MARITIME SECURITY FORUM

GLOBAL SECURITY IN THE 21ST CENTURY

Strategic Transformations, Critical Infrastructures and the New Architecture of the International Order

MARITIME SECURITY | ENERGY SECURITY | CYBER SECURITY | TECHNOLOGICAL ADVANCEMENT | GLOBAL GOVERNANCE | STRATEGIC RESILIENCE

STUDY

BUCHAREST
JUNE 2026

CONTENTS

GLOBAL SECURITY IN THE 21ST CENTURY
Strategic transformations, critical infrastructure and the new architecture of the international order

AUTHORS: Admiral (ret.) PhD. Aurel POPA, Rear Admiral (ret.) PhD. Sorin Learschi

FOREWORD

In recent decades, the international security environment has undergone one of the most profound transformations of the post-war period. Conventional armed conflicts now coexist with hybrid threats, cyber-attacks, technological competition, pressures on critical infrastructure, energy vulnerabilities and disruptions to global supply chains. In this context, security can no longer be understood solely in terms of the military balance between states, but must be analysed as the result of the interaction between numerous political, economic, legal, technological and social systems, which are in a state of constant interdependence.

This study is the result of research aimed at understanding the mechanisms through which seemingly distinct events – regional conflicts, maritime incidents, energy crises, attacks on critical infrastructure or the rapid development of artificial intelligence – come to influence the functioning of the entire international system. The proposed analysis aims to move beyond sectoral approaches and offer an integrated perspective on global security, in which the geopolitical, legal, economic, energy, technological and societal dimensions are treated as elements of a single system.

The preparation of this study was also motivated by the need to develop analytical tools capable of keeping pace with the rapid pace of strategic change. In a world where decisions must be taken swiftly, based on a considerable volume of information, a mere description of events is no longer sufficient. It is essential to identify trends, assess interdependencies and anticipate likely developments. From this perspective, this paper proposes not only an analysis of the security environment, but also a series of conceptual and methodological tools designed for integrated risk assessment, including *the Global Escalation Index*, *Critical Infrastructure Monitoring*, *the Global Security Report* and the *Strategic Gravity* model.

Particular attention is paid to the legal dimension of global security. In an era characterised by rapid technological and geopolitical transformations, international law continues to represent one of the cornerstones of the international order. At the same time, new realities necessitate the development of interpretations and mechanisms capable of addressing the challenges posed by hybrid conflicts, cyber operations, the protection of critical infrastructure and the use of artificial intelligence. This paper argues that the effectiveness of legal norms depends increasingly on their ability to keep pace with developments in the strategic environment and to strengthen the resilience of the international system.

This study does not aim to provide definitive answers or to construct an exhaustive model for interpreting global security. The complexity and dynamism of the phenomena analysed call for caution and an openness to interdisciplinary perspectives. At the same time, the study is based on the conviction that understanding contemporary security requires transcending traditional disciplinary boundaries and fostering an ongoing dialogue between law, international relations, strategic studies, economics, technology and the social sciences.

The authors hope that this work will serve as a useful tool for researchers, academics and students, as well as for practitioners involved in public policy-making, strategic analysis and the management of national and international security. At the same time, the study aims to contribute to strengthening the culture of analysis in the field of security and to promoting an approach based on cooperation, prevention and resilience.

In a world where uncertainty seems to be becoming the norm, and change is the rule rather than the exception, global security can no longer be viewed merely as an objective of states, but as a shared responsibility of the entire international community. Understanding the interdependencies

that define the contemporary world order and developing mechanisms capable of preventing the escalation of crises is, perhaps, one of the most important challenges facing our generation.

If this work succeeds in stimulating critical reflection, interdisciplinary dialogue and the development of new avenues of research on global security, then its fundamental aim can be considered achieved.

THE AUTHORS

ABSTRACT

*The assessment carried out in this paper indicates that the international system is undergoing a period characterised by **high strategic instability**, driven by the simultaneous overlap of multiple conflict hotspots and the intensification of geopolitical competition between the major powers. Unlike in previous periods, current threats are no longer exclusively military in nature, but arise from the interplay between armed conflicts, vulnerabilities in critical infrastructure, economic pressures, technological competition and the use of hybrid instruments of influence. The war in Ukraine continues to be the main source of instability for the Euro-Atlantic area, affecting security in the nd Black Seas, European energy policy and relations between the Russian Federation and NATO member states. At the same time, the Middle East remains one of the world's most volatile regions, where the security of maritime routes and the protection of energy infrastructure directly influence the stability of global markets and the freedom of international trade. In the Indo-Pacific region, strategic competition between the United States and the People's Republic of China continues to manifest itself through the strengthening of military presence, the development of naval capabilities and the intensification of disputes over control of maritime spaces and critical infrastructure. At the same time, the Sahel, the Horn of Africa and the Korean Peninsula demonstrate that regional instability and threats posed by non-state actors continue to present significant challenges to international security. A defining feature of the current strategic environment is the transformation of critical infrastructure into targets of military and geopolitical interest. Energy networks, ports, oil and gas pipelines, submarine cables, satellites and digital systems are becoming essential components of state resilience and collective security. At the same time, cyber-attacks, information operations and the use of artificial intelligence in the military sphere are altering the nature of conflicts and increasing the complexity of the risk assessment process. The analysis concludes that global security is characterised by a high probability of regional incidents with international implications, whilst there are currently no indications suggesting the outbreak of a global military conflict. However, the simultaneous accumulation of multiple crises and their interdependence necessitate the strengthening of international cooperation mechanisms, the development of the resilience of critical infrastructure, and the adoption of integrated tools for strategic analysis and early warning.*

CHAPTER I

1 The Transformation of the International Security Environment

International security is undergoing one of the most profound periods of transformation in contemporary history. Whilst in the first two decades following the end of the Cold War the strategic environment appeared geared towards strengthening multilateral cooperation and expanding the rules-based international order, developments in recent years demonstrate the emergence of a far more complex and less predictable landscape. The resurgence of competition between the major powers, the proliferation of regional conflicts, the rapid development of disruptive technologies and the increasing vulnerability of critical infrastructure have fundamentally altered the nature of threats and the ways in which states define and protect their strategic interests.

The current transformations cannot be explained by the existence of a single conflict or a single international crisis. They are the result of an accumulation of political, economic, technological and military developments that have altered the global balance of power and reduced the capacity of international institutions to manage the new challenges effectively. In this context, security can no longer be analysed solely through the prism of military relations between states, but must be understood as a complex system of interdependencies in which the political, economic, energy, technological, cyber and legal dimensions influence one another.

The war in Ukraine, persistent tensions in the Middle East, strategic competition in the Indo-Pacific, the intensification of attacks on critical infrastructure and the widespread use of autonomous technologies demonstrate that the international environment is characterised by a high degree of volatility and a significant reduction in the ability to anticipate developments. Consequently, the analysis of global security must move beyond traditional approaches and simultaneously integrate the military, economic, energy, technological and societal dimensions of risk.

1.1. From a unipolar order to multipolar competition

The period immediately following the end of the Cold War was dominated by the perception of a unipolar international order, within which the United States enjoyed unprecedented economic, military and technological superiority. The expansion of international organisations, trade liberalisation and the development of economic cooperation created the impression that global interdependence would reduce the likelihood of major conflicts and strengthen international stability.

However, this paradigm began to shift gradually with the rise of the People's Republic of China, the accelerated modernisation of the Russian Federation and the emergence of regional powers capable of influencing the strategic balance within their own spheres of interest. India, Turkey, Saudi Arabia, Brazil and other states have begun to pursue more autonomous foreign policies, whilst organisations such as BRICS and the Shanghai Cooperation Organisation have gained increasing relevance within the architecture of international relations.

The current multipolarity does not imply the existence of a stable balance between the main actors, but rather a constant competition for political, economic, technological and military influence. Unlike the bipolarity characteristic of the Cold War, the current system is marked by the flexibility of alliances and the existence of variable partnerships, forged on the basis of specific interests and time-limited strategic objectives. This configuration leads to increased uncertainty and complicates the process of anticipating geopolitical developments.

1.2. The erosion of the rules-based international order

One of the most significant changes in the contemporary strategic environment is the decline in the effectiveness of traditional mechanisms of international governance. The Charter of the United Nations and the other fundamental instruments of international law continue to provide the legal framework for relations between states, but their application is increasingly influenced by geopolitical rivalries and the difficulty of reaching a consensus amongst the major powers.

Repeated deadlocks within the United Nations Security Council illustrate the limitations of the current system in managing major conflicts. At the same time, the development of under-regulated areas, such as cyber operations, the use of artificial intelligence in the military, autonomous weapon systems and activities carried out in outer space, is creating unprecedented legal challenges.

This development should not be interpreted as a diminishing of the importance of international law, but rather as a demonstration of the need for it to adapt to new technological and geopolitical realities. The ability of international norms to respond to these challenges will be one of the decisive factors for the stability of the international system in the coming decades.

1.3. The changing nature of conflicts

Contemporary conflicts differ significantly from those that characterised the 20th century. Whereas in the past conventional military operations were the primary means of achieving strategic objectives, today they are complemented by actions carried out simultaneously in the informational, cyber, economic and technological spheres.

The war in Ukraine demonstrates that the use of drones, autonomous systems, electronic warfare and attacks on critical infrastructure can decisively influence the conduct of military operations. Similarly, developments in the Middle East highlight the importance of controlling maritime routes and energy infrastructure, and of using non-state actors as instruments of strategic influence.

Consequently, modern conflict must be understood as a multidimensional competition, in which success depends not solely on military superiority, but also on states' ability to protect critical infrastructure, ensure the continuity of economic functioning, and manage information and technology flows.

1.4. Critical infrastructure and strategic resilience

One of the most significant changes of the past decade has been the transformation of critical infrastructure into priority strategic targets. Energy networks, seaports, oil and gas pipelines, submarine cables, communications systems and data centres are now indispensable components of national security and the functioning of the global economy.

Attacks on these infrastructures have consequences that go far beyond the military sphere. They affect the continuity of public services, the stability of energy markets, the functioning of global supply chains and the ability of states to respond effectively to crisis situations. From this perspective, the protection of critical infrastructure is no longer solely a technical responsibility, but an essential component of security and defence policies.

The concept of strategic resilience thus takes on unprecedented importance. A state's ability to prevent, absorb and overcome the effects of attacks on critical infrastructure becomes just as important as its conventional military capability. At the same time, resilience requires strengthening cooperation between public authorities, the private sector and international organisations, as most critical infrastructure operates within transnational and interdependent networks.

The transformations analysed in this chapter demonstrate that the international security environment is undergoing a period of profound redefinition, in which the boundaries between military, economic, energy and technological security are becoming increasingly difficult to distinguish. The resurgence of competition between major powers, the development of disruptive technologies, the vulnerability of critical infrastructure and the proliferation of regional conflicts are shaping an international system characterised by a high degree of complexity and uncertainty.

In this context, strategic analysis must move beyond traditional approaches and incorporate multidisciplinary perspectives capable of explaining the interdependencies between the various domains of security. Only through such an approach is it possible to understand the mechanisms

driving current instability and to underpin public policies aimed at conflict prevention, strengthening resilience and adapting the international security architecture to the challenges of the 21st century.

CHAPTER II

2. The main theatres of conflict and their implications for global security

Regional conflicts are today the main factor transforming the international security environment. Unlike during the Cold War, when the rivalry between the two blocs dominated almost all geopolitical developments, the current strategic landscape is characterised by the simultaneous existence of several hotspots of instability, each with its own causes, actors and implications. However, these conflicts do not unfold in isolation. They are linked by economic, energy, technological and politico-military interests, such that developments in one region have direct or indirect effects on other geographical areas.

The conflict in Ukraine is affecting European energy security and stability in the Black Sea; tensions in the Middle East are impacting global energy markets and maritime trade; and competition in the Indo-Pacific is driving profound changes in defence policies and the global strategic balance. At the same time, instability in the Sahel, the Horn of Africa and the Korean Peninsula is exacerbating global risks through its effects on migration, terrorism, organised crime and economic security.

Understanding these conflicts requires an integrated approach, capable of going beyond a purely military analysis and highlighting the interrelationships between the operational, economic, legal and geopolitical dimensions.

Table 1. Major active conflicts and their characteristics (Situation in 2026)

Conflict / Region	Main actors	Nature of the conflict	Dominant dimensions	Estimated risk level	Overall strategic impact
Ukraine	Ukraine – Russian Federation	Conventional international armed conflict with hybrid elements	Military, energy, cyber, economic, maritime	**Very high**	Is reshaping European security, influencing energy markets, food security and NATO's architecture.
Middle East	Israel, Iran, regional armed groups, the US and partners	Regional confrontation with direct and indirect incidents	Military, energy, maritime	**Very high**	Affects the Strait of Hormuz, the Red Sea, oil prices and regional stability.
Red Sea / Bab el-Mandeb	The Houthi group, international naval coalitions	Maritime and commercial transport threats	Maritime, economic, energy	**High**	Increases global transport costs and disrupts supply chains.
South China Sea	China, the Philippines, Vietnam, Malaysia, the US	Strategic competition and maritime disputes	Naval, geopolitical, economic	**High**	It affects freedom of navigation and global trade in the Indo-Pacific.

Taiwan	People's Republic of China – Taiwan	Strategic crisis with military potential	Military, technological, economic	**High**	Major impact on the global semiconductor industry and on the US–China strategic balance.
Korean Peninsula	North Korea, South Korea, the US, Japan	Strategic confrontation and nuclear deterrence	Military, nuclear	**Moderate–High**	Maintains instability in North-East Asia and requires a permanent military presence.
Sahel	Armed groups, African states, regional organisations	Asymmetric conflict and political instability	Terrorism, human security	**High**	Contributes to migration, cross-border crime and regional insecurity.
Horn of Africa	Sudan, South Sudan, Somalia, armed groups	Internal and regional conflicts	Humanitarian, military	**High**	Causes humanitarian crises and affects the stability of East Africa.
South Caucasus	Armenia, Azerbaijan	Territorial disputes and regional security	Military, political	**Moderate**	Affects the energy corridors between the Caspian Sea and Europe.
Global cyberspace	States, state-sponsored groups, organised crime	Ongoing conflict below the threshold of war	Cyber, information	**High**	Affects critical infrastructure, the digital economy and institutional trust.

2.2. Ukraine – a testing ground for the transformation of modern warfare

The war launched by the Russian Federation against Ukraine represents the most significant conventional conflict to have taken place on the European continent since the Second World War. Beyond its military dimension, the conflict serves as a testing ground for the transformation of modern warfare, in which emerging technologies, information warfare, economic sanctions and attacks on critical infrastructure are used simultaneously to achieve strategic objectives.

One of the most significant features of the conflict is the expansion of the operational theatre beyond the front line. The use of long-range drones enables Ukraine to strike energy and industrial infrastructure located hundreds of kilometres inside the Russian Federation, whilst Russia continues its attacks on Ukrainian energy infrastructure, urban centres and logistical facilities. Under these circumstances, the traditional distinction between the front line and the strategic depth is becoming increasingly irrelevant.

The conflict also demonstrates the importance of information and technology in the conduct of military operations. Commercial satellite imagery, satellite communications systems, artificial intelligence used for battlefield analysis and autonomous drones are fundamentally changing the process of planning and executing operations. Technological superiority is thus becoming a force multiplier comparable to numerical superiority.

The economic dimension of war is equally important. Attacks on refineries, oil terminals and energy infrastructure aim to diminish the adversary's ability to sustain the military effort in the long term. At the same time, economic sanctions and measures restricting technology exports are transforming the economy into a veritable theatre of strategic confrontation.

The conflict is also having a profound impact on the European security architecture. NATO's expansion, the strengthening of its eastern flank, increased defence budgets and the development of the European arms industry are direct consequences of the war. At the same time, the Black Sea region is acquiring unprecedented strategic importance, becoming the point where European security, energy security and freedom of navigation intersect.

2.3. The Middle East – the competition for control of the global energy sector

The Middle East remains one of the world's most volatile regions, primarily due to the interplay of historical rivalries, geopolitical competition and its importance for global energy security. Unlike other theatres of conflict, in this region the military dimension is inseparable from the economic one, as control of energy infrastructure and key maritime routes directly influences the stability of world markets.

Recent events demonstrate that the Strait of Hormuz, Bab el-Mandeb and the Suez Canal are veritable focal points of global security. Any disruption to navigation through these areas has immediate effects on oil prices, maritime transport costs and the functioning of international supply chains.

At the same time, the rivalry between Iran and Israel, the competition between Iran and the Arab Gulf states, and the US military presence all contribute to maintaining a fragile strategic balance. Non-state actors, in particular Hezbollah and the Houthi movement, complete this complex picture, demonstrating that regional influence can also be exerted through organisations that do not formally belong to the state apparatus.

A defining feature of the conflicts in the Middle East is the use of energy infrastructure as a tool for strategic pressure. Refineries, oil terminals, pipelines and export facilities are targets of particular military and economic value, and their protection requires the mobilisation of considerable naval and air resources.

2.4. The Indo-Pacific – the centre of 21st-century strategic competition

Whilst Europe is currently the main theatre of conventional military confrontation, the Indo-Pacific region is the focus of the most significant long-term strategic competition. Economic and military developments in this area are likely to shape the international system for decades to come.

China's growing economic and naval power, the strengthening of partnerships between the United States and its regional allies, and disputes over control of the South China Sea and the status of Taiwan are bringing about a profound transformation of the regional strategic balance.

Unlike in Europe, where military confrontation is already a reality, competition in the Indo-Pacific is primarily played out through demonstrations of force, military exercises, the development of port infrastructure, technological investment and the strengthening of alliances. However, the high density of naval and air presence in the region means that the likelihood of unintended incidents is increasing.

Taiwan occupies a central position in this competition. Beyond its political significance, the island is one of the world's most important centres for the production of advanced semiconductors, which gives it essential strategic value for the global economy.

2.5. Africa – regional insecurity and global implications

Over the past two decades, the African continent has become a space where internal security issues, geopolitical competition and global economic interests intersect. The Sahel region is the most telling example of this development.

Political instability, coups d'état, the activities of armed groups and a diminished international presence have created the conditions for an extremely fragile security environment. At the same time, competition for access to strategic natural resources and the expansion of influence by external actors are amplifying the complexity of the regional situation.

The impact of these developments extends beyond Africa. Migration, cross-border crime, terrorism and the disruption of trade routes directly affect European security and international economic interests.

An analysis of the main theatres of conflict demonstrates that global security is the result of the interplay between multiple regional crises, each with its own particularities, but all influencing the functioning of the international system. Ukraine highlights the transformation of conventional warfare through the integration of emerging technologies and the economic dimension; the Middle East confirms the decisive role of energy and maritime security; and the Indo-Pacific illustrates the strategic competition over the configuration of the future world order.

These conflicts should not be analysed in isolation, but as elements of a strategic environment characterised by interdependence and volatility, in which developments in one region can have systemic effects on global security, the economy and stability. From this perspective, the following chapter will examine the role of maritime security as a central element of the contemporary international order and as a determining factor for the functioning of global trade and the world economy.

Table 2. Indicators used in the assessment of global security

Area of assessment	Strategic indicator	Elements analysed	Level of assessment	Impact on global security
Military security	Intensity of armed conflicts	Number of active conflicts, military operations, mobilisation of forces, use of strategic weapons	Very low – Very high	Determines the overall level of instability and the risk of regional or global escalation.
Geopolitics	Strategic competition between major powers	Relations between major powers, alliances, sanctions, diplomatic tensions	Very low – Very high	Influences the international security architecture and regional stability.
Energy security	Stability of energy markets	Oil and gas production and transport, energy infrastructure, price volatility	Very low – Very high	It affects the global economy, energy security and the resilience of states.
Maritime security	Freedom of navigation and the protection of maritime routes	The situation in straits, naval incidents, the security of ports and trade corridors	Very low – Very high	It affects world trade and global supply chains.
Critical infrastructure	Level of vulnerability of critical infrastructure	Energy networks, ports, pipelines, submarine cables, logistics centres	Very low – Very high	Determines the continuity of the economy and essential services.
Cyber security	Severity of cyber threats	Attacks on digital infrastructure, malware, ransomware, state-sponsored cyber operations	Very low – Very high	May simultaneously affect the economy, public administration and critical infrastructure.
Economic security	Economic resilience	Inflation, international trade, economic sanctions, supply chains	Very low – Very high	It affects financial stability and economic development.
Technological security	Level of development of critical technologies	Artificial intelligence, semiconductors, quantum communications, autonomous systems	Very low – Very high	Determines states' strategic advantage and competitiveness.
Information security	Integrity of the information space	Disinformation, information manipulation, external influence, information warfare	Very low – Very high	It affects public trust and institutional stability.

Climate and humanitarian security	Climate and humanitarian vulnerabilities	Natural disasters, migration, food insecurity and access to resources	Very low – Very high	May lead to regional instability and put pressure on international security.
International governance	Capacity of multilateral institutions	The functioning of the UN, NATO, the EU, the OSCE, the G7, the G20 and international cooperation	Very low – Very high	It affects the international community's ability to prevent and manage crises.
Strategic resilience	Ability to adapt to crises	Continuity of essential services, infrastructure redundancy, recovery capacity	Very low – Very high	Represents the composite indicator of the stability of the international system.

CHAPTER III

Maritime security – the foundation of global economic and strategic stability

3.1. The Sea – the Central Arena of Global Security

Maritime security is one of the fundamental dimensions of contemporary international security. Although armed conflicts are often analysed through the prism of land-based operations, the strategic reality demonstrates that the seas and oceans constitute the invisible infrastructure that underpins the functioning of the global economy. Approximately ninety per cent of international trade is conducted by sea, and the main flows of energy, raw materials and manufactured goods depend on freedom of navigation and the security of the main maritime corridors.

However, the importance of the maritime domain extends beyond the commercial sphere. The seas are simultaneously areas for the projection of military power, arenas of competition for natural resources, global communications infrastructure and areas essential to energy security. For this reason, control of maritime routes and the protection of associated infrastructure have become priority objectives for the major powers and for international security organisations.

Technological developments over the last two decades have profoundly altered the nature of maritime security. The development of naval drones, autonomous surveillance systems, commercial satellites and real-time monitoring technologies has increased states' capacity to control maritime space, but has also heightened the vulnerability of critical infrastructure in the marine environment.

3.2. Maritime straits – strategic hubs of the global economy

The global trading system depends on the existence of mandatory transit points, known in the specialist literature as *maritime chokepoints*. These areas handle very large volumes of commercial and energy traffic, such that any disruption to their operation has disproportionate economic consequences.

Of these, the Strait of Hormuz occupies a central position. Approximately one-fifth of global oil consumption passes through this route every day, which means that any incident in the area has an immediate impact on international markets. Recent events demonstrate that attacks on oil tankers, the use of maritime drones and disputes over control of shipping lanes can simultaneously influence energy prices, transport costs and global economic stability.

The Suez Canal and the Bab el-Mandeb Strait form a second key strategic corridor. They connect the Indian Ocean with the Mediterranean Sea and enable the rapid transport of goods between Asia and Europe. Attacks on commercial vessels in the Red Sea have shown that the temporary blockage of these routes forces shipping operators to use alternative routes via the Cape

of Good Hope, which lengthens transit times, increases fuel consumption and drives up global logistics costs.

The Bosphorus and the Dardanelles continue to serve as gateways to the Black Sea and, by extension, to Ukrainian, Romanian, Bulgarian, Georgian and Russian ports. Since the outbreak of the war in Ukraine, these straits have acquired additional strategic importance, as they are directly linked to the security of agricultural exports, freedom of navigation and the regional military balance.

In the Indo-Pacific region, the Strait of Malacca is one of the world's most important trade routes. It facilitates energy flows between the Middle East and Asian economies and is a key element in the strategic competition between China and the United States. The vulnerability of this route explains the massive investments in the development of alternative corridors and the strengthening of naval presence in the region.

Table 3. Main maritime routes and their strategic importance

Maritime route	Economic importance	Energy importance	Vulnerability	Global impact
The Strait of Hormuz	Very high	Very high	High	Very high
Bab el-Mandeb	High	High	High	High
Suez Canal	Very high	High	Moderate	Very high
The Bosphorus and the Dardanelles	High	Moderate	Moderate	High
Strait of Malacca	Very high	High	Moderate	Very high
Panama Canal	High	Low	Low	Moderate

3.3. The Black Sea – a strategic European region

Since 2022, the Black Sea has become one of the world's most important maritime theatres. The conflict between the Russian Federation and Ukraine has profoundly altered the regional security architecture and demonstrated that the maritime domain can have a decisive influence on the course of a land-based conflict.

Naval operations in the region have highlighted the importance of maritime drones, electronic warfare and long-range strike systems. The destruction or neutralisation of Russian military vessels through the use of naval drones represented one of the most significant tactical innovations of the conflict and has altered the way in which the balance between traditional naval power and new autonomous technologies is assessed.

At the same time, the operation of the maritime corridor for Ukrainian agricultural exports demonstrates that global food security is directly dependent on the stability of the Black Sea. The blockading of ports or damage to logistical infrastructure affects not only the regional economy but also the supply of agricultural products to countries in Africa, the Middle East and Asia.

For NATO member states on the eastern flank, including Romania and Bulgaria, Black Sea security goes beyond the military dimension and becomes a central element of energy, economic and trade security.

3.4. Critical maritime infrastructure

The contemporary maritime domain is no longer defined solely by trade routes and military fleets. Today, the seabed of the seas and oceans is home to critical infrastructure of exceptional strategic importance.

Submarine cables carry over ninety-five per cent of global data traffic, connecting financial systems, government networks and commercial communications. Subsea pipelines transport oil and natural gas to major consumer markets, whilst offshore infrastructure contributes significantly to global energy production.

Incidents in recent years in the Baltic Sea and other maritime regions have demonstrated that these infrastructures are vulnerable to both accidents and deliberate acts of sabotage. Protecting them requires the development of advanced underwater surveillance capabilities, international cooperation and the rapid exchange of information.

3.5. The maritime economy and global security

The functioning of the global economy depends to a decisive extent on the stability of the maritime domain. Shipping costs directly influence the competitiveness of economies, inflation rates and the functioning of global supply chains.

Any disruption to major trade routes has a knock-on effect on the prices of raw materials, energy and consumer goods. Temporary blockages of the Suez Canal, attacks on oil tankers in the Persian Gulf and restrictions imposed in the Black Sea have demonstrated that maritime security is inseparable from economic security.

At the same time, competition for control of commercial ports and logistics infrastructure is taking on an increasingly pronounced geopolitical dimension. Investments made by major powers in the development of ports, container terminals and transport infrastructure reflect the economic and strategic importance of this sector.

An analysis of maritime security demonstrates that the maritime domain is one of the fundamental pillars of the contemporary international order. The stability of trade routes, the protection of subsea infrastructure and freedom of navigation are essential to the functioning of the global economy and directly influence energy and food security.

Recent developments in the Black Sea, the Strait of Hormuz, the Red Sea and the Indo-Pacific confirm that the seas and oceans are no longer merely transit routes, but veritable theatres of strategic competition. In this context, strengthening maritime cooperation, developing surveillance capabilities and protecting critical underwater infrastructure will be among the main priorities of security policies in the coming decades.

CHAPTER IV

4. Critical infrastructure – the new centre of gravity in global security

4.1. The shift in the security paradigm

Over the past two decades, the security of critical infrastructure has moved from the realm of sectoral policies to the centre of national and international security strategies. Whilst in the past its protection was associated almost exclusively with the prevention of technological accidents or natural disasters, recent developments demonstrate that critical infrastructure is now a priority target in geopolitical competition and modern conflicts.

This transformation reflects a profound shift in the nature of power within contemporary society. A state’s ability to protect its population and sustain its institutional functioning no longer depends exclusively on military force, but on the continued operation of complex technical systems

that enable energy supply, digital communications, transport, water supply, financial services and industrial operations. In a globalised economy, the disruption of a single logistics or energy hub can have a knock-on effect on several states and regions.

In this regard, critical infrastructure must be understood as interdependent systems, within which the vulnerability of a single component can affect the stability of the whole.

4.2. The interdependence of critical infrastructure

One of the defining characteristics of contemporary infrastructure is its constant interconnection. Energy systems rely on digital networks for monitoring and control, communications depend on the electricity supply, and modern transport operates via integrated IT platforms.

Table 4. Indicators used in critical infrastructure monitoring

Infrastructure category	Strategic indicator	Parameters monitored	Potential impact	Risk level
Energy	Continuity of production and distribution	Power stations, refineries, LNG terminals, pipelines, electricity grids	Impact on energy and economic security	Low – Very high
Maritime transport	Operation of trade routes	Ports, straits, maritime channels, commercial traffic	Disruption to global trade	Low – Very high
Communications	Stability of global communications	Submarine cables, satellites, internet backbone	Disruption to global communications	Low – Very high
Land transport	Continuity of logistics corridors	Railways, motorways, strategic bridges	Disruption to logistics chains	Low – Very high
Financial sector	Continuity of financial services	Data centres, stock exchanges, payment systems	Economic instability	Low – Very high
Water and health	Essential services	Water supply, hospitals, laboratories	Humanitarian crisis	Low – Very high
Digital	IT infrastructure	Cloud, data centres, 5G networks, AI	Cyber vulnerability	Low – Very high

Table 5. Classification of critical infrastructure

Level	Type of infrastructure	Examples	Impact in the event of unavailability
Level I	Global critical infrastructure	Internet backbone, GPS, submarine cables, SWIFT	Immediate global impact
Level II	Strategic infrastructure	Pipelines, LNG terminals, major ports	Continental impact
Level III	Regional infrastructure	Electricity grids, airports, railway hubs	Regional impact
Level IV	Local infrastructure	Energy distribution, water, healthcare	Local impact

This interdependence generates considerable economic benefits, but it also amplifies the risk of cascading effects. A disruption to the energy supply can simultaneously affect communications, transport, banking systems and medical services, whilst a cyber attack on digital infrastructure can cause disruption comparable to that caused by a conventional military attack.

This phenomenon is known in the specialist literature as **the cascade effect**, and represents one of the most significant challenges for modern security policies.

4.3. Energy – fundamental critical infrastructure

Energy is the central element of all critical infrastructure. The functioning of the modern economy, transport, communications, industry and public services depends directly on the availability of stable and accessible energy resources.

The conflict in Ukraine has demonstrated that energy infrastructure can simultaneously become both a military target and a strategic instrument of influence. Attacks on power stations, refineries, fuel depots and energy transmission lines have aimed not only to diminish the adversary's economic capacity, but also to undermine public morale and limit the ability of institutions to function under normal conditions.

In the Middle East, energy security is influenced by the protection of oil infrastructure and the maritime routes through which resources are transported to global markets. Attacks on oil terminals, pipelines and offshore installations demonstrate that energy infrastructure is one of the most sensitive components of global security.

4.4. The digital revolution and information infrastructure

The digitalisation of the global economy has led to the emergence of a new category of critical infrastructure: information infrastructure. Data centres, communications networks, cloud computing systems, satellites and submarine cables carry huge volumes of information every day, enabling the functioning of the economy, public administration and the international financial system.

In this context, cyber-attacks are no longer aimed solely at stealing information, but can directly affect the functioning of essential services. Disrupting communications, paralysing banking systems, interfering with air traffic control or compromising industrial systems are scenarios with major strategic implications.

Furthermore, the integration of artificial intelligence into the management of critical infrastructure generates both significant opportunities for increased efficiency and new vulnerabilities associated with the manipulation of algorithms or the compromise of autonomous systems.

4.5. The underwater realm – the invisible infrastructure of globalisation

One of the least visible yet most important components of global infrastructure is the systems located on the seabed and ocean floor. Submarine communications cables and pipelines carry information and energy resources that are indispensable to the functioning of the global economy.

Their strategic importance has become evident following incidents in the Baltic Sea and other maritime regions, where damage to submarine pipelines and cables has demonstrated just how vulnerable this infrastructure is and how difficult it is to protect.

Currently, states are developing specialised underwater surveillance systems, autonomous vehicles and smart sensors capable of detecting suspicious activity near subsea infrastructure. This process marks the emergence of a new arena of strategic competition, situated beneath the surface of the seas.

4.6. Critical infrastructure and geopolitical competition

Control over critical infrastructure is today one of the main ways of exerting geopolitical influence. Investment in ports, energy terminals, digital networks and logistics infrastructure is not

aimed solely at securing economic advantages, but also at consolidating political and strategic influence over entire regions.

Initiatives such as the development of transcontinental economic corridors, the expansion of next-generation communications networks, and investment in port infrastructure demonstrate that infrastructure is becoming a tool of foreign policy and of competition between the major powers.

This trend is evident in Europe, Asia, Africa and the Middle East, where infrastructure projects are analysed not only from the perspective of economic viability, but also in terms of their implications for national and regional security.

4.7. Resilience of critical infrastructure

Against a backdrop of multiplying threats, the concept of resilience is taking on unprecedented strategic importance. The resilience of critical infrastructure does not entail the elimination of all vulnerabilities – an impossible objective in a complex and interdependent system – but rather the development of the capacity to prevent, adapt to and recover rapidly from incidents.

This approach requires investment in system redundancy, the diversification of supply sources, the development of effective mechanisms for cooperation between public authorities and private operators, and the use of advanced technologies for the continuous monitoring of risks.

Equally, resilience involves developing an organisational culture geared towards anticipating threats and integrating risk assessment into all stages of the decision-making process.

Critical infrastructure has become one of the main focal points of contemporary international security. Energy, communications, transport, digital systems and subsea infrastructure are indispensable to the functioning of modern societies, and their vulnerability directly affects the economic stability, defence capability and institutional resilience of states.

Recent developments demonstrate that protecting these infrastructures can no longer be treated as a purely technical or administrative issue. It is a strategic responsibility, situated at the intersection of national security, international law, regional cooperation and technological development. Looking ahead to the coming years, strengthening the resilience of critical infrastructure will be one of the fundamental pillars of global security and one of the key prerequisites for maintaining international economic and political stability.

CHAPTER V

5. Energy security – a key factor in international stability

5.1. Energy and the new architecture of global power

Energy is one of the fundamental components of contemporary international security and one of the main factors influencing the balance of power between states. Whilst in the past energy resources were analysed predominantly from the perspective of economic development, developments over recent decades demonstrate that they now constitute a strategic instrument capable of influencing foreign policy, regional stability and even the conduct of armed conflicts.

The transformations that have taken place since the beginning of the 21st century have profoundly altered the relationship between energy and security. Rising global demand, competition for access to resources, the diversification of production technologies and the intensification of geopolitical rivalries have led to the emergence of a new concept of energy security, which goes beyond the economic dimension to include military, diplomatic, legal and technological aspects.

In this context, control over energy sources, transport infrastructure and key maritime routes has become a key element of global strategic competition.

Table 6. The world's main energy corridors

Energy corridor	Resource type	Connected regions	Vulnerability	Strategic importance
Persian Gulf – Hormuz	Oil and LNG	Middle East – Asia – Europe	High	Very high
Caspian Sea – Europe	Oil and gas	Caucasus – EU	Moderate	High
Eastern Mediterranean	Natural gas	Israel – Egypt – Europe	Moderate	High
North Sea	Oil and gas	Western Europe	Low	High
USA – Atlantic	LNG	USA – Europe	Low	High
Australia – Asia	LNG	Australia – Asia-Pacific	Low	High

5.2. Oil and natural gas in geopolitical competition

Oil and natural gas continue to be the main energy resources of the global economy, and their geographical distribution directly influences the shape of international relations.

The Middle East holds some of the world's most significant hydrocarbon reserves, which explains the major powers' constant interest in the region's stability. At the same time, the Russian Federation uses energy exports as a foreign policy tool, whilst the United States has strengthened its international position by developing unconventional hydrocarbon production and expanding exports of liquefied natural gas.

The war in Ukraine has accelerated the process of reconfiguring energy markets. The reduction in European imports from the Russian Federation has led to the diversification of supply sources, the development of liquefied natural gas infrastructure and the strengthening of energy relations with countries in the Middle East, Africa and North America.

This development demonstrates that energy security can no longer be analysed solely in terms of production volumes, but must be assessed in terms of the resilience of supply systems and the ability of states to rapidly adapt trade flows in crisis situations.

5.3. Energy infrastructure – a strategic objective

The conflict in Ukraine and tensions in the Middle East have shown that energy infrastructure is one of the main targets of contemporary conflicts.

Refineries, oil terminals, pipelines, compressor stations, power stations and energy transmission networks are considered strategic targets because damage to them has simultaneous effects on the economy, industry and military capability.

Attacks on energy infrastructure aim to reduce the resources available to sustain the war effort, as well as to exert psychological and economic pressure on the population and public authorities. At the same time, protecting this infrastructure requires the mobilisation of significant military resources and the development of integrated surveillance and defence systems.

Experience in recent years confirms that energy infrastructure must be treated as an essential component of national security and not merely as an element of economic policy.

Table 7. Vulnerabilities of energy infrastructure

Threat	Probability	Impact	Areas affected	Mitigation measures
Military attack	Moderate	Very high	Energy, economy	Air defence
Sabotage	High	High	Pipelines, refineries	Round-the-clock surveillance
Cyber attack	Very high	High	Smart grids	Cyber security
Natural disasters	Moderate	High	Production and transport	Redundancy
Technical faults	Moderate	Moderate	Distribution	Predictive maintenance
Political instability	Moderate	High	Export and transit	Route diversification

5.4. The energy transition and strategic implications

The global transition towards low-carbon energy sources is gradually reshaping the architecture of energy security. The development of renewable energy, the electrification of transport and the expansion of hydrogen use are reducing dependence on fossil fuels, but are creating new vulnerabilities.

The production of green technologies depends to a significant extent on access to critical minerals such as lithium, cobalt, nickel, graphite and rare-earth elements. Control of these resources is thus becoming a new dimension of geopolitical competition.

The People's Republic of China holds a dominant position in the processing of many of these materials and in the production of batteries, photovoltaic panels and components for wind turbines. Consequently, future energy security will depend not only on access to oil and natural gas, but also on the availability of the raw materials required for low-emission technologies.

This transformation marks the shift from the geopolitics of hydrocarbons to the geopolitics of critical minerals.

5.5. Energy and maritime security

Most of the world's energy flows are transported by sea, which gives trade routes exceptional strategic importance.

The Strait of Hormuz, the Suez Canal, Bab el-Mandeb and the Strait of Malacca account for very large volumes of oil, liquefied natural gas and petroleum products. Any disruption to the functioning of these corridors immediately affects international prices and the stability of energy markets.

Recent events have demonstrated that energy security is inseparable from maritime security. Attacks on oil tankers, the use of naval mines, threats to offshore infrastructure and the increased military presence in transit areas make freedom of navigation an essential condition for the functioning of the global economy.

In this context, international naval cooperation and the development of effective mechanisms for monitoring maritime traffic are becoming fundamental components of energy security policies.

5.6. Energy resilience

The concept of energy resilience reflects the ability of a state or organisation to ensure the continuity of supply in the event of major disruptions.

Resilience involves diversifying supply sources and routes, developing storage capacities, interconnecting national and regional networks, modernising infrastructure and strengthening mechanisms for international cooperation.

Experience in recent years shows that states with diversified sources and flexible infrastructure respond more effectively to shocks caused by armed conflicts, natural disasters or economic crises.

At the same time, the digitalisation of energy systems requires the integration of cyber security at all stages of infrastructure management, as cyber-attacks can have effects comparable to those of physical attacks on energy facilities.

Energy security is today one of the fundamental pillars of international security and a key determinant of the geopolitical balance. Control of resources, protection of infrastructure and diversification of supply sources influence states' ability to protect their strategic interests and respond effectively to crisis situations.

Recent developments show that energy is no longer merely an economic resource, but an instrument of power and influence. At the same time, the energy transition is gradually changing the nature of global competition, shifting the focus towards smart infrastructure, clean technologies and access to critical minerals. In this new context, energy security becomes inseparable from economic, technological and maritime security, thereby consolidating its central role in the global security architecture.

CHAPTER VI

6. The Economy and Global Security – Interdependence, Vulnerability and Strategic Competition

6.1. The Economy as a Dimension of Security

In recent decades, the relationship between the economy and security has undergone a fundamental transformation. Whilst during the Cold War the military dimension almost exclusively dominated strategic analysis, recent developments demonstrate that economic power is one of the main instruments through which states project their influence and pursue their geopolitical objectives. The economy is no longer merely the foundation of national development, but a veritable arena of strategic competition, in which access to resources, control of technologies, financial stability and the resilience of supply chains directly influence international security.

Globalisation has created a deeply interdependent economic system, characterised by regional specialisation and the integration of production on a global scale. This model has fostered economic growth and reduced production costs, but has simultaneously generated new vulnerabilities. Recent crises have demonstrated that the disruption of a port, a semiconductor factory or a maritime route can have global economic repercussions within a very short timeframe.

Consequently, economic security is becoming an inseparable component of national and collective security.

6.2. Global supply chains and systemic vulnerability

The modern economy operates through global supply chains that connect thousands of manufacturers, suppliers and logistics operators across all regions of the world. These networks enable the efficient distribution of raw materials and finished products; however, dependence on a small number of logistics hubs and production centres amplifies the risk of systemic disruptions.

The COVID-19 pandemic was the first major test of these chains, and the conflicts in Ukraine and the Middle East have confirmed that the blockage of trade corridors or the deterioration of logistics infrastructure can simultaneously affect industries located thousands of kilometres away. Delays in maritime transport, shortages of electronic components and rising logistics costs have demonstrated that economic resilience depends on the ability of states and companies to diversify their supply sources and reduce critical dependencies.

In this context, many developed economies are promoting processes of **nearshoring**, **friend-shoring** and **strategic reshoring**, whereby certain industrial capacities are relocated to countries considered politically and strategically stable. This trend marks the beginning of a structural reorganisation of globalisation, focused less on maximum economic efficiency and more on security of supply.

6.3. Economic sanctions and financial competition

Economic instruments have become one of the main means of exerting international pressure. Financial sanctions, trade restrictions, restrictions on access to sensitive technologies and asset freezes are being used with increasing frequency to influence the behaviour of states, without resorting directly to military force.

The conflict in Ukraine is the most extensive example of the coordinated use of economic sanctions against a major state actor. Restrictions on access to international financial systems, limits on technology exports and measures to cap revenues from energy exports have demonstrated that the economy can become a strategic instrument comparable to the use of armed force.

At the same time, these developments have accelerated trends towards the fragmentation of the international economic system. Some states are seeking to reduce their dependence on Western currencies, are developing alternative payment mechanisms and are promoting regional trade agreements, which may lead, in the long term, to the emergence of a global economy that is less integrated and more strongly influenced by geopolitical rivalries.

6.4. Technology and the competition for economic advantage

Contemporary strategic competition is increasingly taking place in the technological sphere. Artificial intelligence, quantum computing, semiconductors, next-generation communications and space technologies represent strategic resources comparable to oil or natural gas in the last century.

Control over the production of advanced semiconductors, data processing capabilities and critical technologies influences states' economic competitiveness, military development and strategic autonomy. Consequently, many governments are adopting industrial policies aimed at developing their own technological capabilities and reducing external dependencies.

This competition is giving rise to new forms of strategic protectionism, in which national security is used to justify export restrictions, investment controls and the protection of digital infrastructure.

6.5. Critical minerals and the economy of the future

The energy and digital transitions are amplifying the importance of critical raw materials. Lithium, cobalt, nickel, graphite and rare-earth elements are indispensable for the production of batteries, electric vehicles, energy storage systems and advanced electronic equipment.

The uneven geographical distribution of these resources and the concentration of processing capacity in a few countries are creating new strategic dependencies. Consequently, competition for access to critical minerals is becoming an essential component of economic and technological security, influencing investment, trade relations and foreign policy.

This development indicates that 21st-century geopolitics will be shaped not only by competition for hydrocarbons, but also by access to resources that are indispensable to the digital economy and the energy transition.

6.6. Economic resilience and strategic security

The concept of economic resilience reflects an economy's ability to absorb external shocks, maintain the functioning of essential sectors and return rapidly to a normal level of activity. In the current strategic environment, economic resilience is no longer solely a concern of financial policy, but a central objective of national security strategies.

Building resilience involves diversifying trade relations, strengthening logistics infrastructure, developing domestic industrial capabilities and maintaining strategic reserves of essential products and raw materials. At the same time, international cooperation remains indispensable, as no economy can completely eliminate the effects of global interdependencies.

The global economy has become one of the main arenas of contemporary strategic competition. The interdependencies created by globalisation generate significant opportunities for development, but they equally amplify systemic vulnerabilities. Armed conflicts, economic sanctions, technological competition and disruptions to supply chains demonstrate that economic stability cannot be separated from international security.

In this context, economic resilience is an essential prerequisite for maintaining political and social stability. The ability of states to protect economic infrastructure, ensure continuity of supply and rapidly adapt economic policies to geopolitical developments will be one of the key factors defining the international strategic balance in the coming decades.

CHAPTER VII

7. Hybrid threats and emerging technologies – redefining conflict in the 21st century

7.1. The Transformation of Contemporary Conflict

One of the most significant transformations in the international security environment is the profound change in the nature of conflict. Today, confrontation between states and between various international actors is no longer limited to the use of armed force, but encompasses a complex array of political, economic, informational, technological and legal instruments, employed simultaneously to achieve strategic objectives.

This development reflects the shift from the classical model of conventional warfare to a model characterised by the integration of various forms of pressure, deployed in the physical, informational and digital domains alike. Under these circumstances, the distinction between periods

of peace and conflict is becoming increasingly difficult to identify, and strategic competition is ongoing, even in the absence of direct military confrontations.

The concept of a hybrid threat captures precisely this transformation, referring to the coordinated use of multiple instruments to influence an adversary's decision-making process and undermine its ability to respond effectively.

Table 8. Hybrid threats and the domains affected

Type of hybrid threat	Instruments used	Areas affected	Strategic objective
Disinformation	Social media, mass media, digital platforms	Public opinion, electoral processes	Erosion of trust in institutions
Cyberattacks	Malware, ransomware, APT	Critical infrastructure	Disruption of essential services
Economic pressure	Sanctions, embargoes, trade restrictions	Economy and industry	Influencing political decisions
The instrumentalisation of migration	Controlled migration flows	Internal security	Pressure on neighbouring states
Sabotage	Energy and logistics infrastructure	Energy and transport	Disruption to the functioning of the economy
Information operations	Coordinated campaigns	Information space	Social polarisation and destabilisation
Use of proxy actors	Armed groups, mercenaries	Regional conflicts	Avoiding direct responsibility

7.2. The information dimension of strategic competition

Information has become one of the most important strategic resources of the 21st century. The development of digital platforms and the expansion of social media have radically altered the way in which information is produced, distributed and consumed, transforming the information space into a key arena of geopolitical competition.

Disinformation campaigns, media manipulation and psychological operations aim to influence public perception, erode trust in institutions and polarise democratic societies. Unlike traditional propaganda, these operations use algorithms, digital platforms and automated tools to rapidly amplify certain messages and tailor content to the characteristics of different audience groups.

In this context, protecting the information space becomes a fundamental component of national security, and developing information verification capabilities and strengthening societal resilience are strategic priorities for most states.

7.3. Cyber security and digital infrastructure

The accelerated digitalisation of the economy and public administration has led to a significant expansion of the surface area exposed to cyber-attacks. Energy networks, financial systems, transport infrastructure, hospitals and public administrations depend on complex IT platforms, the compromise of which can have effects comparable to those of a conventional military attack.

Contemporary cyber attacks are not aimed solely at obtaining confidential information. Increasingly, they are directed at disrupting the functioning of essential services, compromising critical infrastructure and undermining public confidence in the state's ability to manage crisis situations.

At the same time, the use of cybercrime groups and non-state actors enables some states to carry out complex operations, reducing the risk of having to assume direct responsibility. This characteristic complicates the attribution of attacks and limits the effectiveness of traditional deterrence mechanisms.

Table 9. Vulnerabilities of digital infrastructure

Infrastructure category	Main vulnerabilities	Potential impact	Estimated risk level	Resilience measures
Data centres	Cyber attacks, power cuts, sabotage	Disruption to digital and financial services	Very high	Geographical redundancy, backups, physical and cyber protection
Internet backbone networks	DDoS attacks, equipment failure, sabotage	Blockage of global communications	Very high	Route redundancy and continuous monitoring
Submarine cables	Sabotage, maritime accidents, hostile underwater activities	Disruption of intercontinental communications	Very high	Naval surveillance and underwater sensors
Mobile networks (5G/6G)	Interference, attacks on radio infrastructure	Disruption to civilian and military communications	High	Segmentation and encryption
Cloud computing	Vendor compromise, ransomware attacks	Disruption of public and private services	High	Multi-cloud and redundancy
Communications satellites	Jamming, anti-satellite attacks, interference	Loss of communications and navigation	High	Redundant constellations and alternative systems
AI platforms	Model manipulation, attacks on training data	Erroneous decisions and disinformation	High	Algorithmic audit and continuous validation

7.4. Artificial intelligence and the transformation of security

Artificial intelligence is one of the most important emerging technologies with an impact on global security. The ability of systems based on advanced algorithms to process very large volumes of information in an extremely short time is changing both the process of strategic analysis and the conduct of military operations.

In the defence sector, artificial intelligence is used for analysing satellite imagery, identifying targets, optimising logistics, supporting decision-making and developing autonomous systems. These applications enhance operational efficiency, but also raise ethical and legal challenges regarding the degree of autonomy of weapon systems and accountability for decisions made by algorithms.

At the same time, artificial intelligence is transforming the work of intelligence services, facilitating the early detection of trends and the rapid integration of information from multiple sources. However, over-reliance on algorithms can create additional vulnerabilities, particularly in situations where systems are manipulated or trained on incomplete or biased datasets.

Table 10. Artificial intelligence and its applications in the field of security

Field	AI applications	Benefits	Risks

Intelligence	Data analysis and pattern detection	Prediction and early warning	Algorithmic bias
Defence	Operational planning and target identification	Faster decision-making	Over-reliance on algorithms
Logistics	Supply optimisation	Operational efficiency	Cyber vulnerabilities
Cyber defence	Attack detection	Rapid response	Attacks on AI models
Surveillance	Satellite and video image analysis	Continuous monitoring	Privacy concerns
Crisis management	Forecasting and simulation	Decision-making	Modelling errors
Critical infrastructure protection	Predictive monitoring	Risk mitigation	Compromise of smart systems

7.5. Drones and autonomous systems

The conflict in Ukraine and developments in the Middle East have demonstrated that drones and autonomous systems represent one of the most significant innovations in contemporary warfare. Their relatively low cost, operational flexibility and ability to carry out missions in high-risk environments have made these platforms indispensable tools for modern military operations.

Drones are used for reconnaissance, surveillance, precision strikes, electronic warfare and assessing the effects of attacks. The development of autonomous systems capable of operating in coordinated groups and adapting their operational behaviour in real time opens up the prospect of a new generation of conflicts, in which the speed of decision-making will exceed human reaction times.

These developments necessitate the development of appropriate legal and ethical frameworks capable of ensuring that the use of autonomous technologies is compatible with the norms of international humanitarian law and the principles of state responsibility.

7.6. Outer space – the new strategic frontier

Outer space is becoming increasingly important for international security. Communications satellites, navigation systems, Earth observation platforms and commercial space infrastructure underpin the functioning of the global economy and modern defence systems.

At the same time, competition to develop space capabilities and the testing of anti-satellite systems are amplifying the security risks in this domain. The damage to or destruction of space infrastructure can simultaneously affect communications, navigation, weather forecasting, environmental monitoring and military operations.

This development highlights the need to strengthen international regulations on the peaceful use of space and the protection of critical space infrastructure.

Table 11. The evolution of emerging technologies and their impact on security

	Current level of development	Areas of application	Strategic impact
	Very high	Strategic analysis, defence, logistics	Very high
	Very high	Military operations and surveillance	Very high
	Rapidly developing	Cryptography and processing	High
	Under development	Secure communications	High
	High	Satellites and strategic observation	High

	High	Health and biosecurity	Moderate–High
	High	Logistics and special operations	High
	Developing	Industry and defence	Moderate

7.7. Governance of emerging technologies

The rapid development of emerging technologies is creating unprecedented opportunities, but also complex risks for international security. The pace of innovation often outstrips the capacity of legal and institutional mechanisms to respond to new challenges, creating areas of regulatory uncertainty.

In this context, international cooperation is essential for developing common principles on the responsible use of artificial intelligence, cyber security, the protection of digital infrastructure and the development of autonomous systems. Technology governance must strike a balance between stimulating innovation and preventing the misuse of new technologies.

At the same time, the development of effective mechanisms for information-sharing and cooperation between states, international organisations, academia and the private sector is an indispensable prerequisite for strengthening global security in a technological environment undergoing constant transformation.

Emerging technologies and hybrid threats are fundamentally altering the architecture of international security. The information domain, digital infrastructure, artificial intelligence, autonomous systems and space complement the traditional dimensions of conflict and give rise to unprecedented legal, political and operational challenges.

In this context, strategic advantage will no longer depend exclusively on military or economic superiority, but on states' ability to integrate emerging technologies into an institutional and regulatory framework that simultaneously ensures operational efficiency, the protection of fundamental rights and respect for the principles of international law. Strengthening technological resilience and developing global governance adapted to the new realities are thus essential conditions for maintaining international stability and security in the 21st century.

CHAPTER VIII

8. Assessment of global strategic risks

8.1. The Need for an Integrated Approach

The complexity of the contemporary international environment requires us to move beyond traditional models of security assessment. In the past, strategic analysis focused almost exclusively on military indicators, such as the size of armed forces, mobilisation capacity or the balance of armaments. Today, this approach is insufficient. International stability is influenced simultaneously by geopolitical, economic, energy-related, technological, climatic and societal factors, which constantly interact and generate cumulative effects.

Strategic risk assessment must therefore be multidimensional and enable the identification of relationships between different categories of threats. An energy crisis can lead to economic instability, which in turn can fuel social tensions, whilst a deterioration in the political climate can encourage the emergence of regional conflicts or the escalation of hybrid threats. Similarly, a

cyberattack on critical infrastructure can have consequences for the financial system, public services and public confidence in state institutions.

From this perspective, global security must be analysed as a dynamic system, in which a change in a single indicator can simultaneously influence numerous other components of the strategic environment.

8.2. Key indicators of strategic risk

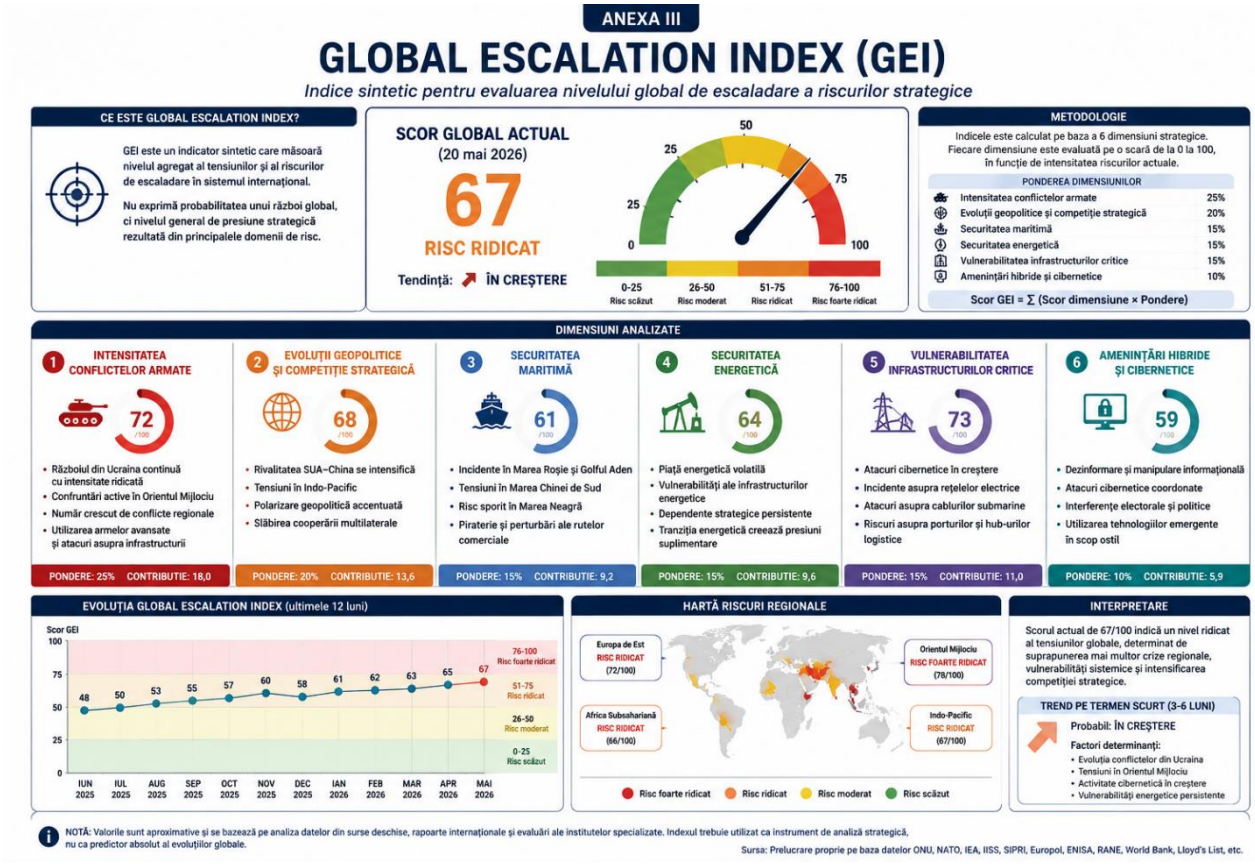
The assessment presented in this paper is based on a set of indicators that reflect the main dimensions of contemporary security. These include the intensity of armed conflicts, the degree of geopolitical stability, energy security, maritime security, the resilience of critical infrastructure, cyber security, economic stability, food security, climate change and the crisis management capacity of international institutions.

None of these indicators alone can explain the evolution of the strategic environment. Their relevance stems from integrated analysis and the observation of medium- and long-term trends. A simultaneous rise in geopolitical tensions, economic vulnerabilities and attacks on critical infrastructure may signal the approach of a period of heightened instability, even if each of these developments, when analysed in isolation, appears manageable.

In this regard, risk assessment should not only aim to identify existing threats, but also to detect gradual changes that may lead to major crises.

Table 12. Indicators used to calculate the Global Escalation Index (GEI)

No.	Area assessed	Main indicator	Elements analysed	Weight in the index (%)	Score (0–100)
1	**Military conflict**	Intensity of armed clashes	Military operations, mobilisation of forces, use of strategic weapons, casualties, expansion of front lines	**20**	0–100
2	**Geopolitics**	Tensions between the major powers	Diplomatic crises, sanctions, alliances, strategic competition, official statements	**15**	0–100
3	**Energy security**	Vulnerability of energy systems	Production, transport, critical infrastructure, volatility of the oil and gas market	**10**	0–100
4	**Maritime security**	Freedom of navigation	Situations in straits, naval incidents, attacks on commercial shipping, maritime blockades	**10**	0–100
5	**Critical infrastructure**	Level of vulnerability	Energy, ports, pipelines, submarine cables, telecommunications, logistics centres	**10**	0–100
6	**Cyber security**	Digital threats	Cyber attacks, information operations, compromise of digital infrastructure	**10**	0–100
7	**Economic stability**	Economic vulnerabilities	Sanctions, market volatility, supply chains, international trade	**8**	0–100
8	**Technological security**	Competition for critical technologies	Artificial intelligence, semiconductors, autonomous systems, quantum communications	**5**	0–100
9	**Humanitarian security**	Impact on the civilian population	Population displacement, civilian casualties, food and health insecurity	**6**	0–100
10	**International governance**	Crisis management capacity	The work of the UN, NATO, the EU, the OSCE, the G7, the G20 and international cooperation	**6**	0–100



8.3. Escalation of regional conflicts

The analysis carried out in the preceding chapters highlights the fact that the war in Ukraine and developments in the Middle East continue to represent the main sources of risk to international security. These conflicts simultaneously affect energy security, economic stability and freedom of navigation, and any regional spillover would have significant consequences for the entire international system.

At the same time, strategic competition in the Indo-Pacific and persistent tensions in the South China Sea must be analysed not only in terms of the possibility of a military conflict, but also in relation to their impact on global trade, advanced technologies and financial markets.

The current assessment indicates that the likelihood of regional incidents remains high, but the risk of a global military conflict breaking out is currently lower. However, the simultaneous overlap of several regional crises could generate cumulative effects that are difficult to anticipate and manage.

8.4. The vulnerability of critical infrastructure

The protection of critical infrastructure is one of the most significant challenges facing contemporary security. Attacks on energy networks, communications systems, port infrastructure and submarine cables demonstrate that these targets are increasingly perceived as strategic power multipliers.

The interdependent nature of modern infrastructure amplifies the risk of cascading effects. A limited disruption to the energy supply can affect communications, transport and financial systems, whilst a disruption to digital infrastructure can simultaneously impact the functioning of public administration, healthcare services and the economy.

For this reason, risk assessments must pay particular attention to the ability of critical infrastructure to withstand stress, to continue operating under stress and to return rapidly to normal parameters following incidents.

8.5. Technological risks and the digital society

Digital transformation generates significant opportunities for economic development and the streamlining of public administration, but it also creates new categories of vulnerabilities. Artificial intelligence, automation, autonomous systems and the expansion of digital infrastructure are increasing modern societies' dependence on complex technologies and global IT platforms.

In this context, the risks associated with cyber-attacks, information manipulation and the misuse of artificial intelligence are becoming increasingly strategically significant. The impact of these threats is not limited to the technological sphere, but affects public trust, institutional stability and the ability of states to respond effectively in crisis situations.

Consequently, any assessment of global security must systematically include an analysis of digital resilience and the level of institutional preparedness for managing emerging threats.

8.6. Developing an integrated assessment model

Building on the analysis presented in this paper, an integrated model for assessing global security can be proposed, based on five major dimensions: geopolitical stability, economic resilience, energy and maritime security, the protection of critical infrastructure, and technological capability. These dimensions are interdependent and must be analysed as a whole, as a change in one of them inevitably affects the functioning of the others.

Such a model does not aim to produce absolute forecasts, but rather to identify trends at an early stage and assess the likelihood of developments with strategic implications. In practice, it can form the basis for the development of tools such as a **Global Escalation Index**, a **Critical Infrastructure Watch** or a **Global Security Dashboard**, capable of synthesising information from different fields into an accessible format and supporting the decision-making process.

The assessment of global strategic risks represents one of the most significant challenges for contemporary security analysis. The complexity of the international environment requires the integration of military, economic, energy, maritime, technological and institutional dimensions into a single analytical framework. Fragmented approaches are no longer sufficient to explain current developments, nor to underpin effective public policies.

Table 13. Indicators of strategic resilience

Area	Indicator	Target	Level of assessment
Energy	Security of supply	Economic performance	Low – Very high
Critical infrastructure	Availability of infrastructure	Continuity of essential services	Low – Very high
Economy	Stability of supply chains	Economic resilience	Low – Very high
Cyber security	Response capacity	Protection of digital systems	Low – Very high
Public institutions	Continuity of governance	Administrative stability	Low – Very high
Public health	Capacity of the healthcare system	Crisis management	Low – Very high
Strategic communication	Public trust	Societal resilience	Low – Very high
International cooperation	Level of coordination	Global crisis management	Low – Very high

The main conclusion arising from the analysis presented is that global security must be understood as an adaptive system, characterised by multiple interdependencies and a high capacity for effects to propagate across different domains. In this context, the development of integrated

monitoring and early warning tools is not merely a methodological option, but a strategic necessity for states, international organisations and institutions involved in global security management.

Table 14. Probability–impact matrix for global risks

Risk	Probability	Impact	Strategic level
Escalation of the war in Ukraine	High	Very high	Critical
Regional conflict in the Middle East	High	Very high	Critical
Blockade of the Strait of Hormuz	Moderate	Very high	Critical
Major attack on critical infrastructure	Moderate	Very high	Critical
Cyber attack on global infrastructure	High	High	Very high
Global energy crisis	Moderate	High	High
Collapse of supply chains	Moderate	High	High
Global food crisis	Moderate	Moderate–High	High
Major incident in the South China Sea	Moderate	Very high	Critical
Militarisation of outer space	Low	High	Moderate

CHAPTER IX

9. Prospective scenarios regarding the evolution of global security

9.1. The need for a forward-looking approach

The contemporary international environment is characterised by a high level of uncertainty, driven by the simultaneous interaction of political, economic, technological, climatic and military factors. Under such conditions, strategic planning cannot be based solely on a retrospective analysis of events or on the mechanical extrapolation of existing trends. The complexity of the international system necessitates the use of forward-looking methods that enable the assessment of several possible directions of development and the identification of factors capable of altering the global balance.

The scenarios presented in this chapter are not predictions, nor do they express absolute probabilities. They are analytical tools that enable an understanding of how various strategic variables may interact and influence international security in the coming years. Their value lies in highlighting the opportunities, vulnerabilities and critical issues on which decision-makers must focus their attention.

9.2. Scenario I – Competitive Stabilisation

The first scenario envisages keeping competition between the major powers within manageable limits and avoiding direct military confrontations. In this scenario, the war in Ukraine

evolves into a frozen conflict or a limited negotiated settlement, without resolving all territorial disputes. In the Middle East, tensions between Iran, Israel and the United States persist, but the parties involved avoid escalation into a full-scale regional war.

Competition between the United States and China is predominantly played out in the economic, technological and commercial spheres, whilst disputes over Taiwan and the South China Sea are managed through deterrence and diplomatic dialogue. International organisations retain their role as platforms for negotiation, even if their effectiveness remains limited.

Economically, global supply chains are adapting to the new geopolitical realities by diversifying routes and relocating some industrial capacity. Investment in critical infrastructure and cyber security is helping to increase the resilience of developed economies.

This scenario is characterised by intense but manageable competition, in which the risk of a global conflict remains low, and international actors prefer to use economic and diplomatic instruments rather than direct military confrontation.

9.3. Scenario II – Multiple regional escalations

The second scenario involves the simultaneous escalation of several regional conflicts and a decline in the international community's capacity to manage these developments effectively.

In Europe, the conflict in Ukraine is intensifying as attacks on critical infrastructure expand and weapon systems with an ever-greater range are being deployed. In the Middle East, incidents in the Strait of Hormuz and the Red Sea are affecting freedom of navigation and causing significant disruption to energy markets. In the Indo-Pacific, military competition around Taiwan and in the South China Sea is leading to naval and air incidents with a high risk of escalation.

The economic consequences of this scenario are significant. Shipping costs are rising, energy and commodity prices are becoming volatile, and global supply chains are under constant pressure. At the same time, the intensification of cyber-attacks and information operations is disrupting the functioning of critical infrastructure and amplifying political polarisation in many countries.

This scenario does not envisage the outbreak of a global conflict, but describes a period characterised by the simultaneous accumulation of several regional crises, capable of significantly affecting the stability of the international system.

9.4. Scenario III – Fragmentation of the international order

In this scenario, geopolitical competition leads to an acceleration of the fragmentation of the international system. Multilateral cooperation gradually declines, and economic relations are reorganised around regional blocs and strategic alliances.

States prioritise national security at the expense of economic efficiency, leading to increased protectionism, restrictions on technology transfer and the development of separate industrial ecosystems. International institutions retain their formal existence, but their influence on crisis management diminishes.

On the technological front, competing digital ecosystems, incompatible standards and IT infrastructures developed separately by the main centres of power are emerging. The fragmentation of the internet, the regionalisation of financial systems and competition for control of critical technologies are profoundly altering the architecture of globalisation.

This scenario depicts a less integrated world, in which cooperation is gradually being replaced by the logic of strategic autonomy and constant competition.

9.5. Scenario IV – Adaptive Cooperation

The most favourable scenario involves the development of new mechanisms for international cooperation, adapted to the technological and geopolitical realities of the 21st century. International actors recognise the global nature of the main threats and agree to strengthen forms of

cooperation in areas such as cyber security, the protection of critical infrastructure, artificial intelligence, climate change and global health.

In this scenario, competition between the major powers continues, but is accompanied by minimum rules governing the management of military incidents, the use of autonomous technologies and the protection of critical infrastructure. New mechanisms for transparency and information-sharing are developed, and regional cooperation helps to reduce economic and energy vulnerabilities.

Although this scenario presupposes political conditions that are difficult to achieve in the short term, it highlights the direction in which the international system could evolve if trust were to be strengthened and international institutions were to adapt to new challenges.

Table 15. Prospective scenarios for global security (2026–2035)

Scenario	Key characteristics	Estimated probability	Strategic impact	Implications
Competitive stabilisation	Competition between major powers, without direct conflict	High	Moderate	Maintaining the strategic balance and adapting international institutions
Multiple regional escalations	Simultaneous intensification of regional conflicts	Moderate–High	High	Increased economic and energy instability
Fragmentation of the international order	Regionalisation of the economy and a decline in multilateral cooperation	Moderate	Very high	The emergence of competing geopolitical blocs
Adaptive cooperation	Strengthening of multilateral mechanisms and the development of global governance	Moderate–Low	Very high positive	Increased resilience of the international system

9.6. Determinants of developments

Regardless of which scenario materialises, the evolution of global security will be influenced by several structural factors. The ability of major powers to manage strategic competition without resorting to direct confrontation, the pace of technological development, the security of critical infrastructure, the stability of energy markets and the effectiveness of international cooperation mechanisms will be the main variables shaping the strategic environment over the next decade.

Equally, the resilience of societies and their ability to cope with multiple crises will be of comparable importance to the evolution of military relations between states.

The forward-looking analysis highlights the fact that the future of global security is not determined by a single event or a single conflict, but by the constant interplay between economic, technological, energy, climate and geopolitical processes. The most likely developments point to the continuation of intense strategic competition, characterised by regional conflicts, technological rivalry and pressure on critical infrastructure, with no clear indications of a global military confrontation.

In this context, preparing for the future must be based on the development of integrated analysis systems, the strengthening of institutional resilience and the promotion of cooperation and ‘ ’ mechanisms capable of reducing the likelihood of regional crises turning into systemic threats. The scenarios presented do not offer definitive answers, but they contribute to an understanding of possible directions of development and to the formulation of strategic decisions tailored to a rapidly changing international environment.

CHAPTER X

General conclusions and perspectives on global security

The analysis carried out in this paper highlights the fact that the international system is undergoing one of the most complex periods of transformation in the last eight decades. Current dynamics cannot be explained solely by the existence of regional conflicts or by shifts in the balance of power between major states. They reflect a structural shift in the way international society functions and in the mechanisms through which global risks are generated, propagated and managed.

One of the study's key conclusions is that international security has become profoundly systemic. In the past, conflicts could be analysed predominantly from a military perspective, and their effects remained, to a large extent, geographically limited. Nowadays, every crisis has multiple consequences for the global economy, critical infrastructure, energy markets, international trade, financial systems and digital communications. Global interdependence transforms almost any major incident into a phenomenon with transnational implications.

In this context, the war in Ukraine and the persistent tensions in the Middle East must be understood not merely as two regional conflicts, but as manifestations of a broader strategic competition over the distribution of power within the international system. Both demonstrate that traditional military objectives coexist with attacks on critical infrastructure, economic pressure, information operations and the use of emerging technologies, which fundamentally alter the nature of contemporary confrontation.

The paper shows that critical infrastructure is one of the main focal points of security in the 21st century. Energy networks, digital communications, ports, submarine cables, pipelines and logistics centres are indispensable to the functioning of modern societies and, at the same time, priority targets for actors seeking to gain a strategic advantage. The vulnerability of these infrastructures not only affects a state's national security, but can also have systemic effects on regional and global stability.

Equally, research confirms that energy security can no longer be separated from maritime security, technological development and geopolitical competition. Control of maritime routes, access to energy resources and critical minerals, and the protection of transport and distribution infrastructure are central elements of contemporary security policies. The energy transition does not eliminate these rivalries, but transforms them, shifting the focus towards new strategic resources and technologies with a major impact on economic and military development.

Another important finding of the analysis is the highlighting of the role of emerging technologies in redefining international security. Artificial intelligence, autonomous systems, quantum communications, big data analysis and the digitalisation of infrastructure are changing both the nature of conflicts and the decision-making process. Technological superiority is becoming a determining factor in strategic power, and the ability to integrate new technologies into an appropriate legal and institutional framework will decisively influence states' positions within the international system.

At the same time, the analysis demonstrates that resilience is becoming the central concept of contemporary security. In an environment characterised by constant uncertainty, the objective of public policy can no longer be the elimination of all threats, but rather the development of societies' capacity to anticipate, absorb and overcome the effects of complex crises. Resilience entails strengthening critical infrastructure, diversifying energy sources, protecting digital systems, enhancing international cooperation and developing effective early-warning mechanisms.

A distinctive contribution of this paper lies in proposing an integrated approach to strategic risk assessment. Rather than a sectoral analysis, the study argues for the need to use tools capable of correlating geopolitical, economic, energy, maritime, technological and climate developments within a single assessment model. Tools such as **the Global Escalation Index**, **Critical**

Infrastructure Watch, **Maritime Security Dashboard**, **Global Energy Security Dashboard** and **Global Security Brief** illustrate how information from different fields can be integrated into a unified process of analysis and strategic decision-making support.

From a methodological perspective, the research demonstrates the value of combining classical geopolitical analysis with methods specific to foresight studies and strategic intelligence. In an international environment characterised by rapid change and complex interdependencies, the value of analysis no longer lies solely in explaining past events, but also in identifying emerging trends and anticipating their implications for global security.

Looking ahead, the international system is expected to remain characterised by intense strategic competition, a proliferation of regional conflicts and the acceleration of technological change. However, this development does not inevitably lead to a global military confrontation. The international community's ability to adapt cooperation mechanisms, develop legal norms for new technologies and strengthen the resilience of critical infrastructure can help to mitigate risks and maintain an acceptable level of stability.

In conclusion, global security in the 21st century must be understood as the result of the interaction between military, economic, energy, technological, legal and societal factors. None of these dimensions can any longer be analysed in isolation. Only an interdisciplinary, systemic and forward-looking approach can provide adequate explanations for the complexity of the contemporary strategic environment and underpin public policies capable of responding to the challenges of the future.

CHAPTER XI

11. A new paradigm of global security – towards a systemic model of strategic analysis

11.1. The Limitations of Traditional Paradigms

For several decades, the analysis of international security has been based on conceptual models developed in a geopolitical context fundamentally different from the present one. Theories of classical and structural realism, liberal institutionalism and various constructivist approaches have convincingly explained numerous developments in the international system; however, the rapid transformations of the last two decades highlight significant limitations in these models when applied to the contemporary strategic environment.

The main reason is that most theories address security in relation to the state and the use of military force, whilst current threats arise from the interaction of complex systems in which state actors coexist with international organisations, multinational companies, digital platforms, global infrastructure and technological networks. In this context, security can no longer be reduced to relations between states, but must be analysed as an emergent property of a global system characterised by multiple interdependencies.

11.2. From military security to systemic security

One of the fundamental conclusions of this research is that global security must be redefined from the perspective of the functionality of the international system.

An international system can be considered secure not only when armed conflicts are absent, but when it retains its capacity to function despite the existence of external shocks. From this perspective, security becomes an expression of systemic resilience and the capacity of institutions, infrastructure and economic mechanisms to absorb disruptions without losing essential functions.

This shift in perspective brings security studies closer to complex systems theory and to approaches developed in the field of organisational resilience, without detracting from the importance of the military dimension. On the contrary, the military component is integrated into a broader set of factors contributing to international stability.

11.3. The polycentric security model

The analysis presented in this paper leads to the formulation of the concept of **polycentric security**, which refers to the simultaneous existence of multiple centres of stability and instability, in a permanent state of interdependence.

In such a system, no single actor holds exclusive control over global security. Stability arises from the interaction between international organisations, states, regional alliances, critical infrastructure, financial markets, energy networks and digital ecosystems.

This perspective explains why a deterioration in security in a single region can have repercussions across the entire system, and why effective responses require cooperation between actors from different fields.

11.4. Strategic intelligence as security infrastructure

In traditional literature, intelligence is analysed primarily as the activity of gathering and analysing information.

However, current transformations allow for a broader interpretation. The capacity to anticipate becomes a critical infrastructure in its own right.

A state that possesses high-performance systems for early warning, predictive analysis and rapid information integration enjoys a strategic advantage comparable to that offered by energy infrastructure or technological superiority.

From this perspective, strategic intelligence ceases to be merely a process and becomes a structural component of a state's resilience.

11.5. Systemic indicators of security

Building on the analysis carried out in the previous chapters, a model based on six fundamental indicators of global security can be proposed:

The first indicator is geopolitical stability, which reflects the level of conflict and competition amongst international actors.

The second is the resilience of critical infrastructure, expressing societies' ability to maintain their essential functions.

The third is energy and food security.

The fourth is technological and digital security.

The fifth is economic resilience.

The final indicator is the quality of international governance and the capacity of multilateral institutions to manage crises.

Together, these indicators enable a systemic assessment of the strategic environment and can form the basis for the development of tools for ongoing monitoring.

11.6. Strategic anticipation

Perhaps the most significant change in the field of international security is the shift from reaction to anticipation.

In the past, strategic analysis was predominantly conducted after events had taken place.

Today, the competitive advantage lies with those actors capable of identifying trends before they have a major impact.

This approach involves the development of permanent monitoring systems based on the integration of geopolitical, economic, climatic, technological and social data within a single analytical framework.

From this perspective, future security will depend less on the speed of reaction and more on the ability to anticipate.

I believe we can further enhance the academic value of the study. At present, the work is an excellent **strategic report**; however, to become a **reference monograph,** it lacks an element found in major works: **its own theoretical framework**. This should not be introduced at the beginning, but after the applied section, as the reader will better understand the model once they have gone through the analysis.

I would introduce an additional chapter, which I believe would represent the study's original contribution.

CHAPTER XII

12. The Theory of Strategic Gravity – an integrated model for the analysis of global security

12.1. Introduction

The analysis presented in the previous chapters highlights that global security can no longer be explained by linear models based exclusively on military relations between states. Contemporary developments demonstrate the existence of complex relationships between critical infrastructure, economic flows, emerging technologies, energy, information and international law. These components do not operate independently, but form a system characterised by permanent interdependencies and the capacity to generate cascading effects.

Building on this observation, this paper proposes a conceptual model known as **the Theory of Strategic Gravity**, through which international security is analysed as the result of the interaction between centres of strategic gravity and the flows connecting them.

The concept does not seek to replace classical theories of international relations, but rather to complement them by introducing a systemic perspective, adapted to the strategic environment of the 21st century.

Table 16. Comparison of classical and systemic models of security analysis

Criterion	Classical model	Proposed systemic model
Main actor	The state	The international system
Dominant sphere	Military	Multidimensional
Threats	Conventional	Conventional and hybrid
Approach	Reaction	Anticipation
Primary instrument	Deterrence	Resilience
Analysis	Sectoral	Integrated
Decision	Response to events	Proactive management
Objective	Territorial defence	System continuity

12.2. Strategic centres of gravity

At any given moment in history, there are a limited number of elements without which the functioning of the international system would be seriously impaired. These elements represent what this study defines as **strategic centres of gravity**.

These are not exclusively states.

A centre of gravity may be an energy infrastructure, a maritime route, a financial system, a digital platform, a critical technology or an international organisation.

Their importance stems from the fact that disrupting the functioning of such a centre has disproportionate effects on the entire international system.

For example, the Strait of Hormuz is an energy centre of gravity.

The Suez Canal is a logistical hub.

Taiwan is a technological centre of gravity due to its role in semiconductor production.

Submarine cables are centres of informational gravity.

The Black Sea is simultaneously a centre of gravity for energy, food and military affairs.

This perspective explains why many contemporary conflicts tend to centre on the same geographical areas and infrastructure.

Table 17. Strategic Centres of Gravity

Strategic centre	Global function	Vulnerability	Systemic impact
Strait of Hormuz	Energy flow	High	Very high
Suez Canal	World trade	Moderate	Very high
Black Sea	Energy and food security	High	High
Taiwan	Semiconductors	High	Very high
Internet backbone	Global communications	High	Very high
Submarine cables	Information flow	High	Very high
SWIFT	Financial system	Moderate	High
GNSS satellites	Navigation and synchronisation	Moderate	High

12.3. Strategic flows

There are constant flows between these centres.

These flows may be material, energy-related, financial, informational or technological.

Global security depends less on the existence of each individual centre and more on the continuity of these flows.

A disruption to energy flows affects the economy.

Disruptions to communications affect financial systems.

The blocking of maritime routes affects world trade.

The compromise of digital infrastructure affects almost all other components of the system.

Consequently, the primary focus of contemporary security is no longer merely the defence of territory, but the maintenance of the functionality of global flows.

12.4. The ripple effect

A fundamental characteristic of complex systems is the propagation of disruptions.

This research argues that global security is influenced by the existence of a **strategic ripple effect**, whereby a local disruption has consequences for regions far away.

An attack on an oil refinery can affect the global oil market.

The blockade of a port can affect the automotive industry on another continent.

The destruction of a submarine cable can affect global financial communications.

Thus, geographical distance ceases to be the main criterion for assessing strategic impact.

Far more important is the position that a particular element occupies within the global network.

12.5. Systemic resilience

In the proposed model, resilience is not viewed exclusively as a property of a state.

It represents the capacity of the entire international system to continue functioning following major disruptions.

This approach explains why certain regional conflicts do not produce global effects, whilst seemingly minor incidents generate international economic crises.

The difference is determined by the strategic position occupied by the affected infrastructure or region.

Consequently, resilience must be analysed simultaneously at local, regional and global levels.

12.6. Strategic gravity and anticipation

Perhaps the most important implication of the model is that it allows for the anticipation of developments.

Rather than focusing exclusively on existing conflicts, the analysis must be directed towards changes occurring in centres of strategic gravity.

Rising tensions in a peripheral region may have a limited impact.

By contrast, changes occurring in a centre of strategic gravity are far more likely to generate global effects.

This perspective can underpin the development of modern early-warning systems based on the continuous monitoring of critical infrastructure, maritime routes, energy markets and essential technologies.

The Theory of Strategic Gravity proposes a reinterpretation of global security as the result of the interaction between centres of gravity and the flows connecting them. From this perspective, power is no longer defined exclusively by the military or economic capacity of states, but by the position they occupy within a global network of infrastructure, technologies, resources and institutions.

The model highlights that a system's vulnerability is determined not only by the intensity of threats, but also by the strategic importance of the elements affected and the degree of interdependence between them. This approach provides an analytical framework capable of explaining both the rapid spread of contemporary crises and the difficulty of managing them through traditional instruments.

Perfect. If the intention is for this work to become a **standard monograph**, I believe it is still missing a chapter that very few studies address: **the legal dimension of global security**. As a specialist in international law, this could become one of the work's distinctive chapters and lend it academic originality.

CHAPTER XIII

13. International law in the new security environment – between normative stability and strategic transformation

For over seven decades, international law has been one of the main instruments for organising and stabilising relations between states. The Charter of the United Nations, international

humanitarian law, the law of the sea and numerous other legal regimes have created a normative framework designed to prevent conflicts and peacefully manage international disputes. However, the rapid changes in the contemporary strategic environment raise fundamental questions regarding the capacity of international law to respond to challenges that go beyond the framework for which these norms were originally designed.

Current conflicts highlight the existence of a permanent tension between normative stability and the dynamics of geopolitical realities. The emergence of cyber warfare, the use of artificial intelligence in the military sphere, the development of autonomous systems, the militarisation of outer space and the expansion of competition over critical infrastructure demonstrate that many situations are not yet subject to sufficiently clear and uniformly accepted regulations.

In this context, international law is not facing a crisis of legitimacy, but is undergoing a process of adaptation to a strategic order undergoing profound transformation.

13.1. The Charter of the United Nations and strategic competition

The Charter of the United Nations continues to form the legal foundation of the contemporary international order. The principles of state sovereignty, the prohibition on the use of force, the peaceful settlement of disputes and international cooperation remain essential pillars of international law.

However, strategic competition between the major powers frequently limits the effectiveness of the mechanisms established by the Charter. Repeated deadlocks within the Security Council reflect the difficulty of applying collective mechanisms in a system characterised by intense geopolitical rivalries. At the same time, many contemporary conflicts involve non-state actors, cyber operations and activities conducted below the threshold of armed conflict, which complicates the application of traditional rules on the use of force.

This development does not diminish the relevance of the Charter, but rather highlights the need to interpret it within a technological and geopolitical context that differs from that of 1945.

13.2. International humanitarian law and the transformation of war

One of the most significant contemporary legal challenges is adapting international humanitarian law to the transformation of armed conflicts. The use of drones, autonomous systems, cyber operations and artificial intelligence raises questions regarding the application of the established principles of distinction, proportionality and precaution.

These principles remain fully valid. What is changing is the operational context in which they must be applied. Algorithm-assisted decision-making, automatic target identification and the use of autonomous platforms necessitate the development of additional mechanisms for control and accountability.

In this regard, the main challenge is not to abandon existing rules, but to interpret and apply them in a profoundly different technological environment.

13.3. The Law of the Sea and Maritime Security

Changes in maritime security confer unprecedented strategic relevance on the United Nations Convention on the Law of the Sea (UNCLOS). Freedom of navigation, the regime governing maritime zones, the protection of the marine environment and the use of natural resources are essential elements of economic and geopolitical stability.

Conflicts in the Black Sea, the Red Sea and the South China Sea demonstrate that the application of rules governing freedom of navigation and the protection of maritime infrastructure is now inextricably linked to energy security and the functioning of international trade. At the same time, the development of subsea infrastructure and the vulnerability of communication cables call

for further consideration regarding the legal protection of these assets and the responsibility of states in preventing and investigating incidents.

13.4. International law and critical infrastructure

One of the most significant transformations analysed in this paper is the shift in the focus of security towards critical infrastructure. From a legal perspective, this development raises issues concerning the classification of attacks against civilian infrastructure, states' obligations regarding prevention and protection, and international liability for cross-border damage.

At present, much critical infrastructure is operated by private entities, functions within transnational networks and serves several states simultaneously. This reality necessitates the development of forms of legal and institutional cooperation that go beyond the traditional paradigm of exclusively territorial jurisdiction.

The protection of critical infrastructure must be understood as a shared obligation, derived both from the national interest of each state and from the need to maintain the functionality of the international system.

13.5. Artificial intelligence and international law

The use of artificial intelligence in the field of security represents one of the most significant legal challenges of our time. Algorithms are integrated into processes of analysis, command and control, logistical planning, cyber defence and autonomous weapon systems, which raises issues regarding the attribution of responsibility and compliance with international obligations.

In the author's view, the development of international norms dedicated to artificial intelligence must follow three main directions. The first concerns ensuring human control over decisions involving the use of force. The second focuses on transparency and the auditability of systems used in critical areas. The third involves establishing clear mechanisms of legal liability for harm caused by the use of autonomous systems.

These principles do not seek to limit technological progress, but rather to integrate it into a regulatory framework compatible with the fundamental values of international law.

13.6. Towards an international law of resilience

The analysis carried out in this paper leads to the conclusion that international law is gradually evolving from a system predominantly geared towards the prevention of armed conflicts to one that is also concerned with safeguarding the functioning of the international system. In this context, the concept of resilience takes on a legal dimension of its own.

A potential **international right to resilience** would incorporate obligations regarding the protection of critical infrastructure, cooperation in the field of cyber security, the exchange of information on cross-border risks, ensuring the continuity of essential services, and the development of common mechanisms for responding to complex crises. This development does not entail abandoning existing norms, but rather extending them to respond to a reality in which systemic vulnerabilities simultaneously affect several states and areas of activity.

The transformations in the contemporary strategic environment do not diminish the importance of international law, but rather enhance its relevance. In a world characterised by technological competition, economic interdependence and global infrastructure, international law remains the indispensable framework for limiting the use of force, protecting individuals and facilitating cooperation between states. At the same time, new challenges call for doctrinal and normative developments aimed at strengthening resilience, protecting critical infrastructure and regulating emerging technologies.

Viewed from this perspective, international law is not merely a set of rules applicable in times of crisis, but an essential component of the global security architecture and a determining factor in the stability of the international system in the 21st century.

Table 18. Summary of strategic conclusions

Area	Main conclusion	Strategic priority
Geopolitics	Multipolarity intensifies competition	Very high
Conflicts	Persistence of regional conflicts	Very high
Energy	Diversification is essential	High
Critical infrastructure	Requires integrated protection	Very high
Maritime security	Freedom of navigation is vital	High
Technology	AI is redefining security	Very high
International law	Adaptation of regulations is required	High
International cooperation	Remains essential for stability	Very high
Resilience	Is becoming the central concept of security	Critical
Strategic analysis	Anticipation must take precedence over reaction	Criticism

FINAL CONCLUSIONS

This paper has sought to analyse the profound transformations that global security is undergoing in the first half of the 21st century, within a context characterised by intensified strategic competition, technological acceleration, unprecedented economic and energy interdependencies, and the proliferation of actors capable of influencing international stability. The analysis has demonstrated that the contemporary security environment can no longer be understood through traditional models, built exclusively around power relations between states and the use of military force. On the contrary, global security must be interpreted as the result of the interaction between complex systems, within which the military, economic, energy, technological, legal, informational and societal dimensions are deeply interconnected.

One of the fundamental conclusions of the research is that the international order is undergoing a period of structural reconfiguration. The war in Ukraine, developments in the Middle East, strategic competition in the Indo-Pacific region, the intensification of cyber threats and the accelerated development of artificial intelligence are not independent phenomena, but expressions of a systemic transformation that is simultaneously altering the nature of conflicts, the distribution of power and the mechanisms of international governance. In this context, the traditional distinction between peace and war is becoming increasingly difficult to define, and strategic competition is taking place on an ongoing basis, through the integrated use of military, economic, informational, legal and technological instruments.

The research highlights the fact that critical infrastructure has become one of the main focal points of international security. Energy networks, seaports, pipelines, submarine cables, communications systems, digital platforms and logistics infrastructure are indispensable to the functioning of the global economy and, at the same time, priority targets of geopolitical competition. Their vulnerability has effects that transcend national borders and influence regional and global security. Consequently, the protection of critical infrastructure must be approached as a shared responsibility, underpinned by international cooperation, information sharing and the strengthening of institutional resilience.

This paper demonstrates that energy security and maritime security are inseparable dimensions of international stability. Recent developments have confirmed the decisive role of

major maritime routes and energy infrastructure in the functioning of the global economy, as well as the major impact that their disruption can have on financial markets, supply chains and food security. Equally, the energy transition is redefining strategic competition through the focus on critical minerals, clean technologies and the new infrastructure required for a low-carbon economy.

Another important finding of the research concerns the role of emerging technologies in transforming international security. Artificial intelligence, autonomous systems, big data analytics, quantum communications and the digitalisation of critical infrastructure are changing both the decision-making process and the nature of military and civilian operations. These developments create significant opportunities for increasing efficiency and anticipating risks, but they also give rise to legal and ethical challenges concerning accountability, human control and the protection of fundamental rights. In this regard, technological development must be accompanied by the strengthening of international governance and the gradual adaptation of international law to the new realities.

From a legal perspective, the analysis confirms that international law retains its central role in organising relations between states, but is subject to a continuous process of adaptation. The established norms concerning the prohibition of the use of force, international humanitarian law, the law of the sea and state responsibility continue to form the foundation of the international order. At the same time, the new challenges posed by cyber operations, artificial intelligence, critical infrastructure and autonomous technologies necessitate the development of legal interpretations and mechanisms capable of responding to a rapidly changing strategic environment.

The main contribution of this paper lies in proposing a systemic perspective on global security. Rather than a sectoral approach focused exclusively on armed conflicts or geopolitical competition, the research promotes an integrated model in which security is analysed in relation to the functioning of the international system and the interdependencies between its main components. Within this conceptual framework, analytical models such as **the Global Security Brief**, **the Global Escalation Index**, **Critical Infrastructure Watch**, **the Early Warning Framework** and the concept of **Strategic Gravity** have been developed; these are tools designed for the integrated monitoring and assessment of global risks.

The proposed model is based on the idea that international stability does not depend solely on the military balance between the major powers, but also on the continuity of the energy, trade, information and technology flows that underpin the functioning of the global economy. From this perspective, the centres of strategic gravity are represented by infrastructures, technologies and regions whose disruption has systemic effects on the entire international environment. This approach provides an additional explanatory framework for understanding the rapid spread of contemporary crises and for underpinning policies geared towards prevention and anticipation.

The paper argues that resilience must become the central concept of modern security policies. In an international system characterised by uncertainty and multiple interdependencies, security can no longer be defined exclusively by military defence capability, but by the ability of societies and institutions to anticipate, absorb and overcome the effects of complex crises. Strengthening resilience requires investment in critical infrastructure, the development of effective early-warning mechanisms, the diversification of energy sources, the protection of cyberspace and the strengthening of international cooperation.

Looking ahead, the international strategic environment is likely to remain characterised by intense geopolitical competition, rapid technological change and the emergence of increasingly complex risks. However, research shows that a slide towards global confrontation is not inevitable. The international community's ability to adapt existing institutions, strengthen multilateral cooperation and develop legal norms compatible with the new technological realities can contribute significantly to mitigating risks and maintaining the stability of the international system.

In conclusion, global security in the 21st century must be understood as a dynamic process of managing interdependencies and systemic vulnerabilities, in which prevention, anticipation and resilience take on an importance comparable to that of military deterrence and collective defence. Only through an interdisciplinary, integrated and forward-looking approach will it be possible to

formulate public policies and cooperation mechanisms capable of responding to the challenges of an international order undergoing profound transformation.

From this perspective, this paper does not aim to provide definitive answers, but rather to contribute to the development of an analytical paradigm adapted to the realities of the 21st century. The complexity of the strategic environment requires moving beyond fragmented approaches and developing tools capable of integrating the geopolitical, economic, energy, technological and legal dimensions into a coherent model of analysis and anticipation. This represents, in the author's view, one of the key directions for the evolution of security studies in the coming decades and for the consolidation of an international order that is more resilient, more cooperative and better prepared to manage the challenges of the future.

SELECTED BIBLIOGRAPHY

I. International organisations and official documents

1. European Commission. 2020. *EU Security Union Strategy 2020–2025*. Brussels.
2. European Commission. 2023. *European Economic Security Strategy*. Brussels.
3. European Council. 2022. *A Strategic Compass for Security and Defence*. Brussels.
4. International Maritime Organisation (IMO). *Annual Report 2024*. London.
5. NATO. 2022. *NATO Strategic Concept*. Madrid.
6. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.
7. Organisation for Security and Co-operation in Europe (OSCE). *Annual Report 2024*. Vienna.
8. United Nations. 1945. *Charter of the United Nations*.
9. United Nations. 1982. *United Nations Convention on the Law of the Sea (UNCLOS).*
10. United Nations Development Programme (UNDP). *Human Development Report 2025*. New York.
11. United Nations Office for Disaster Risk Reduction (UNDRR). *Global Assessment Report on Disaster Risk Reduction 2025*.
12. United Nations Security Council. *Reports of the Secretary-General on the Protection of Critical Infrastructure*. New York.
13. World Bank. *World Development Report 2025*. Washington, D.C.
14. World Economic Forum. 2025. *Global Risks Report 2025*. Geneva.

II. International research institutes

1. Brookings Institution. *Annual Report 2024*. Washington, D.C.
2. Centre for Strategic and International Studies (CSIS). *Critical Minerals Security Programme Reports*. Washington, D.C.
3. Chatham House. *The World Today*. London.
4. International Institute for Strategic Studies (IISS). 2025. *The Military Balance 2025*. London: Routledge.
5. International Institute for Strategic Studies (IISS). *Strategic Survey 2024*. London.
6. RAND Corporation. *National Security Research Reports*. Santa Monica.
7. Stockholm International Peace Research Institute (SIPRI). 2025. *SIPRI Yearbook 2025: Armaments, Disarmament and International Security*. Oxford University Press.

8. SIPRI. *Military Expenditure Database*.
9. German Marshall Fund. *Geostrategy Reports*.
10. Atlantic Council. *Global Strategy Papers*.
11. Carnegie Endowment for International Peace. *Strategic Europe*.

III. Key academic literature

1. Allison, Graham. 2017. *Destined for War: Can America and China Escape Thucydides's Trap?* Boston: Houghton Mifflin Harcourt.
2. Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.
3. Buzan, Barry. 1983. *People, States and Fear*. Brighton: Harvester Press.
4. Clausewitz, Carl von. 1976. *On War*. Edited by Michael Howard and Peter Paret. Princeton University Press.
5. Freedman, Lawrence. 2013. *Strategy: A History*. Oxford University Press.
6. Gray, Colin S. 2015. *The Strategy Bridge*. Oxford University Press.
7. Kaplan, Robert D. 2012. *The Revenge of Geography*. Random House.
8. Keohane, Robert O., and Joseph S. Nye. 2012. *Power and Interdependence*. 4th ed. Pearson.
9. Kissinger, Henry. 2014. **World Order**. Penguin Press.
10. Mearsheimer, John J. 2014. **The Tragedy of Great Power Politics**. Updated ed. W. W. Norton.
11. Nye, Joseph S. 2004. **Soft Power**. PublicAffairs.
12. Nye, Joseph S. 2011. *The Future of Power*. PublicAffairs.
13. Waltz, Kenneth N. 1979. *Theory of International Politics*. Addison-Wesley.
14. Allison, Graham, and Philip Zelikow. 1999. **Essence of Decision**. Longman.
15. Kaldor, Mary. 2012. *New and Old Wars*. Stanford University Press.

IV. Energy, critical infrastructure and security

1. International Energy Agency (IEA). *World Energy Outlook 2024*. Paris.
2. Energy Agency. *Energy Security Review 2025*.
3. International Renewable Energy Agency (IRENA). *World Energy Transitions Outlook 2025*.
4. European Union Agency for Cybersecurity (ENISA). *Threat Landscape Report 2024*.
5. *Global Infrastructure Outlook*.
6. OECD. *Economic Outlook 2025*.
7. World Trade Organisation (WTO). *World Trade Report 2024*.
8. International Chamber of Shipping. *Annual Review 2025*.
9. Lloyd's List Intelligence. *Maritime Risk Reports*.
10. BIMCO. *Shipping Market Review*.

V. Artificial Intelligence and Cyber Security

1. National Institute of Standards and Technology (NIST). 2024. *AI Risk Management Framework*.
2. OECD. 2024. *OECD Framework for Artificial Intelligence Governance*.
3. UNESCO. 2021. *Recommendation on the Ethics of Artificial Intelligence*.
4. OpenAI. *Governance of Advanced Artificial Intelligence Systems*. Policy Papers.
5. Microsoft. *Digital Defence Report 2024*.
6. Google Threat Intelligence Group. *Annual Cybersecurity Report*.

7. ENISA. *Cybersecurity Threat Landscape*.
8. World Economic Forum. *Global Cybersecurity Outlook 2025*.

VI. International Law and Global Governance

1. Crawford, James. 2019. *Brownlie's Principles of Public International Law*. 9th ed. Oxford University Press.
2. Shaw, Malcolm N. 2021. *International Law*. 9th ed. Cambridge University Press.
3. Orakhelashvili, Alexander. 2022. *Akehurst's Modern Introduction to International Law*. Routledge.
4. Dinstein, Yoram. 2021. *War, Aggression and Self-Defence*. Cambridge University Press.
5. Schmitt, Michael N., ed. 2017. *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
6. International Law Commission. *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*.

VII. Statistical sources and databases

1. ACLED (Armed Conflict Location & Event Data Project).
2. SIPRI Military Expenditure Database.
3. IMF Data.
4. World Bank Open Data.
5. UN Comtrade Database.
6. MarineTraffic Global Shipping Database.
7. International Energy Agency Statistics.
8. NATO Open Source Assessments.
9. Eurostat.
10. UNCTAD Maritime Transport Statistics.
11. FAOSTAT.

ANNEX 1 – ABBREVIATIONS

- ACLED – Armed Conflict Location & Event Data Project
- IISS – International Institute for Strategic Studies
- IMO – International Maritime Organisation
- IMF – International Monetary Fund
- NATO – North Atlantic Treaty Organisation
- OSCE **LIST** – Organisation for Security and Co-operation in Europe
- OSINT – Open Source Intelligence
- RAND – RAND Corporation
- SIPRI – Stockholm International Peace Research Institute
- UN – United Nations
- UNCLOS – United Nations Convention on the Law of the Sea
- UNDP – United Nations Development Programme
- WEF – World Economic Forum
- AI – Artificial Intelligence
- CCDCOE – Cooperative Cyber Defence Centre of Excellence
- CSIS – Centre for Strategic and International Studies

- ENISA – European Union Agency for Cybersecurity
- EU – European Union
- IAEA – International Atomic Energy Agency
- IEA – International Energy Agency
- WTO – World Trade Organisation