institutions have little capacity for ensuring services and order; and each sphere of the state is susceptible to external influences, interventions and manipulations, whether stimulated by other states, communities or multinational corporations (Job, 1992: 18). Furthermore, among fragile and weaker states, the intricately contentious nation-building process, which was required to be simultaneously initiated in the political, social, economic as well as security domains, added a highly delicate challenge for the relatively inexperienced regimes (Swain, 2012: 3). The setbacks emanating from the often flawed, politically inspired and unproductive nation-building drives have, therefore, been fueling socio-economic dissention among aggrieved ethnic groups that sometimes, exacerbated irreconcilable internal conflicts.

It is pertinent to note that national security concerns of the developed and developing states, in the contemporary world are hard to equate in many domains, as the threat perceptions are often varied. The resource rich developed world presently does not contemplate large scale military conflicts, but continues to be perturbed with nonconventional security concerns, mostly emanating from external sources. These externally instigated threats may include terrorist activities, mass migrations from conflict ridden as well as resources scarce parts of world, narcotics trade, transnational criminals, pandemics, and so on. On the other hand, underdeveloped nations may not be confronted with an external threat but still their national security, and even survival continue to be in a precarious situation. Consequently, for the developing states, national security has mostly internal rather than external dimensions, where the 'regime' instead of 'state' is often being confronted, and where conflicts usually occur due to the irreconcilable demands arising from ethnic, religious, as well as national community aspirations (Job, 1992: 3). Thus, according to Bilgin

(2003), those who study Third World security, usually criticize near absolute focus on the intra-state conflicts, and crises that have traditionally been dominating the thinking about security (p. 205).

Contemporary Security Dynamics: A Shifting Paradigm

In the conventional wisdom, a nation state has to predominantly rely on military means for protecting its territorial integrity, not only against external intrusions, but even if domestically challenged by the violence. Emergence of present day security threats has, nonetheless, led to the modification of this established notion wherein, reliance on military means alone for national security is declining. Caballero-Anthony (2016) is of the view that in a broadest context, the concept of non-traditional security reflects the trend of shifting away from the conventionally leaned state-centric, military focus on the security paradigms (p. 23). Thus, in comparison to typical military threats, various other security factors such as political, economic, environmental, and information spheres, besides resource scarcity, terrorism, weapon proliferation, pandemics, transnational crime, narcotics trade, piracy, mass migrations, and so on, are deemed far more concerning (Craig, 2007, p. 103). Some of these deliberately executed security threats may include dimensions such as: weapon proliferation; electronic warfare; industrial as well as economic espionage; urban or guerrilla warfare; and violent insurgencies, especially terrorism (Schilling, 2002: 3). Additionally, modern day world has also been witnessing numerous variants of political warfare wherein, national security has been challenged with regime change operations, economic sanctions, and several other constrictions.

It is being largely accepted that the security threats 'at the lower end of the conflict spectrum' have assumed more prominence, owing to the escalating fluidity that has been shaping global political dynamics (Chalk, 2000: 1). The national security challenges in such environments are intriguing and highly complicated, with various domains intertwined and often trespassing diverse spheres. According to Chinese perspective, non-traditional threats are transnational in nature; can transcend the military sphere; mostly these may be unpredicted as well as instantaneous; and many at times, intertwined with traditional security challenges (Craig, 2007: 102). The contention that these threats can often be interwoven with conventional threats, sounds closer to the concept of hybrid warfare. Presumably, this perspective brackets all such hazards with the deliberately executed adversary's actions that may exacerbate an ongoing crisis in any domain. Prevalent global dynamics have, thus, least semblance with the cold war era where not only the threat was well recognized and conceivable, but the identity of the perpetrators was never in much ambiguity. Consequently, present world is a 'world of grey area phenomena,' wherein the conventional military-based notions of power and security may have only a fractional relevance (Chalk, 2000: 2).

It may be pertinent to suggest that the argument for the need of enhancing focus on non-traditional security threats does neither dismiss, nor even undermine the relevance of conventional warfare. It only highlights several new challenges to national security, which may be beyond the established paradigm of conventional conflict, but equally devastating and way more complicated. The core argument against the primacy of traditional security concept is, its near exclusive focus on state as well as territorial integrity, that tends to neglect other drivers of 'disorder' stemming from conflicts other than interstate wars, which emanate from issues linked with people's identities, historical contexts and resources (Caballero-Anthony, 2016: 22). In the hindsight, extending debate on non-

traditional security reflects shifting of focus from conventionally inspired territorial security to the human security. The post-Cold War, security perceptions, therefore, not only highlight the military realities prevalent in the contemporary world, but congruently underline the significance of evolving challenges in the political, economic as well as social domains (Snyder, 2012: 1). Consequently, it becomes vital to detect, pinpoint and categorize these evolving threats by all available resources, especially intelligence, and evaluate potential damage, likely means of attack as well as preventive strategies (Schilling, 2002: 8).

Intelligence and Non-Traditional Security Challenges

Interplay of Intelligence and Security

The contemporary global system reflects interplay of several state and non-state actors, each pursuing survival, security, an influential role and capacity of enhancing its political, economic and strategic rewards. These aspirations, regarded to be legitimate, rational as well as common to every actor, are always contested and unviable to abandon at any cost. Resultantly, global players - particularly the nation states - devise all conceivable mechanisms, methodologies and means to surpass their competitors in terms of prior information, better anticipation and superior policies. Such aspirations may not be attainable without an adequately structured intelligence system, which proficiently anticipates and responds to the evolving global strategic dynamics. Intelligence plays a significant role not only in the quest of national security but also the decision making on strategically vital and sensitive matters, by helping reduce some of the prevalent uncertainties. This objective is achieved by the intelligence agencies through acquiring crucial information, and making forecasts based on the collected data regarding the issue under deliberations at the policy level. Hence, the role of national security intelligence needs to be comprehended by taking into cognizance the inevitable influences of constant factors like anarchic global structure, power contestation and conflicts.

While prior information about every facet of statecraft to anticipate the impending developments, and prepare adequate response is inevitable, it becomes even more obligatory, if a nation is facing security concerns. When confronted with national security threats, the states respond either through diplomatic means or by employing force - an interplay of carrots and sticks- nevertheless, the options adopted are dictated by the acquired information regarding an adversary. In case of adverse situations, decision makers prefer minimum ambiguities and, look for superior intelligence evaluations compared with the ones available to the rivals. Overcoming ambiguities and uncertainties with a prompt, yet deliberately inferred intelligence forecasting becomes even more decisive, when challenged with least perceptible modes of security threats. Thus, while confronting these unconventional challenges, national intelligence hierarchies are required to draw a comprehensive risk mosaic, encompassing and deliberating over every presumable security domain. It is, hence, widely accepted that comprehensive, and precise information is equally vital for the policymakers as well as commanders of the military during the process of strategy formulation (Breckinridge, 2019: 7). However, this information can be regarded as actionable intelligence only when it has undergone a comprehensive process of acquisition, analysis and timely dissemination.

National security objective in the past has mostly been the preservation of territorial integrity against the well-identified external adversaries, who would predominantly resort to various dimensions of kinetic activities through military instrument. According to Rathmell (2002), culmination of the Cold War as well as onset of the 'information revolution' have decisively transformed the established sources, methodologies and institutional structures of the intelligence (p. 87). The threat matrix in the post-cold war era has meanwhile drastically changed with emerging challenges being multifarious, far more dynamic, and rapidly evolving (Moore et al., 2020: 1). Consequently, the intelligence services have generally been confronted with increasingly chaotic, and immensely fluid international environments that left many officials of the intelligence community perplexed, and struggling to adapt (Rathmell, 2002: 87). Cavelty & Mauer (2009), summarize the contemporary operational environments by stating that: 'whereas Cold War intelligence by and large knew the problem and could envisage an objective reality that it was seeking to comprehend, contemporary intelligence . . . is in the position of not even knowing whether there is a single objective reality out there that it is trying to capture' (p. 134).

Transition of Security Paradigm and Intelligence

The transition of security from traditional to non-traditional domain, essentially represents the evolution of global strategic dynamics. International system has been recurrently transforming and vacillating between war and peace, necessitating a vibrant and adaptable approach towards security challenges. Growing influence of non-traditional security concerns after seemingly declining appetite for large scale conventional wars, has induced new ambiguities in the modes and methodologies of conflict. Intelligence, therefore, is challenged to keep pace with the evolving strategic dynamics and place greater focus on identifying fresh drivers of potential security risks. National security intelligence organizations have to stay abreast of new ideologies, emerging technologies, newly introduced political systems, latest alliances, and evolving power centers that necessitate frequent as well as timely realignments (Lahneman, 2011: x). The principal difference between preset day and cold war era intelligence, has been the identity of the adversaries as well as clarity vis-à-vis potential sources of national security hazards. Contrary to earlier patterns where adversary was conventionally structured, identifiable and usually foreseeable; contemporary security threats are much more amorphous, indistinct and unpredictable. It, thus, not only makes intelligence task complicated and mystifying, but also demands greater awareness about the evolving political, economic, strategic and social dynamics.

A paradigm shift in security calculus places all the instruments of state in a situation of quandary, necessitating transformation for developing adaptability and lessening strategic ambiguities. While reducing uncertainties is continuously pursued irrespective of the modes of potential threats, yet against non-traditional security menaces, it is even more vital. The transition of warfare from conventionality to non-conventionality is itself ambiguous, unpredictable, indistinct and hard to comprehend, and respond at the onset. With timely information, intelligence assures decision-advantage that not only allows added opportunities than the options available to the rivals, but also develops the capacity of making choices with greater certainty, promptness, and potential impact compared to the opponents (Sims, 2022: 31). Meanwhile, intelligence may have to rely more on apparently insignificant and, at times, seemingly incongruous indicators for evaluating, analyzing, and forecasting the persistently evolving threat mosaic. During this process, intelligence is required

to probe and explore even some of those domains, which may initially appear irrelevant to the evolving threat perception. It is, thus, comprehensible that intelligence not only maps the plausible challenges but also lists and ranks seemingly improbable, or least likely threats to allow decision advantage to the policy makers.

Intelligence functions cover a broad range of activities, not only forecasting prior to the occurrence of an incident, but even the post-event investigations for drawing pertinent lessons, identifying failures and fixing responsibilities. Notwithstanding significance of both, the reactive as well as proactive activities, intelligence seeks to think ahead, to anticipate the future, and then based on the envisaged assumptions, make efforts to adapt (Nicander, 2011: 536). While this cycle of actions is common to every intelligence operation, whether challenged by conventional or non-conventional threats, the complexity of tasks may induce divergent methodologies. Intelligence activity against conventional threats may not be radically divergent to basic training, however, dealing with unconventional issues would require different skill sets. Non-traditional security aspects are usually categorized complexed and intriguing, because it is not only hard to predict the risk intensity at the earlier stages, but equally perplexing is determining the adequacy of potential response. Consequently, according to Quiggin (2007), national security intelligence will have a broader as well as harder role in the future, and against changes occurring repeatedly, the agencies would need to reach out even beyond organizational input for acquiring necessary knowledge to meet the evolving challenges (p. 22).

Influence of Technology on Intelligence Operations

Intelligence tasks in the contemporary era are, essentially, far more complicated, intricate and challenging than the earlier times, where technological progression had not reached the present zenith. The acquisition of information as well as transmission of operational directives - functions once regarded most arduous - have been made easier by modern communication facilities. During contemporary security environments, the intelligence functions become more demanding since the perpetrators frequently exploit communication era facilities conveniently as compared to state's security apparatus. In many instances, intelligence officials find it hard to align themselves with the state of the art communication era gadgetry, and continue to rely on outdated methodologies. Apparently, this trend is reflective of the organizational inertia, where the officials are hesitant to abandon functional cultures, and stay immune to the necessity of adaptableness. The tendency echoes the past inclinations of the intelligence organizations, when acquisition of the information was deemed much more demanding. Essentially, at the time of establishing modern intelligence community, the availability of information was scarce, reasonably expensive, and regarded authoritative only when shared by the organizations classified as credible (Berkowitz & Goodman, 2000: 22).

The present era manifests a paradigm shift in the international political and strategic dynamics as well, since the technological innovations are influencing every sphere of human interactions all over the world. Modernization of technology has brought wealth at the doorsteps of younger generations who have innovative minds, and capacity of generating far more financial rewards compared to usual labor forces. This process is spawning new social fault lines in the traditional societies, and disrupting the existing conventional balance not only among various domestic entities, but between different regions as well. The rising discontent with the evolving economic

order amongst deprived communities is emerging as a tangible security hazard at domestic, regional as well as global level. Modern communication means and resultant ease of access to every type of information, whether real or fabricated, is further exacerbating security challenges. Interplay of technology and economy has not been as swaying on security realm at any other time, since it has ensued in the rise of several non-conventional threats. Consequently, the ongoing financial and technical revolution has also led to information processing that not only directly affects security intelligence, but simultaneously influences almost everyone's life (Sims, 2022: 541).

Intelligence has been, and continue to be a wide-ranging process, encompassing several facets including direction from the policy makers, acquiring of information, its processing for developing situational mosaic, and dissemination for action. In case of non-traditional challenges, following a structural mechanism does not preclude the intelligence from focusing on any aspect, which may evolve in to a greater risk at some later stages. However, continued applicability of this longstanding structural framework, adhered to in the form of intelligence cycle for intelligence functions, may now be facing a challenge from ongoing technological progress. Modern gadgetry immensely facilitates not only the information acquisition, but processing of intelligence, collation as well as dissemination through emerging technology. Notwithstanding abundance of information, intelligence has to now cope with the challenge of differentiating real from the fake, and actual from deliberately cultivated data. Contemporary intelligence is, therefore, operating in an environment where adversaries can very conveniently make use of digital technology for developing convincing fakes, to mislead or disrupt intelligence efforts (Hershkovitz, 2022: 36). It may thus be inevitable to adhere a structural process for not only staying abreast of the evolving situation, but avoid deliberately constructed and fake intelligence leads.

Conventional Intelligence Crafts and Transformation Dilemmas

Intelligence work can be regarded among the most structured, well-deliberated and carefully planned activities for some specific objectives. Conventionally, national security intelligence functions commence with a direction from policy makers on a particular issue, where information is needed for developing clarity, a process called intelligence cycle. This cyclic process has traditionally been at the core of how most of the intelligence organizations function, and are structured (Hershkovitz, 2022: 27). While for traditional security challenges, intelligence officials tend to rely on conventional methodologies since the threat is likely to transpire in familiar domains, the pattern can differ for unconventional dimensions. Good intelligence can opt for a different course when confronted with non-traditional risks and, officials may not always count on established methodologies. Here is a paradox as well since, intelligence receives direction about the potential threats and aspects to be monitored from the requirements disseminated by the policy makers (Lahneman, 2011: 1). Does it imply that the intelligence cycle is obsolete or redundant when the nation faces non-traditional security threats? Essentially, this long established procedural structure never loses its relevance, however, in case of asymmetric, irregular or nonconventional challenges, probe even beyond the actual mandate may be crucial.

Intelligence in the conventional domain has mainly been focusing on the provision of early warning, a function once deemed to be among the core responsibilities of the agencies. Increasing connectivity is trespassing the restrictions imposed by even stringent of the borders, thus presently diminishing the role of state. In this highly interdependent world, there are expanding threats and

risks with diversifying modes, and increasing vulnerabilities of the societies in different realms. It is, therefore, evident that the rapid advancement of communication technologies and resultant impact of information warfare has added a highly complicated challenge for the national security intelligence. Consequently, these evolving dynamics of the security environments necessitate evaluation of the state's conventional early warning systems for identifying the sources of risk as well as threat (Nicander, 2011: 540). While information operations have always been among the vital components of warfare, its contemporary use is becoming even more pronounced and rewarding. The deliberately planned and strategically executed employment of visual as well as aural communication, for influencing the perceptions and responses of a targeted audience is viewed as an essential part of the strategy for achieving the politico-military objectives (Goldman, 2024: 87).

Present-day national security intelligence is being confronted by several multidimensional as well as complicated security challenges that emanate from often indistinct, and mostly unconventional sources. These threats are perceived to be originating from non-state actors, extremists, weapon as well as drug proliferators, transnational criminal gangs and cyber activists, as much as from conventional state aggression (Omand, 2014: 14). The multiplicity of these challenges and potential collusion with host of natural calamities, necessitate review of intelligence methodologies. While effective intelligence plays a crucial role in the timely identification of evolving security threats, rising spectrum of contemporary challenges can make prompt response more complicated. These evolving security concerns may appear benign at the evolutionary stage, thus a perceptible involvement by the intelligence agencies can be presumed impulsive or unwarranted by the masses. On the other hand, during such a scenario, intelligence operations would be vital in formulating effective response by focusing on an adversary's unconventional capabilities, identifying the target audience, and professing potential modes and means of threat (Goldman, 2024: 84). Hence, it would be inevitable to evolve acquired information for anticipating 'potential threats patterns', while taking into consideration all aspects, including those appearing irrelevant at the outset.

Contrary to the traditional methodologies, the acquisition of information may now cede its once distinctive prominence in the intelligence operations, to the necessity of 'sense making' from what is so plenteously acquirable from numerous resources. According to Omand (2012), every effective intelligence agency in the future would function as a knowledge management organization, and encourage innovation as well as creativity (p. 156). Consequently, role of analysts, working at desks would assume precedence in comparison to those functioning in the field, and undertaking orthodox intelligence activities. Richard Fadden, the Director of the Canadian Security and Intelligence Service (CSIS) emphasized this reality in 2012 by stating that, 'suddenly the ability to make sense of information is as valued a skill as collecting it' (Allen, 2012). Hence, intelligence analysts would take up the role of sense-makers and help identify the adversaries as terrorists, potential rebels, instigators of a social movement, religious extremists, and irrational fanatics (De Graaff, 2014: 7). However, without the capacity of 'situational awareness, explanation, prediction and strategic notice,' the generation of a viable set of plausible hypotheses by the intelligence analysts, for appropriately professing new pattern of threat becomes unlikely (Omand, 2014: 24).

Intelligence: Preparing for the Evolving Challenges

In the post-cold war world, the necessity of adaptation by the intelligence organizations for evolving challenges, has been an extensively debated subject in the West. One of the negative traits attributed to the intelligence officials is the lack of 'critical thinking' that helps in developing imaginative intelligence products. Thus, anticipation and forecasting impending threats has always been challenging, since it involves 'critical thinking' for comprehending intentions of the adversaries. The emergence of non-traditional security threats, with a multitude of non-attributable activities and unrecognizable actors, has further complicated this challenge. Consequently, the limits of rationalism, influence of cognitive bias as well as the secrecy culture prevalent in the intelligence organizations, impedes the creative thinking and results in the strategic intelligence failures (Bury & Chertoff, 2020: 50). In the words of Bohm (2004), a renewed scholar on creative thinking, 'the act of seeing deeply (and not merely verbally or intellectually), is also the act in which originality and creativity can be born (p. 32).' Hence, contemporary intelligence organizations are required to understand human cognitions, and embrace imaginative and creative thinking for reducing discourse failures, while identifying the structures as well as the harmony of threats (Hatlebrekke, 2019: 63).

Corresponding to the nature of functions, intelligence has traditionally been a clandestine activity that by and large managed to evade public scrutiny in the past. Intelligence agencies relied mostly on limited interface with the masses, often resorting to one-way transmission of security related issues or other related concerns, if deemed essential. Information revolution has, altered this equation, and the emergence of many speedier means has not only reduced intelligence's near monopoly of early warning capacity, but subject their activities to more public scrutiny. With this longstanding perception now eroding fast; people not only demand greater transparency but express more interest towards security issues and appear increasingly critical of policy makers (Hershkovitz, 2022: 79). Evolving challenges from non-conventional security domain subject intelligence operations to greater public focus, as some of the activities may appear unnecessary to masses and attract criticism. Apparently, intelligence agencies cannot sustain absolute reliance on clandestine mode, especially in the communication era and may have to introduce some form of transparency in their activities. Prima facie, it seems a farfetched idea, especially when viewed in the context of well-established and traditional operational norms of intelligence where, culture of secrecy continues to have a vital significance.

Intelligence is expected to be far more proactive, forward looking and focused on identifying various exploitable 'blind spots' in the national security sphere well in advance, even during the apparent peace times. Inability of identifying these blind spots not only reflects negligence and poor imagination, but also insufficient knowledge regarding an adversary's strategic intent or capacity (Goldman, 2024: 88). Identifying these 'blind spots' would entail intelligence to devise a more innovative operational mechanism that, at times, may defy the conventional and most frequently employed methodologies. It would, thus, necessitate far greater focus on analytics than other intelligence crafts, and over long term developments than the ongoing routine incidents. Intelligence analysts would need the attributes of creative thinking as well as cognitive awareness, and also integrate with the private sector, for staying conversant with the exploding data and evolving technologies (Bury & Chertoff, 2020: 50). The US policy makers responded to the post-cold

war arena with the National Intelligence Strategy, issued in October 2005 and identified characteristics required to be developed among the intelligence professionals: “(1) results focused; (2) collaborative; (3) bold; (4) future-oriented; (5) self-evaluating; and (6) innovative (Hastedt & Skelley, 2008, p. 112).”

Why Intelligence Should Transform?

In order to be effective, responsive and proactive, intelligence needs to maintain compatibility with the evolving nature of warfare, and explore the avenues of national security where it has to assume a paradigm shift. Apparently, the emergence of non-traditional warfare has also decisively influenced military affairs, besides many other dimensions like technological progression and strategy. Consequently, intelligence organizations would be required to keep track of the ongoing Revolution in Military Affairs (RMA) for initiating their own Revolution in Intelligence Affairs (RIA) for staying relevant, adaptable and compatible. It is believed that the scope of the RMA has been so extensive that RIA is inevitable for maintaining balance among various instruments of national power; globally, intelligence communities cannot be categorized as effective; and the evolving threat spectrum augurs for the need of undertaking transformational changes in the intelligence functions (Lahneman, 2011: xx-xxi). Irrespective of the nature of transformation, whether evolutionary or even revolutionary, the organizational culture of intelligence will have to raise compatibility with the ever evolving dimensions of national security threats.

While elaborating transformation of the US intelligence, Biltgen & Ryan (2016) identify four ages of intelligence: first age commencing during World War II with the establishment of the Office of Strategic Services (OSS); in early 1960s during cold war, the second age begun; the terrorist attack of 11 September, 2001 led to the decade of a third age; and since mid-2014, diversified threats and unprecedented technological progress has dawned the fourth age (pp. 21-22). Intelligence during these eras faced multi-dimensional actors, ranging from opposing military forces during the 2nd world war to ideational adversaries in the cold war; and from the non-state actors in the beginning of the 21st century to cognitive warfare of the contemporary digitalized world. According to the analysts, four paradigm shifts have prompted internal organizational innovations among intelligence setups globally: rising sway of information revolution as well as open-source intelligence, undermining the monopoly on knowledge; increasing counterterrorism missions, without adequate in-house comprehension of anthropological domain, religions, languages, and cultures; inevitability of pluralism as well as innovation in intelligence methodologies for alternative views; and approaching the new vulnerabilities evolving in the information society with a foresight (Nicander, 2011: 544).

National security intelligence can function proficiently and deliver viable feedback to the policy makers, when the input from the entire intelligence community is collectively evaluated. However, departmental rivalries, credit seeking tendencies and propensity of functioning in silos mitigate prospects of any meaningful collaboration among intelligence setups. According to Foryst (2009), intelligence services would need to function collaboratively, for improving the relevance and value of the eventual intelligence product (pp. 415–418). The Robb–Silberman Commission report on Iraq’s weapons of mass destruction identifies same fact, and suggests that the Intelligence Community (IC) has been “allocating among intelligence priorities in a way that seemed sensible to them, but were not optimal for a community wide perspective” (Ireland, 2017: 48). Although,

collaborative input by the intelligence is crucial in every situation, it assumes added importance while identifying threat patterns during non-traditional challenges. The multi-dimensionality of contemporary issues can be addressed only when intelligence organizations abandon 'stovepipe mentality,' that essentially promotes the tendency of working in silos. Inter-intelligence coordination, lateral sharing of information as well as assessments, enhancing functional versatility against the evolving challenges and assenting a consensual way forward on sensitive tasks, therefore, is inevitable.

CONCLUSION

Evaluating success or failure of intelligence has been an extensively debated subject over the years among the national security experts, with several diverging views available in the literature. The benchmark for these assessments of intelligence functions has predominantly been focused on the conventional warfare, usually involving military surprises. The most cited instances in this regard are Operation Barbarossa, Japanese's strategic surprise at Pearl Harbor in World War II, and the Battle of Yom Kippur (Barnea, 2021, p. xiii). Investigations of the Pearl Harbor attack by Japan revealed that various American institutions had adequate information and if it was collated, analyzed, and disseminated timely, the early warning would have prompted necessary defensive measures (Breckinridge, (2019, p. 5). Despite the focus on conventional wars, some of other strategic surprises primarily from non-conventional domain like the 9/11 attacks, or widespread popular uprisings especially Palestinian Intifadas, and political upheavals such as Arab Spring, have also been deliberated (Barnea, 2021, p. 1). It is, however, pertinent to suggest that intelligence failures cannot be attributed to any specific dimension, and the inferences drawn after evaluations at various times and places are equally applicable to all modes of security, whether traditional or non-traditional.

The challenges in the nonconventional security paradigm have emerged in the post-cold war arena as a serious security threat, not only for the domestically fragile developing states, but the developed world as well. It has been inferred that aspects such as 'defensive thinking; stale assumptions; reactive posture; constrained imagination; absence of national strategy; constrained perceptions; and failures' identified as major challenges for a highly resourced intelligence like the US, decisively impeded response capacity (Foryst, 2009, pp. 398–400). There have been loud voices over the necessity of undertaking 'intelligence reforms,' a recurring phenomenon that comes under extensive debate, whenever new form of security threat becomes crucial. These efforts, nonetheless, turned out to be far more complicated than initially perceived, and fixated approach by intelligence officials restricted any meaningful progress in this regard. The hereditary organizational structures of the intelligence, primarily designed and developed to address the military dominated conventional threats, resulted in inertia and resisted calls for the change. Consequently, initiatives aimed at reforming intelligence for mitigating real world hazards, and incorporating opportunities into the strategic, operational, as well as tactical domains often fail to produce desired outcome (Moore et al., 2020, p. 12).

It is an undeniable fact that intelligence setups had to frequently undergo substantial changes to meet the evolving threats, which have not only been mutating in the construct, but likewise, there has been diversification of the actors as well. Intelligence that has been focusing on an identifiable conventional threat during the Cold War, had to realign against terrorist activities from diversified

sources, mainly non-state actors after September 11; and is now confronted with increasingly asymmetric, non-traditional, and unpredictable threats, which continue to emanate from multiple vectors (Biltgen & Ryan, 2016, p. 22). However, it is generally perceived that the intelligence agencies have not been able to keep pace with the rapidly evolving national security threat matrix after the culmination of cold war. Most of the scholars on the subject have identified this fact by suggesting that intelligence methodologies involving collection, analysis and consumption continued to follow the Cold War paradigm, which has been inadequate against current challenges. While there is nothing radically flawed with the cold war intelligence paradigm, it was required to evolve with the changing dynamics of emerging threats. Consequently, intelligence may need to rely more on evolutionary process for transformation instead of undertaking a radical change through some revolutionary steps.

References:

- Allen, I. (2012, Jul. 2). Intel analysts taking over leading role in spy game. *IntelNews.org*. <https://intelnews.org/2012/07/02/01-1025/>.
- Anthony, M. C., Emmers, R., & Acharya, A. (Eds.). (2006). *Non-traditional security in Asia: Dilemmas in securitization*. Ashgate.
- Aydın, M. (2011). *Non-traditional security threats and regional cooperation in the Southern Caucasus*. IOS Press.
- Barnea, A. (2021). *We never expected that: A comparative study of failures in national and business intelligence*. Rowman & Littlefield.
- Berkowitz, B. D., & Goodman, A. E. (2000). *Best truth: Intelligence in the information age*. Yale University Press.
- Bilgin, P. (2003). Individual and societal dimensions of security. *International Studies Review*, 5(2), 203-22. <https://doi.org/10.1111/1521-9488.502002>.
- Biltgen, P., & Ryan, S. (2016). *Activity-based intelligence: principles and applications*. Artech House.
- Bohm, D. (2004). *On Creativity*. Routledge.
- Booth, K. (2007). *Theory of world security*. Cambridge University Press.
- Breckinridge, S. (2019). *The CIA and the US Intelligence System*. Routledge.
- Bury, P., & Chertoff, M. (2020). New intelligence strategies for a new decade. *The RUSI Journal*, 165(4), 42-53. <https://doi.org/10.1080/03071847.2020.1802945>.
- Buzan, B., Waever, O. and de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner.
- Caballero-Anthony, M. (2016). *An introduction to non-traditional security studies: A transnational approach*. SAGE Publications.
- Caballero-Anthony, M., & Cook, A. D. (Eds.). (2013). *Non-traditional security in Asia: Issues, challenges and framework for action*. Institute of Southeast Asian Studies.
- Cavelty, M. D., & Mauer, V. (2009). Postmodern intelligence: Strategic warning in an age of reflexive intelligence. *Security Dialogue*, 40(2), 123-44. <https://doi.org/10.1177/0967010609103071>.
- Chalk, P. (2000). *Non-military security and global order: The impact of extremism, violence and chaos on national and international security*. Springer.
- Craig, S. L. (2007). *Chinese perceptions of traditional and nontraditional security threats*. Strategic Studies Institute, US Army War College. <https://press.armywarcollege.edu/monographs/690/>.

- Dalby, S. (1995). Security, intelligence, the national interest and the global environment. *Intelligence and National Security*, 10(4), 175-97. <https://doi.org/10.1080/02684529508432332>.
- De Graaff, B. (2014). By way of introduction: A systemic way of looking at the future of intelligence. In I. Duyvesteyn, B. de Jong, & J. van Reijin (Eds.), *The Future of Intelligence: Challenges in the 21st century*. (1-13). Routledge.
- Foryst, C. A. (2009). Missing from U.S. intelligence analysis: The concept of "Total U.S." *International Journal of Intelligence and CounterIntelligence*, 22(3), 396-420.
- Goldman, J. (2024). Influence operations and the role of intelligence. In R. Acros, I. Chiru, & C. Ivan. (Eds.), *Routledge Handbook of Disinformation and National Security*. (84-94). Routledge.
- Hastedt, G. P., & Skelley, B. D. (2008). Intelligence in a turbulent world: Insights from organization theory. In P. Gill, S. Marrin, & M. Phythian (Eds.), *Intelligence theory*. (126-44). Routledge.
- Hatlebrekke, K. A. (2019). *Problem of secret intelligence*. Edinburgh University Press.
- Hershkovitz, S. (2022). *The future of national intelligence: How emerging technologies reshape intelligence communities*. Rowman & Littlefield.
- Ireland, L. (2017). 21st century intelligence: The need for a one-team-one-fight approach. *PRISM*, 7(1), 46-57. <https://www.jstor.org/stable/26470497>.
- Jarvis, L., & Holland, J. (2014). *Security: A critical introduction*. Bloomsbury Publishing.
- Job, B. L. (Ed.). (1992). *The insecurity dilemma: National security of third world states*. Lynne Rienner.
- Krause, K., & Williams, M. C. (2002). *Critical security studies: Concepts and strategies*. Routledge.
- Lahneman, W. J. (2011). *Keeping US intelligence effective: The need for a revolution in intelligence affairs*. Scarecrow Press.
- Moore, D. T., Moore, E., Cantey, S., & Hoffman, R. R. (2020). Sensemaking for 21st century intelligence. *Journal of Intelligence History*, 20(1), 45-59.
- Nicander, L. D. (2011). Understanding intelligence community innovation in the post-9/11 world. *International Journal of Intelligence and CounterIntelligence*, 24(3), 534-68.
- Omand, D. (2012). Into the future: A comment on agrell and warner. *Intelligence and National Security*, 27(1), 154-56. <https://doi.org/10.1080/02684527.2012.621610>.
- Omand, D. (2014). The future of intelligence: What are the threats, the challenges and the opportunities? In I. Duyvesteyn, B. de Jong, & J. van Reijin (Eds.), *The Future of Intelligence: Challenges in the 21st century*. (14-26). Routledge.
- Quiggin, T. A. (2007). *Seeing the invisible: National security intelligence in an uncertain age*. World Scientific.
- Rathmell, A. (2002). Towards postmodern intelligence. *Intelligence and National Security*, 17(3), 87-104. <https://doi.org/10.1080/02684520412331306560>.
- Schilling, W. R. (2002). *Nontraditional warfare: Twenty-first century threats and responses*. Potomac.
- Sims, J. E. (2022). *Decision advantage: Intelligence in international politics from the Spanish Armada to Cyberwar*. Oxford University Press.
- Singh, N. K., & Nunes, W. (2013). Drug trafficking and narco-terrorism as security threats: A study of India's North-east. *India Quarterly*, 69(1), 65-82.
- Singh, N. K., & Nunes, W. (2016). Nontraditional security: Redefining state-centric outlook. *Jadavpur Journal of International Relations*, 20(1), 102-24.

- Snyder, C. A. (2012). Contemporary security and strategy. In C. Snyder (Ed.), *Contemporary security and strategy*. (1-16). Palgrave.
- Srikanth, D. (2014). Non-traditional security threats in the 21st century: A review. *International Journal of Development and Conflict*, 4(1), 60-68.
- Swain, A. (2012). *Understanding emerging security challenges: threats and opportunities*. Routledge.
- Thomas, C. (1987). *In search of security: The Third World in international relations*. Rienner.

Date of Publication	June 2, 2025
---------------------	--------------