

National Security in the Context of Asymmetric Threats

Mohamed Rafik Laib
Souk Ahras University
m.layab@univ-soukahras.dz

Received: 24/10/2025

Accepted: 25/02/2026

Abstract:

In recent decades, the world has witnessed a profound transformation in the nature of security threats facing states and societies, security challenge are no longer confined to traditional interstate wars; rather, they have expanded to include asymmetric dimensions such as terrorism, organized crime, cyberattacks, health crises, environmental disasters, and economic challenges, this transformation has led to the emergence of the concept of comprehensive and multidimensional security, which goes beyond military power to encompass economic, health, environmental, social, and technological dimensions within a strategic framework focused on prevention and risk management. The importance of studying Asymmetric Threats lies in the fact that they pose complex challenges to national security, as they are transnational, multidimensional, and rapidly evolving, making effective responses difficult without scientific understanding and integrated strategies, moreover, addressing these threats requires regional and international cooperation, the use of advanced technologies, and the adoption of flexible and comprehensive policies aimed at protecting individuals, society, and the state alike, therefore, research in this field is essential for developing national and regional strategies capable of effectively and efficiently confronting future security challenges.

Keywords: National Security ; Asymmetric Threats

I. INTRODUCTION

In recent decades, the world has witnessed a profound transformation in the nature of security threats facing states and societies, security challenge are no longer confined to traditional interstate wars; rather, they have expanded to include asymmetric dimensions such as terrorism, organized crime, cyberattacks, health crises, environmental disasters, and economic challenges, this transformation has led to the emergence of the concept of comprehensive and multidimensional security, which goes beyond military power to encompass economic, health, environmental, social, and technological dimensions within a strategic framework focused on prevention and risk management.

The importance of studying Asymmetric Threats lies in the fact that they pose complex challenges to national security, as they are transnational, multidimensional, and rapidly evolving, making effective responses difficult without scientific understanding and integrated strategies, moreover, addressing these threats requires regional and international cooperation, the use of advanced technologies, and the adoption of flexible and comprehensive policies aimed at protecting individuals, society, and the state alike, therefore, research in this field is essential for developing national and regional strategies capable of effectively and efficiently confronting future security challenges.

This study aims to:

- Examine the concept of asymmetric threats, their various types, and distinguishing characteristics.
- Analyze the theoretical and security frameworks that explain these threats and the ways to address them.
- Review practical examples of Asymmetric Threats and their impact on national security.
- Evaluate national strategies and international cooperation as tools for countering these threats.
- Present a future-oriented perspective on the challenges and opportunities in managing asymmetric security.

The research problem is centered on the following main question:
How can states confront asymmetric threats that endanger national security, given their multidimensional nature, transnational scope, and rapidly changing characteristics?

This main question gives rise to several sub-questions, including:

- What are the different characteristics and types of asymmetric threats?
- How do contemporary security theories explain these threats?
- What role do national strategies and international cooperation play in countering them?
- What are the future challenges and opportunities for ensuring comprehensive and sustainable security?

Chapter One: Theoretical and Conceptual Framework.

This chapter addresses the theoretical and conceptual framework of the study, focusing on the concept of comprehensive national security and its various dimensions: political, military, economic, social, health, environmental, and cyber. It also examines Asymmetric Threats such as terrorism, organized crime, cyberattacks, health and environmental disasters, and economic crises, highlighting their characteristics and dimensions.

In addition, the chapter presents the main security theories explaining non-traditional security, ranging from realism to human security, in order to provide an analytical foundation for understanding the nature of these threats and the ways to confront them.

Section One: The Concept of National Security and Its Evolution.

This section examines the concept of national security and its various dimensions, with a focus on its historical evolution across different stages, starting from traditional military security, through the Cold War period, and reaching the stage of comprehensive security in the context of globalization and the digital revolution, the section aims to clarify how the

understanding of security has shifted from protecting the state and its borders to a comprehensive and multidimensional approach that includes political, economic, social, environmental, cyber, and health dimensions, while involving multiple actors at both the national and international levels.

First: The Concept of National Security.

The concept of national security is one of the core concepts in political science and international relations, as it has historically been associated with the state's ability to protect its political entity and ensure the integrity of its territory against external threats, this concept emerged within the framework of the international system based on the nation-state and the balance of power, where military threats occupied a central position among sources of danger facing states, one of the most well-known classical definitions views national security as a relative rather than absolute concept, Arnold Wolfers defined national security as "the absence of threats to acquired values and the absence of fear that such values will be attacked" (Wolfers, 1952, p. 485), this definition clearly highlights the psychological dimension of security alongside the material one, emphasizing that the sense of security is no less important than possessing instruments of power.

Barry Buzan, on the other hand, criticized the restriction of national security to the military dimension and proposed a more comprehensive perspective, arguing that national security consists of several interrelated sectors, he explains that national security includes the military, political, economic, and societal sectors, and that a threat in any one of these sectors may evolve into an overall threat to the state (Buzan, 1991, p. 18), this approach represents one of the earliest systematic attempts to expand the concept of security beyond the traditional military framework, theoretical approaches to national security vary according to different schools of thought, while neorealism focuses on power and balance of power as the essence of security, liberal and constructivist approaches expand the concept to include the role of institutions, values, and identity, Stephen Walt notes that this variation reflects differences in defining sources of threat rather than disagreement over the importance of security itself (Walt, 1991, p. 212).

With the end of the Cold War, the concept of national security underwent a qualitative transformation, it was no longer limited to protecting the state from military aggression but expanded to include asymmetric threats, Buzan and Hansen argue that this transformation marked a shift in security studies from a narrow focus on the state to a broader approach encompassing society and individuals (Buzan & Hansen, 2009, p. 10).

Accordingly, national security can be regarded as a dynamic and evolving concept, shaped by historical context and the nature of prevailing threats, and cannot be confined to a single fixed definition.

Second: The Evolution of the Concept of National Security.

The concept of national security has passed through several successive historical stages, closely linked to the nature of the international system, the dominant forms of conflict, and the types of threats faced by states at each stage, this evolution reflects a transition from a narrow military approach to a comprehensive and multidimensional analytical framework.

1- The Traditional Stage (Pre-Cold War):

During this stage, national security was closely associated with military power and the state's ability to protect its territorial borders and deter external aggression, this understanding prevailed within the classical international system based on the nation-state and power competition, where security was measured by military capabilities, alliances, and balance of power.

Hans Morgenthau argues that the primary objective of the state in international politics is survival through power, and that security is achieved through deterrence and military balance (Morgenthau, 1948, p. 13), Barry Buzan also notes that traditional security thinking reduced

national security to the military dimension, neglecting other aspects of political and social life (Buzan, 1991, p. 16).

2- The Cold War Stage:

With the outbreak of the Cold War, the concept of national security expanded relatively, as it became linked not only to conventional military confrontation but also to ideological and political conflict between the Eastern and Western blocs, nuclear deterrence, arms races, and military alliances played a central role in defining national security during this period.

Stephen Walt points out that security studies during the Cold War focused on military threats between great powers, with particular emphasis on nuclear deterrence and strategic stability (Walt, 1991, p. 213), Kenneth Waltz also argues that the bipolar structure of the international system forced states to define their national security in terms of existential rivalry with an ideological opponent (Waltz, 1979, p. 102).

3- The Post-Cold War Stage:

With the end of the Cold War and the collapse of the Soviet Union, the concept of national security experienced a qualitative shift, the centrality of direct military threats declined, while new asymmetric threats emerged, such as international terrorism, illegal migration, organized crime, economic crises, and environmental degradation.

In this context, Barry Buzan emphasizes that the end of bipolar conflict opened the way for expanding the concept of security to include non-military sectors, arguing that national security became linked to societal, economic, and environmental security, not merely territorial integrity (Buzan, 1991, p. 19), Buzan and Hansen further note that this period represented a pivotal turning point in the evolution of international security studies (Buzan & Hansen, 2009, p. 9).

4- The Contemporary Stage:

In the context of globalization and the accelerating digital revolution, national security has become a comprehensive and multidimensional concept, encompassing political, economic, social, environmental, cyber, and health security, the state is no longer the sole actor in achieving security; international organizations, multinational corporations, non-state actors, and even individuals now play significant roles, Ulrich Beck argues that contemporary societies face a “risk society”, where threats are transnational and cannot be contained by traditional military means (Beck, 1992, pp. 21–23), Buzan and Hansen also emphasize that contemporary security is based on a comprehensive preventive approach focused on risk management rather than mere reaction (Buzan & Hansen, 2009, p. 12).

Third: Dimensions of National Security:

In contemporary political thought, national security is no longer a single-dimensional concept but rather a comprehensive analytical framework based on the interaction of several integrated dimensions, a disruption in any one of these dimensions can pose a direct or indirect threat to state security and stability, Buzan stresses that national security cannot be fully understood without analyzing its various sectors as an interconnected system (Buzan, 1991, p. 19).

1- The Political Dimension:

The political dimension constitutes a fundamental pillar of national security, as it relates to political stability, regime legitimacy, and the state’s ability to manage internal conflicts peacefully; it includes the effectiveness of political institutions, respect for the rule of law, and levels of political participation, Buzan argues that weak political legitimacy or fragile institutions may constitute a security threat no less serious than external military threats (Buzan, 1991, p. 95), Robert Jackson similarly notes that states suffering from internal legitimacy crises are more vulnerable to security collapse (Jackson, 1990, p. 29).

2- The Military Dimension:

The military dimension remains the traditional core of national security and concerns the protection of sovereignty, territorial integrity, and deterrence of external military threats; it includes armed forces’ capabilities, military technology, and defense doctrine.

Morgenthau emphasizes that military power is the primary instrument for ensuring state survival in an anarchic international system (Morgenthau, 1948, p. 14), while Waltz highlights deterrence as a decisive element of national security (Waltz, 1979, p. 91).

3- The Economic Dimension:

Economic security relates to the state's ability to maintain economic stability, secure strategic resources, and sustain growth and development. Economic crises, sanctions, and supply chain disruptions have become real threats to national security, Buzan asserts that economic weakness can undermine a state's ability to defend itself and maintain political and social stability (Buzan, 1991, p. 109), Gilpin also emphasizes that economic power has become a central component of national security in the modern era (Gilpin, 2001, p. 11).

4- The Social Dimension:

The social dimension is linked to maintaining social cohesion, national identity, and societal stability, as well as limiting ethnic, sectarian, or cultural divisions, this dimension is commonly referred to in security literature as societal security.

Buzan notes that threats to collective identity or the fragmentation of the social fabric can lead to internal conflicts that weaken the state and threaten national security (Buzan, 1991, p. 119), Buzan and Wæver further stress that societal security has become a central issue in multi-identity societies (Buzan, Wæver, & de Wilde, 1998, p. 119).

5- The Environmental and Health Dimension:

Climate change, natural disasters, and global pandemics have introduced a new dimension to national security, namely environmental and health security, global health crises such as COVID-19 have demonstrated that non-military threats can disrupt state institutions and weaken economic and security capacities.

Ulrich Beck argues that modern societies face transboundary environmental and health risks that cannot be contained by traditional means (Beck, 1992, p. 21), Buzan and Hansen also emphasize that environmental and health security have become integral components of contemporary national security (Buzan & Hansen, 2009, p. 72).

6- The Cyber Dimension:

Cybersecurity represents one of the newest dimensions of national security and relates to protecting cyberspace, information infrastructure, communication networks, and sensitive state data; cyberattacks have become an effective means of weakening states without resorting to conventional military force.

Joseph Nye argues that cyber power has become a fundamental component of power in international politics due to its direct impact on national security, the economy, and sovereignty (Nye, 2011, p. 113), Clarke and Knake also emphasize that cyberattacks can paralyze vital state institutions and generate long-term strategic effects (Clarke & Knake, 2010, p. 30).

Fourth: The Shift toward Comprehensive Security:

The escalation of Asymmetric Threats at the international level—such as terrorism, transnational organized crime, cyberattacks, and environmental and health disasters—has led to the emergence of the concept of comprehensive national security, this concept is based on integrating various security dimensions within a single strategic framework that emphasizes prevention and risk management rather than mere reaction (Buzan & Hansen, 2009, p. 15).

This shift reflects a growing recognition that state security cannot be achieved through military power alone but requires a comprehensive approach that includes economic and social development, good governance, strong state institutions, and international cooperation (Buzan, Wæver, & de Wilde, 1998, p. 10), contemporary challenges such as climate change, global pandemics, and cyber threats are transboundary in nature and cannot be effectively addressed without regional and international partnerships.

Ulrich Beck emphasizes that modern societies live in a “risk society,” characterized by diverse and unpredictable threats, making comprehensive, preventive security strategies based

on proactive risk management essential (Beck, 1992, p. 24), Joseph Nye also argues that comprehensive power in the twenty-first century rests on balancing military, economic, political, and technological elements, reinforcing the need for integrated security (Nye, 2011, p. 118).

Comprehensive security is also characterized by flexibility and adaptability to rapid changes in the international environment. It encompasses political, economic, social, environmental, health, and cyber security, while emphasizing cooperation between states and international and non-governmental actors to ensure sustainable security (Buzan & Hansen, 2009, p. 18), it can thus be viewed as a logical extension of the evolution of the national security concept toward a multidimensional and cross-sectoral approach that links state security with societal security.

This section concludes that the concept of national security has evolved to become more comprehensive and complex, military power alone is no longer sufficient to guarantee state security; rather, national security has become closely linked to sustainable development, good governance, and the ability to confront Asymmetric Threats such as terrorism, cyberattacks, environmental disasters, and pandemics, this transformation underscores the importance of adopting integrated and flexible strategies to preserve state stability and enhance comprehensive security.

Section Two: The Concept of Asymmetric Threats.

This section examines the concept of Asymmetric Threats, which refer to risks that do not necessarily arise from conventional military conflicts between states. Instead, they include terrorism, transnational organized crime, cyberattacks, natural disasters, pandemics, and economic crises.

The section focuses on the defining characteristics of these threats—such as their transboundary nature, multidimensionality, and unpredictability—which make confronting them dependent on multi-actor security strategies as well as regional and international cooperation.

First: Definition of Asymmetric Threats.

Asymmetric Threats refer to any risk that affects the security of the state or society but does not fall within the framework of traditional military conflicts between states (Buzan & Hansen, 2009, p. 25), these threats are characterized by their transnational nature, multidimensional impacts, and unpredictability, and they often require comprehensive responses encompassing political, economic, social, environmental, health, and technological dimensions, rather than relying solely on military measures.

This category of threats includes phenomena such as international terrorism, transnational organized crime, cyberattacks, environmental disasters, and global pandemics, all of which pose direct or indirect threats to state stability and the sustainability of national security (Buzan & Hansen, 2009, p. 26), Christoph Walker defines Asymmetric Threats as: “Events or processes that threaten the stability of the state or society but originate outside the traditional military framework, and require multi-sectoral security approaches” (Walker, 2010, p. 45).

This definition highlights the interconnectedness and complexity of Asymmetric Threats, as they are often intertwined in such a way that a threat in one dimension can generate consequences in other dimensions, for example, cyberattacks may severely affect the national economy or critical infrastructure, while natural disasters can undermine public health and social stability.

Consequently, the ability to prevent and manage risks has become a core requirement in addressing these threats, traditional military approaches alone are no longer sufficient to ensure security; instead, it has become essential to integrate national security policies with strategies of sustainable development, good governance, and multilateral international cooperation (Buzan & Hansen, 2009, p. 27).

Second: Characteristics of Asymmetric Threats.

Asymmetric Threats possess several key characteristics that distinguish them from traditional military threats and make them more complex to address, thereby requiring comprehensive and multi-actor strategies (Buzan, Wæver, & de Wilde, 1998, p. 35):

1- Transboundary Nature:

These threats often extend beyond the borders of a single state, as in the case of international terrorism, illegal migration, and cross-border pandemics, due to their transnational character, no state can effectively confront them in isolation from other states or from regional and international organizations.

2- Unpredictability:

Asymmetric Threats are difficult to predict in terms of timing and location, for instance, the outbreak of a new virus or a strategic cyberattack may occur suddenly and have a profound impact on state stability, necessitating rapid and flexible response plans.

3- Multidimensionality:

Asymmetric Threats intersect with multiple dimensions of security, including political, economic, social, health, and environmental security, this makes their assessment and management highly complex. For example, cyberattacks can disrupt economic systems and critical infrastructure, leading to political and social instability.

4- Wide-Ranging Impacts:

The effects of these threats often extend to society as a whole, not only to state institutions or military borders, terrorism or natural disasters, for instance, may disrupt daily life, exacerbate poverty, and increase levels of social insecurity.

5- Requirement for Multi-Actor Cooperation:

Addressing Asymmetric Threats cannot rely solely on national state capabilities. It requires regional and international cooperation among governments, international organizations, the private sector, and civil society, in this context, institutions such as the United Nations, global health organizations, and security alliances play a critical role in responding effectively to these threats.

Taken together, these characteristics demonstrate that Asymmetric Threats require comprehensive and cross-sectoral security strategies that integrate military, political, economic, social, and environmental dimensions, reflecting the transformation in the understanding of national security in the twenty-first century (Buzan, Wæver, & de Wilde, 1998, p. 36).

Fourth: Examples of Asymmetric Threats.

Asymmetric Threats manifest in several practical phenomena that have had tangible impacts on national security across the globe, the most prominent examples include:

1- International Terrorism:

International terrorism constitutes a direct threat to both state and societal security, targeting civilians and vital institutions alike, prominent examples include organizations such as Al-Qaeda and ISIS, which have carried out large-scale attacks resulting in significant human and material losses, and have undermined political and economic stability in affected states (Buzan & Hansen, 2009, p. 27), Kessler further notes that international terrorism frequently operates across borders and requires multilateral cooperation to be effectively countered (Kessler, 2014, p. 52).

2- Cybersecurity Threats:

Attacks on information infrastructure and the theft of sensitive data have become among the most significant Asymmetric Threats, particularly given the increasing reliance on digital technologies, contemporary examples include cyberattacks targeting banks and government institutions, which undermine national economies and erode public trust in the state (Clarke & Knake, 2010, p. 30).

3- Natural Disasters and Pandemics:

Environmental disasters and pandemics represent asymmetric threats that directly affect social and economic stability, a prominent example is the COVID-19 pandemic, which triggered a global health crisis and generated severe economic, political, and social pressures (Beck, 1992, p. 24), and these cases underscore the importance of incorporating health and environmental dimensions into national security strategies.

4- Illegal Migration and Transnational Crime:

These phenomena pose direct threats to internal stability by affecting social, economic, and political security, they include drug and arms trafficking, human trafficking, and irregular migration, all of which often require regional and international cooperation to be effectively addressed (Buzan & Hansen, 2009, p. 28).

These examples illustrate that Asymmetric Threats are interconnected and multidimensional, necessitating comprehensive national security approaches that combine military, political, economic, social, technological, and environmental measures (Buzan & Hansen, 2009, p. 25).

This section concludes that Asymmetric Threats constitute a complex challenge to national security, as they transcend the scope of traditional military capabilities and require a comprehensive approach encompassing political, military, economic, social, health, and environmental dimensions, the analysis highlights that understanding these threats and recognizing their defining characteristics is a fundamental step toward developing effective security strategies capable of addressing contemporary and future risks.

Section Three: Theories Explaining Non-Traditional Security

This section focuses on the theories that explain the concept of non-traditional security and the ways to address contemporary threats that go beyond conventional military boundaries, these theories include classical realist security theory, the Copenhagen School of broadened security, liberal interdependence theory, and human security theory.

The section highlights the contribution of each theory to understanding the various dimensions of security, ranging from military power and sovereignty to the protection of individuals and societies, it also examines how these theories can be integrated to provide a multi-level and multidimensional framework for addressing Asymmetric Threats.

First: Traditional Security Theory (Realist Security Theory).

Traditional security theory, grounded in political realism, focuses on the state as the primary actor in the international system and on conventional military threats, this theory is based on the assumption that the international system is inherently anarchic, prompting states to seek survival through the accumulation of power, particularly military power and deterrence, accordingly, security is closely linked to a state's military capabilities and strategic position (Morgenthau, 1948, p. 16).

From this perspective, external threats are viewed as the main determinants of a state's defense and strategic policies, military alliances and the balance of power are considered essential tools for achieving stability and security, while national sovereignty and territorial integrity occupy a central position in the concept of security.

However, with the emergence of Asymmetric Threats in the twenty-first century—such as international terrorism, cyberattacks, and transboundary pandemics—classical realism has faced difficulties in explaining these phenomena, this is due to its primary focus on conventional military power and the state as the sole decision-maker in security affairs. For example, cyberattacks do not require a physical army and are not constrained by geographical borders, while pandemics cannot be deterred through military force; this clearly illustrates the limitations of the traditional security model (Morgenthau, 1948, p. 16).

Thus, while classical realism remains useful in explaining direct military threats, it is limited in addressing multidimensional and transnational threats, necessitating the development of more comprehensive theoretical frameworks that incorporate economic, political, social, and environmental dimensions of security.

Second: Broad Security Theory (The Copenhagen School).

The Copenhagen School of security, led by Barry Buzan and Ole Wæver, introduced the concept of securitization, which expands security beyond the traditional military focus to include political, economic, social, cultural, environmental, health, and cyber dimensions (Buzan, Wæver, & de Wilde, 1998, p. 8), this theory argues that threats are not purely objective realities but are constructed through political discourse, in other words, an issue becomes a security threat when it is framed as such by authoritative actors, thereby legitimizing the adoption of extraordinary measures to address it.

This framework provides an effective explanation for Asymmetric Threats such as international terrorism, cyberattacks, environmental disasters, and global pandemics, as these phenomena are multidimensional and cannot be addressed through military force alone. For example:

- Cyberattacks require coordination between the public and private sectors to protect digital infrastructure.
- Global pandemics demand integrated health policies at both national and international levels.
- Environmental disasters necessitate joint environmental and economic policies and cooperation among states and international organizations.

By employing the concept of broadened security, these threats can be understood as security issues with multiple dimensions, thereby expanding the scope of traditional security policies and strategies to encompass all vital sectors of the state and society (Buzan, Wæver, & de Wilde, 1998, p. 9).

Third: Complex Interdependence Theory (Liberal Approach).

The liberal approach to international relations—particularly complex interdependence theory, developed by Robert Keohane and Joseph Nye—emphasizes that relations among states and international actors are multi-layered and interconnected, and that security is no longer confined to military power alone (Keohane & Nye, 1977, p. 21). This theory assumes that non-traditional challenges such as cyberattacks, transnational crime, global pandemics, natural disasters, and irregular migration cannot be addressed without international cooperation and multilateral institutions. For instance:

- Cyberattacks targeting banks or energy networks require global coordination and shared regulatory frameworks between states and private institutions.
- Global pandemics such as COVID-19 necessitate coordinated health policies and data sharing among states and international organizations.
- Transboundary environmental threats such as climate change require international agreements to regulate and manage natural resources.

From this perspective, security shifts from a focus on the individual state and national sovereignty to a comprehensive, multi-actor security framework that integrates political, economic, social, environmental, health, and technological dimensions, thus complex interdependence theory offers a strong explanatory framework for understanding Asymmetric Threats and managing international risks collectively (Keohane & Nye, 1977, p. 22).

Fourth: Human Security Theory.

Human security theory provides a modern framework that places individuals and communities at the center of security concerns, rather than focusing exclusively on the state, according to the United Nations Development Programme (UNDP, 1994, p. 22), human security includes protection from poverty, hunger, disease, internal conflict, and political violence, enabling a comprehensive understanding of security beyond the traditional military dimension, this theory is particularly well suited to explaining Asymmetric Threats, as many of these threats directly affect individuals before impacting the state or society, for example:

- Natural disasters such as floods and earthquakes threaten the lives of individuals and local communities, requiring rapid humanitarian responses.

- Global pandemics, such as COVID-19, affect public health, economies, and societies as a whole, highlighting the need for strong health systems and effective preventive strategies.
- Irregular migration and transnational crime affect individual safety and fundamental human rights, necessitating social and humanitarian interventions alongside security measures.

From this perspective, human security complements the previous theories:

- Realism focuses on the state and military power,
- The Copenhagen School expands the concept of threats,
- Liberalism emphasizes international cooperation,
- Human security places individuals and communities at the heart of security policies.

This theoretical integration enables the formulation of comprehensive and sustainable security strategies capable of addressing multidimensional Asymmetric Threats, with a strong emphasis on prevention and human protection as a priority (UNDP, 1994, p. 23).

Fifth: Theoretical Integration for Addressing Asymmetric Threats.

The four security theories can be integrated to provide a multi-level framework for understanding and responding comprehensively to Asymmetric Threats:

1- Realist Security Theory:

Provides the foundation for understanding the importance of power and defensive capabilities in confronting direct military threats, such as organized terrorist attacks or cross-border hostilities (Waltz, 1979, p. 91).

2- The Copenhagen School (Broad Security):

Focuses on expanding and politically diagnosing threats, demonstrating that security issues are not merely objective realities but are constructed through political discourse that legitimizes extraordinary measures to address multidimensional threats such as cyberattacks and environmental disasters (Buzan, Wæver, & de Wilde, 1998, p. 10).

3- Liberalism and Complex Interdependence:

Emphasizes the importance of international cooperation and multilateral institutions, as transboundary threats such as pandemics and cyberattacks require coordinated strategies among states and international organizations to ensure effective risk management (Keohane & Nye, 1977, p. 21).

4- Human Security Theory:

Places individuals and communities at the center of security concerns, highlighting the need to protect people from poverty, hunger, disease, violence, and internal conflict—making it particularly relevant for understanding Asymmetric Threats that directly affect human lives (UNDP, 1994, p. 22).

Through this theoretical integration, comprehensive and adaptable security strategies can be developed to address multidimensional and evolving Asymmetric Threats. This framework combines military capability, political threat construction, international cooperation, and human protection, reflecting the shift from a state-centric understanding of security to a comprehensive, multi-level approach capable of confronting terrorism, cyber threats, environmental disasters, pandemics, and other contemporary challenges.

This section concludes that understanding non-traditional security requires the integration of multiple theoretical perspectives, realism contributes to assessing power and defense capabilities; the Copenhagen School highlights the role of political discourse in defining threats; liberalism emphasizes international cooperation; and human security places individuals and societies at the core of security concerns, this theoretical integration provides a flexible and effective strategic framework through which comprehensive security policies can be formulated to confront the complex and evolving threats of the modern era.

The chapter ultimately concludes that national security is no longer confined to military power alone but depends on a comprehensive, multidimensional approach. Asymmetric

Threats are complex and multifaceted; requiring integrated strategies, the theoretical synthesis of realism, the Copenhagen School, liberalism, and human security offers an effective framework for understanding these threats, paving the way for subsequent chapters on the types of threats and the national and international strategies for addressing them.

Chapter Two: Types of Asymmetric Threats.

This chapter examines the various forms of Asymmetric Threats that confront national security in the modern era; these include terrorism and organized crime, cyber threats, health and environmental threats, and economic threats.

The chapter focuses on the characteristics of these threats, their transnational nature, their multidimensional impacts, and the difficulty of predicting them; it also highlights the security dimensions of each type of threat, thereby contributing to a deeper understanding of their effects on both the state and society.

Section One: Terrorism and Organized Crime.

Terrorism and organized crime represent some of the most prominent Asymmetric Threats facing states and societies today, these threats are characterized by their transnational reach, interconnected dimensions, and reliance on illicit financing, making them highly complex security challenges, this section aims to clarify the concepts of terrorism and organized crime, examine their characteristics, and analyze their security dimensions, with particular emphasis on their impact on political, social, and economic stability.

First: Definition of Terrorism and Organized Crime.

Terrorism is defined as the use of violence or the threat of violence to achieve political, religious, or ideological objectives, often targeting civilians or government symbols in order to instill fear and influence political decision-making (Hoffman, 2006, p. 40).

According to the United Nations, terrorism includes:

“Acts intended to cause death or serious bodily injury to civilians or non-combatants, with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act” (United Nations, 1999, p. 5).

Terrorism can be distinguished from organized crime in terms of ultimate objectives: terrorism seeks political or ideological goals, whereas organized crime primarily aims at direct and illicit financial gain, however, the two phenomena often intersect, as terrorist groups may exploit organized crime networks to finance their operations or engage in illegal activities to enhance their capabilities (Laqueur, 2003, pp. 15–18), transnational organized crime refers to planned and structured criminal activity carried out by groups of individuals with the aim of obtaining illicit material benefits, such activities include drug trafficking, human trafficking, arms smuggling, and money laundering (UNODC, 2010, p. 13).

Organized crime is characterized by secrecy, hierarchical or network-based structures and the ability to evade law enforcement, its activities often extend beyond national borders, making international cooperation essential for effective countermeasures.

The Relationship between Terrorism and Organized Crime:

- **Terrorist Financing:** Some terrorist groups rely on organized crime activities such as drug trafficking and money laundering to fund their operations.
- **Exploitation of Instability:** In conflict zones, terrorist groups may exploit criminal activities to expand their influence or secure financial resources.
- **Multidimensional Threat:** Both phenomena threaten political, social, and economic security, necessitating comprehensive and multi-level security policies.

Second: Characteristics of Terrorism and Organized Crime.

Terrorism and organized crime share several key characteristics that make them complex security challenges and require multi-level response strategies:

1- Transnational Nature:

Terrorist and organized crime activities frequently extend beyond the borders of a single state, such as international terrorist networks or global drug trafficking routes, making regional and international cooperation essential.

2- Networked and Structured:

These phenomena rely on sophisticated and clandestine organizational structures, whether terrorist cells or criminal syndicates, with a strong capacity for strategic planning and covert execution.

3- Illicit Financing:

Organized crime networks are often used to finance terrorist operations, creating an interlinked cycle between transnational crime and terrorism and complicating efforts to track and disrupt illegal financial flows.

4- Multidimensional Impact:

Terrorism and organized crime affect political, economic, social, and even human security, they undermine state stability, weaken national economies, disrupt social cohesion, and directly threaten individual lives (Laqueur, 2003, p. 15).

5- Unpredictability and Difficulty of Control:

The secretive and complex nature of these activities makes them difficult to anticipate or eliminate quickly, requiring advanced intelligence capabilities, continuous monitoring, and flexible preventive strategies.

These characteristics demonstrate that terrorism and organized crime constitute asymmetrical, multidimensional threats, addressing them cannot rely solely on military or legal measures but requires an integrated approach encompassing political, social, economic, and informational security—reflecting the shift toward a comprehensive security paradigm.

Third: Security Dimensions of Terrorism and Organized Crime.

Terrorism and organized crime pose multidimensional threats to national and international security, which can be analyzed through the following dimensions:

1- Political Dimension:

Terrorist groups threaten state stability and legitimate governance by targeting government institutions or influencing political decision-making, organized crime, in turn, undermines state authority and legal institutions through corruption, money laundering, and intimidation, weakening the state's ability to enforce the rule of law (Hoffman, 2006, p. 41).

2- Military and Security Dimension:

Counterterrorism requires equipping security and intelligence forces to combat armed groups, secure borders, and protect critical infrastructure, it also necessitates coordination among national agencies and international partners to combat transnational criminal activities (Laqueur, 2003, p. 16).

3- Economic Dimension:

Terrorism and organized crime directly affect investment, tourism, and financial markets; they increase security costs and create an unstable economic environment that hinders development and economic growth (Laqueur, 2003, p. 16).

4- Social Dimension:

These threats undermine trust between citizens and the government, weaken social cohesion, and generate widespread fear and insecurity, such conditions may increase susceptibility to extremist narratives or criminal behavior (Laqueur, 2003, p. 17).

These dimensions highlight that terrorism and organized crime are not merely military or legal threats but complex, asymmetrical, and multidimensional challenges, addressing them requires comprehensive security strategies that integrate political action, intelligence cooperation, economic measures, and civil society engagement—reflecting the evolution

toward a holistic and integrated security framework, this section concludes that terrorism and organized crime represent multidimensional threats that require an integrated response combining security enforcement, international cooperation, and societal awareness, addressing these phenomena cannot be limited to military measures alone; it must also encompass economic, social, and political dimensions to ensure state stability and protect citizens from the consequences of transnational criminal and terrorist activities.

Section Two: Cyber Threats.

Cyber threats are among the most prominent manifestations of asymmetric threats facing states in the digital age, they are transnational in nature, rapidly evolving, and have significant impacts on political, economic, and social security, this section focuses on defining cyber threats, identifying their characteristics and types, and analyzing their associated security dimensions, while emphasizing the importance of developing effective protection mechanisms to address these growing risks.

First: Definition of Cyber Threats.

Cyber threats refer to any attack or malicious activity targeting information systems, digital data, or the electronic infrastructure of a state or private institutions, with the intent of disrupting operations, stealing information, or causing economic, political, or social damage (Libicki, 2007, p. 3), the U.S. Cybersecurity and Infrastructure Security Agency (CISA) defines a cyber threat as: “Any event or series of unwanted events on an information system, including cyberattacks on networks or attacks on critical infrastructure, that threaten national security, economic security, or social stability”(CISA, 2020, p. 4).

Cyber threats can be classified into the following main types (CISA, 2020, p. 4):

1- Attacks on Critical Infrastructure:

Such as electricity grids, water systems, airports, and transportation networks, which may affect millions of people and disrupt essential state services.

2- Cyberattacks on Data:

Including the theft, manipulation, or destruction of sensitive information, whether governmental, commercial, or military.

3- Malware and Virus Attacks:

These attacks target operating systems or databases, causing major disruptions to vital institutions.

4- Attacks on Individuals and Institutions:

Such as cyber extortion, phishing, or attacks on personal devices, which may result in financial losses or threaten individual safety.

These classifications demonstrate that cyber threats are transnational, persistent, and rapidly adaptable, making them one of the most significant contemporary asymmetric threats to national security, consequently, they require multi-stakeholder cooperation and comprehensive security strategies involving states, private institutions, and international organizations.

Second: Characteristics of Cyber Threats.

Cyber threats represent one of the most significant forms of asymmetric threats and possess several characteristics that make them complex security challenges, these characteristics can be summarized as follows (Kello, 2013, p. 13):

1- Transnational Nature:

Cyberattacks can be launched from anywhere in the world, regardless of geographical borders, making regional and international cooperation essential for tracking and effectively countering such attacks.

2- Stealth and Concealment:

Cyberattacks are often difficult to detect or attribute quickly, allowing malicious activities to persist over extended periods and complicating immediate preventive responses.

3- Dynamic and Rapidly Evolving:

Cyber threats rely on advanced technologies that continuously evolve, including malware, viruses, and artificial intelligence-based attacks; this requires constant updates to cybersecurity strategies to keep pace with emerging techniques.

4- Wide-ranging Impacts:

Cyberattacks can affect economic, political, social, and even health security by disrupting critical infrastructure and compromising sensitive data, thereby threatening national stability.

5- Multi-Stakeholder Response Requirement:

Addressing cyber threats cannot rely solely on state efforts; it requires the participation of private companies, international organizations, and civil society to develop comprehensive security policies and advanced technical solutions.

These characteristics illustrate that cyber threats are more complex and sophisticated than traditional threats, and that countering them necessitates a comprehensive, multi-level security framework encompassing national security, economic security, critical infrastructure protection, and the promotion of digital awareness among individuals and institutions.

Third: Security Dimensions of Cyber Threats.

Cyber threats represent a form of asymmetric threats that affect national security through several interrelated dimensions:

1- Political Dimension:

Cyberattacks may target elections, government institutions, or the confidentiality of political decision-making processes, thereby threatening state stability and the integrity of political systems. For example, cyberattacks on U.S. electoral systems in 2016 demonstrated the capacity to influence public opinion and undermine democratic processes (Kello, 2013, p. 13).

2- Economic Dimension:

Cyberattacks affect financial institutions, stock markets, and supply chains, causing substantial material losses and long-term impacts on investment and economic confidence, notable examples include the WannaCry and NotPetya attacks on global corporations, which resulted in billions of dollars in losses (Libicki, 2007, p. 4).

3- Military and Security Dimension:

Cyberattacks can be used to disrupt military communications or national defense networks, increasing the risk of physical attacks or weakening overall security preparedness, attacks on Ukraine's energy infrastructure illustrated the significant impact of cyber operations on both military and civilian security (CISA, 2020, p. 4).

4- Social Dimension:

Cyber threats undermine digital trust between citizens and institutions, increase public anxiety and information disorder, and contribute to the spread of misinformation or political propaganda, thereby negatively affecting social cohesion.

These dimensions demonstrate that cyber threats are complex and multidimensional, and that addressing them requires comprehensive strategies integrating state authorities, the private sector, and international institutions to enhance political, economic, military, and social security simultaneously (Libicki, 2007, p. 4).

This section concludes that cyber threats constitute an increasingly complex challenge for states and societies, as they cannot be countered through traditional means alone; instead, they require multi-level strategies encompassing secure digital infrastructure, international cooperation, and the development of advanced detection and response capabilities, adopting such policies strengthens national stability, protects critical information assets, and contributes to reducing the negative impacts of cyber threats on national security.

Section Three: Health and Environmental Threats.

Health and environmental threats are among the most prominent non-traditional challenges facing states and societies in the modern era, they are transboundary, long-term, and multidimensional in nature, encompassing epidemics, pandemics, natural disasters, and

climate change, this section aims to clarify the concept of health and environmental threats, their main characteristics, and their various security dimensions, with particular emphasis on their direct impact on individuals, society, and overall state stability.

First: Definition of Health and Environmental Threats.

Health threats refer to risks that pose widespread dangers to the health of individuals and societies, such as epidemics, pandemics, and infectious diseases, which can directly affect state stability and national security (Fidler, 2004, p. 15), these threats, include pressure on healthcare systems, increased mortality rates, disruption of public services, and broad economic and social repercussions.

Environmental threats, on the other hand, are risks associated with natural disasters, climate change, and environmental degradation, which can affect critical infrastructure, economic resources, and the social and political stability of states (Barnett & Adger, 2007, p. 615), examples of such threats include floods, wildfires, water scarcity, and land degradation.

These threats combine direct impacts on individuals and communities with broader consequences for national, economic, and political security, making them a central component of contemporary asymmetric threats; this underscores the need for comprehensive and multi-actor security strategies to address them effectively.

Second: Characteristics of Health and Environmental Threats.

Health and environmental threats possess several characteristics that make them complex non-traditional security challenges (Kickbusch & Silberschmidt, 2007, p. 3):

1- Transboundary Nature:

Epidemics and environmental disasters can spread across national borders, making regional and international cooperation essential for coordinated and effective responses.

2- Long-term Impact:

The effects of these threats often extend over long periods, as in the case of climate change or the depletion of natural resources, requiring sustainable strategies for risk management.

3- Multidimensional Nature:

These threats encompass health, economic, social, and political dimensions. A single pandemic or environmental disaster can affect individuals' lives, the national economy, social stability, and state decision-making processes.

4- Difficulty of Prediction and Control:

The unpredictable nature of epidemics and environmental disasters makes proactive intervention and security planning particularly challenging; necessitating advanced monitoring and analytical mechanisms to mitigate potential damage.

5- Need for Multi-Stakeholder Coordination:

Addressing these threats cannot be achieved by the state alone; it requires the involvement of governments, international organizations, the private sector, and civil society to develop effective and sustainable response plans, these characteristics indicate that health and environmental threats are integral to comprehensive national security, as their impacts intersect with multiple security dimensions and require integrated, multi-level strategies to ensure preparedness, prevention, and risk reduction.

Third: Security Dimensions of Health and Environmental Threats.

Health and environmental threats represent multidimensional challenges to national security, as their effects extend across health, economic, social, political, and environmental spheres, compelling states to develop comprehensive strategies to address them (Barnett & Adger, 2007, p. 615):

1- Health and Security Dimension:

Epidemics and pandemics affect a state's healthcare capacity by increasing mortality rates, placing pressure on hospitals, and creating shortages of medical resources, as witnessed during the COVID-19 pandemic, this makes health security an integral component of national security.

2- Economic Dimension:

Natural disasters and epidemics cause significant material losses by disrupting production, reducing investment, and weakening supply chains, thereby directly affecting national economic stability.

3- Social Dimension:

These threats increase social vulnerability through job losses, weakened social cohesion, and declining trust between citizens and governments, exacerbating internal tensions and increasing the risk of societal conflict.

4- Political Dimension:

Health and environmental threats can undermine political stability by placing immense pressure on state institutions, weakening governance capacity, and complicating strategic decision-making processes during crises.

5- Environmental Dimension:

This dimension includes the effects of climate change, water scarcity, and the depletion of natural resources, which threaten the sustainability of societies and states and increase the likelihood of conflicts over natural resources, these dimensions demonstrate that addressing health and environmental threats requires integrated, multi-actor security strategies involving states, international organizations, the private sector, and civil society, in order to mitigate risks and ensure comprehensive national security.

This section concludes that health and environmental threats constitute an increasingly complex strategic risk, affecting the health, economic, social, and political security of states, it also emphasizes the necessity of preventive planning and multi-actor responses involving governments, international organizations, and the private sector to minimize damage and enhance sustainability, understanding and addressing these threats through an integrated approach contributes to achieving comprehensive security and protecting societies from contemporary non-traditional risks.

Section Four: Economic Threats.

Economic threats are among the most prominent non-traditional challenges affecting state stability and national security; these threats include financial crises, inflation, fluctuations in the prices of essential resources, and economic blockades, all of which can transform economic problems into political and social crises, this section aims to clarify the concept of economic threats, their main characteristics, and their multiple security dimensions, with a focus on how they affect the state and society.

First: Definition of Economic Threats.

Economic threats refer to any risks that affect a state's economic stability, its capacity for growth, and the security of its vital resources; these threats typically include financial crises, economic recession, and hyperinflation, fluctuations in the prices of key resources, as well as economic blockades or international sanctions (Buzan & Hansen, 2009, p. 45), studies indicate that such threats are not merely financial or economic issues in a narrow sense, but can evolve into political and social risks that directly affect national security, this is particularly evident when economic instability leads to job losses, declining living standards, rising poverty, and increased migration, making economic security a fundamental component of comprehensive national security (Krahmann, 2003, p. 76).

Second: Characteristics of Economic Threats.

Economic threats possess several characteristics that make them asymmetric threats with both direct and indirect impacts on national security (Buzan & Hansen, 2009, p. 48):

1- Transnational Nature:

Economic crises often spread through global markets, such as international financial crises or fluctuations in oil prices, rendering the response of a single state insufficient.

2- Dynamic and Rapid Impact:

Economic threats can emerge suddenly and cause severe losses within a short period, such as abrupt financial downturns or stock market collapses.

3- Multidimensional Nature:

These threats simultaneously affect political, social, and economic dimensions, as economic crises may lead to social unrest or a loss of trust in political institutions.

4- Complexity and Difficulty of Control:

Economic threats involve an interaction between internal and external factors, including global financial policies and fluctuations in resource prices, which limit the effectiveness of purely national or preventive interventions.

5- Need for Multi-Stakeholder Coordination:

States often need to cooperate with international financial institutions, regional organizations, and the private sector to mitigate the impacts of economic threats and ensure market and economic stability.

Third: Security Dimensions of Economic Threats.

Economic threats intersect with multiple dimensions of national security, as their impacts extend beyond the economic sphere to include social, political, and security aspects (Buzan & Hansen, 2009, p. 49):

1- Economic Dimension:

Economic crises directly affect investment, production, and trade, potentially leading to declines in gross domestic product and rising unemployment, thereby weakening the state's ability to respond to other crises.

2- Social Dimension:

Economic instability can increase poverty and social vulnerability, intensify internal tensions among citizens, and threaten social cohesion and societal stability.

3- Political Dimension:

Economic pressures pose challenges to good governance and strategic decision-making, and may result in declining political legitimacy or widespread public protests.

4- Security Dimension:

Severe economic crises may lead to mass protests, internal unrest, and conflicts over resources, threatening national security and necessitating intervention by security institutions to maintain stability.

These dimensions demonstrate that economic threats constitute a core element of contemporary Asymmetric Threats, as they affect national security at multiple levels and require comprehensive strategies that integrate economic resilience, social and political coordination, and security protection.

This section concludes that economic threats represent a multidimensional risk, affecting a state's economic, social, and political security, and potentially leading to internal protests and instability if not addressed effectively, the analysis also emphasizes the importance of strategic planning, international cooperation, and preventive responses to reduce the impact of these threats and enhance economic and social stability.

The chapter concludes that Asymmetric Threats represent a complex challenge that goes beyond the scope of traditional military power and affects all dimensions of national security. It highlights the need for a comprehensive approach to understanding and managing these threats, taking into account their multidimensional and transboundary nature, this analytical foundation paves the way for examining national strategies and international cooperation mechanisms for addressing Asymmetric Threats in the following chapter.

Chapter Three: Strategies for Confronting Asymmetric Threats.

This chapter examines the approaches and strategies adopted by states and the international community to confront Asymmetric Threats; it addresses national strategies, regional and international cooperation, and the development of risk management mechanisms, the chapter emphasizes the importance of integrating all dimensions of security—political, military, economic, social, health, and environmental—within a comprehensive framework, while

adopting flexible and proactive strategies that enable effective responses to transboundary and constantly evolving threats.

Section One: National Strategies.

National strategies constitute a fundamental tool for guiding the state in confronting both traditional and Asymmetric Threats, They define security, political, and economic objectives and direct resources and actions to ensure the protection of national sovereignty, internal stability, and national security, this section aims to present the concept of national strategies, their characteristics, and their objectives, while highlighting their importance in building state capacity to address complex and evolving challenges.

First: Definition of National Strategies.

National strategies refer to the official frameworks and plans formulated by the state to define its security, political, and economic objectives, and to guide resources and actions toward achieving them (Gray, 2010, p. 3), these strategies aim to enhance national security, protect vital interests, and ensure the capacity to confront both traditional and Asymmetric Threats, including terrorism, cyberattacks, economic crises, and health or environmental disasters (Nye, 2009, p. 23), national strategy represents a comprehensive roadmap that directs government institutions—security, economic, and administrative—toward achieving state stability, protecting citizens, and ensuring long-term sustainability, it also enables effective coordination among national institutions and international partners to address rapidly changing and transboundary threats.

Second: Characteristics of National Strategies.

National strategies are characterized by several features that make them an effective tool for managing national security and confronting traditional and Asymmetric Threats (Gray, 2010, p. 12):

1- Comprehensiveness:

They encompass all dimensions of security—political, military, economic, social, health, and environmental—ensuring a holistic approach to addressing threats at the state level.

2- Flexibility:

National strategies are adaptable to regional and international changes and emerging threats, allowing for rapid and effective responses to evolving challenges.

3- Collaboration:

They require coordination among governmental institutions, the private sector, and international organizations, enhancing collective capacity to confront transboundary threats.

4- Proactivity:

These strategies focus not only on responding to crises after they occur, but also on prevention and risk reduction through forward planning and strategic resource allocation.

5- Actionability:

National strategies include concrete plans and programs for resource allocation and goal implementation, making them practical and operational rather than merely theoretical frameworks.

Third: Objectives of National Strategies.

National strategies aim to achieve a set of core objectives that strengthen national security and state stability in the face of both traditional and Asymmetric Threats, including:

1- Protecting national sovereignty and vital interests:

Safeguarding state independence and decision-making autonomy, and securing vital resources to ensure the continuity of essential state functions.

2- Ensuring internal stability and social cohesion:

Promoting national unity and trust between citizens and the state, and reducing social tensions that may be exploited by terrorist groups or Asymmetric Threats.

3- Enhancing defensive capabilities and addressing security threats:

Developing armed forces, security services, and intelligence agencies to effectively confront traditional military threats, terrorism, and cyber threats.

4- Ensuring economic security and financial sustainability:

Protecting the national economy from financial crises, fluctuations in essential resource prices, and economic blockades, thereby ensuring stable economic growth and living standards.

5- Developing capacity to manage health and environmental crises and natural disasters:

Establishing plans and strategies to respond to pandemics, environmental disasters, and climate change, thereby mitigating their impact on individuals and critical state infrastructure.

Formulating these objectives in a comprehensive and strategic manner enables the state to unify national efforts and coordinate with international partners to confront transboundary and multidimensional threats effectively (Gray, 2010, p. 13).

This section demonstrates that national strategies represent a comprehensive and flexible roadmap that enables the state to prevent and respond to crises effectively, the analysis underscores the importance of their inclusiveness, inter-institutional cooperation, and adaptability in addressing diverse threats, thereby enhancing the state's ability to protect its vital interests and ensure national security and stability.

Section Two: Regional and International Cooperation.

Regional and international cooperation constitutes a fundamental pillar in confronting transboundary Asymmetric Threats such as terrorism, cyberattacks, pandemics, and economic crises; this cooperation enables information sharing, strategic coordination, and the enhancement of joint capacities among states and regional and international organizations, this section aims to clarify the concept of cooperation, its importance, and its security, economic, health, and cyber dimensions.

First: Definition of Regional and International Cooperation.

Regional and international cooperation refers to the coordination of policies and actions among states and regional and international organizations to confront shared threats, whether security-related, economic, health-related, or environmental (Keohane, 1984, p. 71), this cooperation seeks to strengthen national capacities, exchange information and expertise, and implement joint strategies to mitigate the effects of transboundary risks.

Nye emphasizes that international cooperation includes several key elements, such as (Nye, 2009, p. 24):

- 1- Intelligence information sharing among states to combat terrorism and transnational organized crime.
- 2- Technical and training support to enhance states' capacities in managing complex crises.
- 3- Developing joint emergency strategies to address pandemics, natural disasters, and economic crises.
- 4- Implementing multilateral agreements to enhance regional and international security and stability.

This definition highlights that international cooperation is no longer an option, but rather a strategic necessity for addressing Asymmetric Threats characterized by transboundary nature and multidimensional impacts, requiring active participation from states, international organizations, the private sector, and civil society.

Second: The Importance of Cooperation in Confronting Asymmetric Threats.

Regional and international cooperation plays a vital role in addressing Asymmetric Threats across several domains:

1- Combating terrorism and organized crime:

International and regional cooperation facilitates intelligence sharing, coordination of security operations, and disruption of financial networks, thereby enhancing states' ability to confront transnational terrorist groups and criminal organizations (Buzan & Hansen, 2009, p. 52).

2- Countering cyber threats:

Due to the transboundary and technologically advanced nature of cyberattacks, international cooperation is essential for exchanging expertise, building secure digital infrastructure, and developing joint monitoring and response mechanisms (Kello, 2013, p. 18).

3- Health and environmental threats:

Pandemics and environmental disasters transcend national borders, necessitating the exchange of scientific data, cooperation in emergency planning, and support for vulnerable states to strengthen preventive capacities and rapid response mechanisms (Kickbusch & Silberschmidt, 2007, p. 7).

4- Economic crises:

Global economic crises require coordination of financial and monetary policies, support for international financial stability, and collective measures to mitigate the effects of economic shocks at national and regional levels (Krahmann, 2003, p. 80).

This vital role of international cooperation reflects the necessity of multilateral coordination in confronting asymmetric and multidimensional threats, as no single state can effectively manage these risks independently.

Third: Dimensions of Regional and International Cooperation.

Regional and international cooperation encompasses several interrelated dimensions that reflect the multi-level nature of contemporary security:

1- Security dimensions:

Including military alliances, intelligence sharing, and coordination in combating terrorism and transnational crime, thereby enhancing national and regional security.

2- Economic dimensions:

Encompassing financial cooperation, combating money laundering, and protecting global markets from economic crises to ensure national and regional economic stability.

3- Health and environmental dimensions:

Involving the exchange of expertise and scientific data to address pandemics, natural disasters, and climate change, enhancing rapid response capabilities and reducing the impact of transboundary risks.

4- Technological and cyber dimensions:

Including the protection of cyberspace, sharing information on cyber threats, and establishing joint digital security protocols to enhance information stability and electronic infrastructure resilience.

Strengthening regional and international cooperation reflects the shift toward comprehensive, multidimensional security, where the state's ability to protect itself extends beyond military power to include strategic coordination, information sharing, and effective international partnerships (Buzan, Wæver, & de Wilde, 1998, p. 18).

This section demonstrates that regional and international cooperation enhances states' capacity to confront shared risks more effectively than unilateral efforts. It also enables the coordination of resources and expertise, information exchange, and the development of joint response mechanisms, making security strategies more comprehensive and capable of addressing complex and evolving challenges in the contemporary world.

Section Three: Future Challenges and Opportunities.

States today face an increasing array of complex Asymmetric Threats, including terrorism, cyberattacks, pandemics, environmental disasters, and economic crises. These threats pose significant challenges in prediction, management, and international coordination, at the same time, this evolving environment offers opportunities to enhance international cooperation, adopt advanced technologies, and develop comprehensive and multidimensional security strategies, this section aims to explore the most significant future challenges and opportunities in the field of non-traditional security.

First: Future Challenges.

States face several future challenges in the realm of non-traditional security, including:

1- The escalation of transnational terrorism and organized crime:

As terrorist organizations evolve and increasingly utilize modern technologies, predicting attacks and tracking financial networks becomes more difficult, complicating security responses (Hoffman, 2006, p. 60).

2- Advanced cyber threats:

The expansion of digitalization and reliance on digital infrastructure exposes states to sophisticated cyber threats such as cyber espionage, digital extortion, and disruption of vital services, necessitating the development of advanced defensive strategies (Kello, 2013, p. 25).

3- Unpredictable pandemics and environmental disasters:

Climate change, droughts, and natural disasters, alongside the emergence of new pandemics, place immense pressure on public health systems, food security, and environmental stability, increasing state vulnerability to transboundary threats (Barnett & Adger, 2007, p. 622).

4- Global economic challenges:

Financial volatility, economic crises, and trade wars affect state stability and weaken their ability to address internal and external crises, potentially increasing poverty, migration, and social tensions (Krahmann, 2003, p. 85).

5- The complexity of managing international cooperation:

The multiplicity of actors and coordination challenges among states and international organizations may hinder effective responses to transboundary threats, necessitating the development of flexible and efficient cooperation mechanisms at regional and international levels (Keohane, 1984, p. 75).

Second: Future Opportunities:

Alongside challenges, the evolving security landscape also presents opportunities for enhancing cooperation, innovation, and resilience.

1- Strengthening regional and international cooperation:

Cooperation among states and regional and international organizations represents one of the most important opportunities for confronting Asymmetric Threats, this includes developing multilateral agreements, intelligence sharing, coordinating emergency plans, and sharing human and technical resources, past experiences demonstrate that states engaged in regional and international cooperation networks are better equipped to address terrorism, organized crime, and transboundary crises (Nye, 2009, p. 30).

2- Leveraging technology to enhance security:

Advanced technologies play a critical role in early threat detection and prediction, the use of artificial intelligence, big data analytics, and advanced cybersecurity technologies contributes to monitoring cyberattacks, analyzing transnational crime patterns, and predicting health pandemics (Libicki, 2007, p. 12).

3- Adopting the concept of comprehensive and multidimensional security:

Integrating military, economic, social, health, and environmental security enables more effective responses to complex challenges. This approach emphasizes the integration of traditional and non-traditional security policies within a unified strategic framework focused on prevention and risk management rather than reactive responses (Buzan, Wæver, & de Wilde, 1998, p. 22).

4- Benefiting from international experiences and best practices:

Studying past major crises provides valuable insights for developing flexible national and regional strategies. Lessons learned from the COVID-19 pandemic and major cyberattacks highlight the importance of emergency planning, joint training, and coordination among multiple actors (Kickbusch & Silberschmidt, 2007, p. 14).

5- Investing in education and awareness:

Raising public awareness of non-traditional security issues is a fundamental pillar of national preparedness; this includes educating human resources in cybersecurity, public health, disaster management, and crisis response training, as well as promoting community awareness programs to enhance societal resilience (UNDP, 1994, p. 32).

This section demonstrates that future challenges require integrated and flexible strategies, while emerging opportunities offer pathways to strengthen international cooperation, technological innovation, and human capacity development, by adopting a comprehensive and multidimensional security approach, states can respond effectively to complex threats and transform risks into opportunities for enhanced stability and sustainable development.

The chapter concludes that confronting non-traditional threats requires an integrated approach that combines national capabilities, international cooperation, and proactive preparedness, it also emphasizes the necessity of utilizing modern technologies, strengthening human capacities, and adopting a comprehensive multidimensional security framework to ensure states' ability to protect their vital interests and maintain internal and external stability.

Conclusion:

This research has demonstrated that the concept of security is no longer limited to traditional military security or solely protecting the state, rather, it now encompasses multiple dimensions, including political, economic, social, environmental, health, and digital technology aspects, the importance of unconventional threats has also emerged, such as terrorism, organized crime, cyberattacks, environmental disasters, pandemics, and economic crises, all of which require comprehensive and integrated strategies to address them effectively.

The study addressed three main axes: the theoretical and conceptual framework of unconventional security, the types and dimensions of unconventional threats, and national and international response strategies, in addition to analyzing future challenges and opportunities.

1- Findings:

- **Transformation of the concept of security:** Security now includes human, economic, health, environmental, and cyber dimensions, rather than solely the state's military capabilities.
- **Nature of unconventional threats:** These threats are often transboundary, multidimensional, unpredictable, and complex, necessitating international and regional cooperation.
- **Effectiveness of theoretical integration:** Combining realism, the Copenhagen School, liberalism, and human security theory provides a framework capable of analyzing contemporary threats and formulating appropriate policies.
- **Importance of national strategies:** Comprehensive and actionable strategic planning enhances the state's ability to confront threats, both internally and across borders.
- **Critical role of international and regional cooperation:** Addressing transboundary threats such as terrorism, organized crime, pandemics, and cyberattacks can only be achieved through policy coordination, information sharing, and building strategic alliances.
- **Future challenges:** These include rapid technological developments, global economic crises, climate change, and emerging pandemics, requiring dynamic and adaptable strategies.

2- Recommendations:

- **Strengthen national strategies:** Develop comprehensive plans covering all security dimensions, with an emphasis on proactive and flexible approaches to threats.

- **Enhance international and regional cooperation:** Adopt multilateral agreements for information sharing, coordinated responses, and establishing joint mechanisms to counter transboundary threats.
- **Invest in technology and digital intelligence:** Utilize artificial intelligence, digital analytics, and early-warning tools to detect risks and respond swiftly and effectively.
- **Focus on human and societal security:** Protect individuals, promote social cohesion, and ensure the stability of essential services in the face of health and environmental crises.
- **Build human and institutional capacities:** Develop specialized educational and training programs in cybersecurity, public health, and disaster response.
- **Adopt a comprehensive and multidimensional security approach:** Integrate military, economic, health, environmental, and social dimensions to achieve an integrated and sustainable response to current and future challenges.

Bibliography:

1- Books:

- Beck, U. (1992). *Risk society: Towards a new modernity*. London: Sage.
- Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post-Cold War era* (2nd ed). London: Harvester Wheatsheaf.
- Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*, Cambridge: Cambridge University Press.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder: Lynne Rienner.
- CISA (Cybersecurity and Infrastructure Security Agency). (2020). *Cybersecurity threats and trends*. Washington, DC: U.S. Department of Homeland Security.
- Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. New York: HarperCollins.
- Fidler, D. P. (2004). *SARS, governance and the globalization of disease*. Boulder: Lynne Rienner.
- Gilpin, R. (2001). *Global political economy: Understanding the international economic order*. Princeton: Princeton University Press.
- Gray, C. S. (2010). *War, peace and international relations: An introduction to strategic history*. Routledge.
- Hoffman, B. (2006). *Inside terrorism* (2nd ed.). New York: Columbia University Press.
- Jackson, Robert H. (1990). *Quasi-States: Sovereignty, International Relations, and the Third World*. Cambridge: Cambridge University Press.
- Kello, L. (2013). *The virtual weapon and international order*. New Haven: Yale University Press.
- Keohane, R. O. (1984). *After hegemony: Cooperation and discord in the world political economy*. Princeton: Princeton University Press.
- Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence: World politics in transition*. Boston: Little, Brown.
- Kessler, R. (2014). *Terrorism and global security*. London: Routledge.
- Kickbusch, I., & Silberschmidt, G. (2007). *Global health governance: Opportunities and challenges*. Berlin: Springer.
- Laqueur, W. (2003). *The new terrorism: Fanaticism and the arms of mass destruction*. New York: Oxford University Press.
- Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. Cambridge: Cambridge University Press.

- Morgenthau, H. J. (1948). *Politics among nations: The struggle for power and peace*. New York: Alfred A. Knopf.
- Nye, J. S. (2009). *Understanding international conflicts: An introduction to theory and history* (7th ed.). London: Pearson.
- Nye, J. S. (2011). *The future of power*. New York: Public Affairs.
- UNDP (United Nations Development Programme). (1994). *Human development report 1994*. New York: Oxford University Press.
- United Nations. (1999). *Report of the United Nations experts group on terrorism*. New York: United Nations.
- UNODC (United Nations Office on Drugs and Crime). (2010). *The globalization of crime: A transnational organized crime threat assessment*. Vienna: United Nations.
- Walker, C. (2010). *Non-traditional threats and global security*. London: Routledge.
- Waltz, K. N. (1979). *Theory of international politics*. Boston: Addison-Wesley.

2- Journal Articles

- Barnett, J., & Adger, W. N. (2007). Climate change, human security and violent conflict. *Political Geography, Amsterdam: Elsevier*, 26(6), 614–615.
- Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security, Boston: Harvard University*, 38(2), 7–40.
- Kickbusch, I., & Silberschmidt, G. (2007). Global health diplomacy: The need for new perspectives, strategic approaches and skills in global health. *Bulletin of the World Health Organization, Geneve: the World Health Organization*, 85(3), 201–205.
- Krahmann, E. (2003). Conceptualizing security governance. *Cooperation and Conflict, Thousand Oaks: Sage Publications*, 38(1), 73–94.
- Walt, S. M. (1991). The renaissance of security studies. *International Studies Quarterly, New York: Oxford University Press*, 35(2), 211–239.
- Wolfers, A. (1952). National security. *Political Science Quarterly, New York: The Academy of Political Science*, 67(4), 481–502.