PUBLIC GOODS AND PUBLIC POLICIES IN THE FIELD OF SECURITY: THE INTERSECTION BETWEEN ECONOMY AND DEFENCE STRATEGY IN THE CONTEXT OF CONTEMPORARY TRANSFORMATIONS

Major Daniel-Dorin CUCURĂ

The 405th Logistic Support Battalion "Năsăud",
Doctoral Student at The Doctoral School of Administrationand Public Policies,
Faculty of Political, Administrative and Communication Sciences,
"Babeș-Bolyai" University, Cluj-Napoca
DOI: 10.55535/RMT.2025.3.35

This article examines security as a national and global public good, positioning it at the intersection between the economy and defence strategy. The central objective is to analyse how economic resources and available infrastructures shape military capabilities and, conversely, how defence strategies sustain the stability required for economic development. Methodologically, the research combines a theoretical analysis of the specialised literature on public goods and public policies with an applied examination of the contemporary context, including the COVID-19 pandemic and the conflict in Ukraine. The findings show that security goes beyond its traditional military dimension, encompassing health, energy, cyber and societal aspects, which assigns public administration the role of orchestrator of resources and international cooperation. The case studies confirm that investments in defence, resilience and emerging technologies contribute simultaneously to security and economic development.

The contribution of this paper lies in articulating an integrated perspective on security as a public good, supported by coherent public policies and international partnerships. The conclusions and recommendations target decision-makers and practitioners in public administration and security, suggesting directions for governance adapted to contemporary transformations.

Keywords: national security; public goods; public policy; military strategy; economy and defence;

INTRODUCTION

The accelerated transformations of the international security environment over the past decades have profoundly redefined how states and international organisations understandand manage security issues. Emerging technologies – from artificial intelligence to autonomous systems and biotechnologies – together with geopolitical changes and recent global crises have extended the concept of security beyond the strictly military dimension. Security must therefore be regarded as a fundamental public good that encompasses health, energy, cyber and social dimensions. Public administrationis at the core of this process, tasked with ensuring policy coherence, allocating resources and stimulating inter-institutional and international cooperation.

Starting from the premise that security is inseparably linked to the economy, this study aims to highlight the interdependence between economic resources and available infrastructures on the one hand and military strategies on the other. Financial resources, critical infrastructures, human capital and innovation capacity define the possibilities and limitations of building defence capabilities. Conversely, internal and external security and stability generate the conditions necessary for investment, trade and sustainable development. The COVID-19 pandemic and the conflict in Ukraine have clearly shown that economic and social vulnerabilities rapidly turn into security risks and that a lack of effective coordination can amplify their impact.

The paper proposes a dual approach: on the one hand, from a theoretical perspective, security is addressed through the lens of public good sand public policy theories, with an emphasis on its characteristics of non-excludability and non-rivalry; on the other hand, the applied part focuses on how the economy directly influences contemporary military strategies, illustrated by relevant case studies on Romania, NATO, the EU and global implications. The article ends with a set of conclusions and recommendations designed to provide useful benchmarks for decision-makers in public administration structures to adapt governance to the challenges of contemporary transformations.

In light of these considerations, a solid theoretical foundation is needed to explain how security can be conceptualised as a public good and toout line the public policy instruments through which it isprovided.

The pace of change in the security environment has accelerated significantly in the last decade, driven by the convergence of technological progress (artificial intelligence, automation, biotechnologies), geopolitical shifts (redistribution of power, the return of great-power competition) and systemic crises (COVID-19, the conflict in Ukraine). The *"new revolution in military affairs"* is no longer merely technological but also organisational, doctrinal and social, requiring a reconfiguration of the role of public administration in managing security as a public good.

Against this background, the emphasis falls on governance, on the ability of public institutions to coordinate resources, on cooperation within alliances and on societal resilience. Equally important is the integration of cyber, energy and health dimensions into the broader concept of security, moving beyond the strictly military logic. National and international securityis a public good with properties of non-excludability and non-rivalry (Samuelson, 1954), which has two main consequences for public administration:

- *(I) the state becomes the provider of last resort of security;*
- *(II) inter-institutional and international coordination is indispensable for managing externalities and cross-border risks.*

Public policies in the field of security must balance allocative efficiency with democratic legitimacy and the protection of rights. In this context, the emphasisis on governance, on the capacity of public institutions to coordinate resources, on cooperation in alliances and on societal resilience. It is equally essential to integrate cyber, energy and health dimensions into the broad concept of security, moving beyond the strictly military logic.

The paper investigates the intersection between the economy and defence strategy: how economic resources and available infrastructures condition strategic options, and how strategic choices shape the economic structure and development trajectory. Methodologically, we adopt a dual approach consisting of a theoretical framework (public goods, public policies, political economy of security) and an applied analysis with case studies (Romania, NATO, EU, lessons from the pandemic and the conflict in Ukraine), integrating comparative and institutional perspectives.

PUBLIC GOODS AND PUBLIC POLICIES IN THE FIELD OF SECURITY

The theoretical analysis of security as a public good starts from the fundamental concepts formulated in the specialised literature. Public goods are defined by their characteristics of non-excludability and non-rivalry, as emphasised by Samuelson (1954) and later developed by Musgrave (1959). This category includes goods which, once provided, can not exclude beneficiaries, and whose use by one individual does

not reduce availability for others. National security corresponds to this pattern, since the protection provided by the state is felt by all citizens regardless of their individual contribution.

Subsequent developments have nuanced this perspective by introducing notions such as club goods (Buchanan, 1965), which are excludable but non-rival upto a certain congestion threshold, and common-pool goods (Ostrom, 1990), characterised by open access but at risk of over use. More recently, the concept of global public goods (Kaul et al., 2003) has offered a useful framework for understanding security at the transnational level, where threats such as international terrorism, climate change or financial instability can not be managed exclusively by a single state.

A central element of the theoretical debate is the *"free rider"* problem, analysed by Olson (1965). This explains the tendency of actors to underfund public goods while benefiting from the contributions of others. In the security field, the phenomenon is visible in alliances, where fair burden-sharing represents a constant challenge. Institutional mechanisms and international norms play a role in limiting opportunistic behaviour and ensuring the cooperation needed for the provision of collective security.

With regard to public policies, they follow a specific cycle: problem identification, formulation of solutions, implementation of measures and evaluation of results. The classical model of the policy cycle (Dunn, 2017) has been adapted in the security field through the integration of risk management and resilience. Thus, public administration structures must be able to rapidly identify new types of threats, formulate effective responses, mobilise resources and evaluate the impact of implemented policies. All these stages require a high degree of coordination between national institutions and international partners.

The ethics of security constitutes another essential dimension of the theoretical framework. The provision of security can not be separated from respect for the rule of lawand the fundamental rights of citizens. Civilian control over the armed forces, decision-making transparency and institutional accountability are indispensable conditions for the democratic legitimacy of security policies. Security is the refore not only a technical objective but also a deeply political and normative one.

Overall, the theoretical framework presented demonstrates that security needs to be viewed as a complex public good, located at the intersection of economic needs, strategic imperatives and ethical constraints. These theoretical foundations form the basis for the applied analysis in the next chapter, where the interaction between the economy and defence strategy is detailed through case studies and practical examples.

The Theory of Public Goods: Definitions and Extensions

The concept of the public good has become a fundamental benchmark of modern economic theory. In its classical form, developed by Paul Samuelson (1954) and further elaborated by Richard Musgrave (1959), public goods are those goods or services simultaneously characterised by **non-excludability** and **non-rivalry**. Non-excludability means that, once the good is provided, it is not possible – or is very costly – to exclude certain individuals from consuming it. Non-rivalry implies that the use of the good by one individual does not diminish its availability for other members of the community. Classic examples include street lighting, national defence or floodprotection.

Later literature has refined this category. Buchanan (1965) introduced the concept of **club goods**, that is, goods which are in principle non-rival but to which access can be restricted to members of a group paying a fee (such as toll motorways or cable networks). He showed that, through voluntary association, individuals can share the costs of providing a non-rival good and limit accesstoavoidcongestion.

Elinor Ostrom (1990), on the other hand, emphasised **common-pool resources** – resources characterised by rivalry but difficult to exclude, such as forests, fishing grounds or underground water. She demonstrated that, in the absence of collective management, these resources can be over used, a phenomenon known as the *"tragedy of thecommons".*

Finally, Kauland colleagues (2003) extended the perspective by introducing the notion of global public goods to designate those goods whose benefits and costs transcend state borders. Relevant examples include climate stability, international financial security or the fight against global terrorism. This extension underlines that the provision of global public goods requires international cooperation and robust multilateral institutions.

Within this theoretical framework, **security** emerges as a complex and particular example. At the national level, defence and public order can be considered pure public goods, since the protection offered by the state extends to all citizens without discrimination and without additional marginal costs per beneficiary. However, as threats become transnational – international terrorism, cyber-attacks, the proliferation of weapons of mass destruction – security takes on the features of a **global public good**, whose effective provision depends on cooperation between states, military alliances and international institutions.

Thus, the theory of public goods provides not only a conceptual framework for understanding security but also an argument for public policies aimed at sharing responsibilities and resources between national and international actors.

This approach lays the groundwork for the in-depth analysis of the relationship between economy and defence strategy in the following chapters.

The Free Rider Problem and Collective Governance

One of the best-known obstacles to the efficient provision of public goods is the ***"free rider"* problem** theorised by Mancur Olson (1965). This describes the tendency of actors – whether individuals, organisations or states – to benefit from a public good without contributing proportionally to its costs. Because public goods are characterised by non-excludability, each participant has an incentive to reduce their own contribution, hoping that others will cover the costs while they enjoy the benefits free of charge. The result, in the absence of corrective mechanisms, is underfunding and insufficient provision of the good in question.

In the field of international security, the free rider problem is particularly evident in **military alliances**. Mechanisms such as NATO involve burden sharing among members for financing common capabilities, participating in operations and maintaining interoperability. In practice, however, some states tend to contribute less than others, relying on the protection offered by stronger allies. This asymmetry creates political tensions and can undermine the cohesion of the alliance in the long term, especially when costs increase or threats diversify.

Collective governance thus emerges as a necessary response to limit opportunistic behaviour. It relies on **rules, norms and institutions** that establish mutual expectations, define contribution criteria and provide monitoring and sanctioning mechanisms. In NATO, for example, the agreed target of allocating 2% of GDP to defence functions as a shared norm, intended to encourage convergence of efforts and reduce the free-riding phenomenon. Transparent reporting of expenditure, periodic capability assessments and integrated planning also contribute to holding member states accountable.

Beyond military alliances, collective governance also encompasses **multilateral institutions and international agreements** managing global public goods, such as non-proliferation regimes or cooperation in the cyber domain. Establishing common standards, verification procedures and mutual support mechanisms helps to create an atmosphere of trust and reduce opportunistic behaviours.

Thus, the free rider problem and collective governance solutions are inseparable in analysing security as a public good. They explain why the mere existence of a common interest is not sufficient for cooperation and why institutions, rules and norms are essential for the effective provision of security at national, regional and global levels. This perspective sets the stage for the discussion of concrete

instruments through which public administrations can stimulate equitable participation and ensure the sustainability of alliances and partnerships in the field of security.

Public Policies: The PolicyCycleandInstruments

The analysis of security as a public good can not be complete without a clear understanding of **the process of designing and implementing public policies**. The classical model of the policy cycle, described by Dunn (2017), offers a useful conceptual framework for capturing decision-making dynamics. This model identifies four main stages – *problem definition, policy formulation, implementation* and *evaluation* – which, although presented sequentially, in practice overlap, recur and are continually adjusted. In the field of security, this flexibility is essential because the strategic environment is marked by uncertainty, rapid change and the emergence of new threats.

The first stage, **problem definition**, involves recognising and precisely delineating the risks and vulnerabilities that affect national or international security. At this stage, public administration must mobilise multidisciplinary expertise and consult relevant actors in order to understand the root causes of threats. Without proper diagnosis, policies risk being reactive and ineffective.

The second stage, **policy formulation**, entails the development of response options and the selection of appropriate instruments. Here institutional creativity comes into play and the ability to combine different types of tools: regulation, taxation, subsidies, contracting, public-private partnerships or direct investment in capabilities. In the security domain, instruments can include the elaboration of doctrines and strategies, capability planning, procurement and modernization programmes, as well as measures of international cooperation, strategic education or public communication to strengthen societal support.

The third stage, **implementation**, turns political decisions into concrete actions. This requires interinstitutional coordination, efficient resource management and continuous progress monitoring. In security, implementation is reflected in the conduct of military exercises, the commissioning of critical infrastructure, the completion of procurement processes or the operation of training and strategic education programmes.

Finally, **policy evaluation** plays the role of measuring the efficiency, effectiveness and impact of actions undertaken. It provides feedback for the adjustment of future decisions and contributes to institutional learning. In the security field, evaluation may take the form of capability audits, after-action reviews or periodic reports to national and international bodies.

Throughout this cycle, **the choice of instruments** is very important. There is no universal set of tools suitable for all situations; public administration must adapt the policy mix according to the nature of the threat, the resources available and the international framework. In the case of security, this may mean combining investments in emerging technologies with strengthening public-private partnerships, reinforcing the regulatory framework and developing a strategic culture among personnel and the wider population.

Thus, the policy cycle model and the diversity of available instruments provide an essential framework for the governance of security as a public good. They show that the success of policies depends not only on the formulation of ambitious objectives but also on rigorous implementation, continuous adaptation to changes in the strategic environment and ongoing evaluation of results.

Public Administration and Risk Management

In the context of accelerated transformations and complex threats, public administration faces a reality characterized by uncertainty, volatility and multiple interdependencies. Traditionally, public institutions were mainly oriented toward linear planning and responding to predictable events. At present, however, this approachis no longer sufficient. Risk and **resilience management** are becoming central tools for prioritizing interventions and allocating resources efficiently in the face of diverse and often unpredictable threats.

Risk management involves identifying, assessing and addressing potential hazards before they materialize. In the security field, this process covers not only traditional military risks but also those associated with public health, cybersecurity and energy. Integrated management of these risks allows proactive planning, reduction of vulnerabilities and the creation of rapid response mechanisms. At the same time, resilience complements risk management: it refers to the ability of public and private systems to absorb shocks, adaptand return to normal functioning after a disruption.

In this context, ***"all-hazards"*** models are attracting increasing attention. These propose an integrated approach to all types of risks, regardless of their source, avoiding fragmentation by sector or agency. Through this model, public administration develops standardized plans and procedures applicable to a wide range of emergency situations, whether pandemics, cyberattacks or natural disasters. A major advantage of the *"all-hazards"* approach is efficiency: instead of preparing separate plans for each type of risk, institutions build versatile capabilities adaptable to multiple scenarios.

In parallel, the ***"whole-of-government/whole-of-society"*** model reflects the need for interinstitutional coordination and the active involvement of all societal actors. *"Whole-of-government"* entails close collaboration between different ministries and governmental agencies, over coming traditional institutionals. *"Whole-of-society"* extends this logic by involving the private sector, non-governmental organizations, academia and citizens in the development and implementation of security policies. This model recognizes that, in the face of complex threats –from cyber attacks to energy and health crises – no single actor possesses all the necessary resources and expertise.

Applying these models in public administration has direct consequences for **national security policies**. For example, integrating health, cyber and energy security into a coherent strategy requires coordination mechanisms, information sharing and joint exercises between institutions. At the same time, risk management must be accompanied by strategic communication and public education so that citizens understand the measures taken and contribute to collective resilience.

Therefore, public administration becomes not only a provider of services, but also an orchestrator of a **national security ecosystem** in which the public sector, private sector and civil society collaborate to prevent and manage risks. Risk and resilience management, applied with in the *"all-hazards"* and *"whole-of-government/whole-of-society"* frameworks, represents an indispensable pillar of modern security policies.

Ethics of Security and Democratic Legitimacy

In a democratic society, **the provision of security** can not be separated from respect for the rule of law and the protection of fundamental civil rights. Although the need for protection against internal and external threats may lead governments to adopt firm measures, these measures must be designed and implemented in ways compatible with democratic principles. Transparency, accountability and civilian control over the armed forces constitute the pillars of legitimacy. Their absence can lead to abuses of power, loss of public trust and even the under mining of long-term security.

Transparency in the field of security implies clear communication of objectives, budgets and policy results in a manner that does not compromise sensitive aspects but that gives citizens and their representatives the ability to understand and evaluate the actions taken. **Accountability** requires mechanisms through which decision-makers and institutions are held responsible for errors or abuses, including through audits, public reports or independent investigations. **Civilian control** over the armed forces represents a fundamental guarantee of democracy: the military

and security structures must serve the interests of society under the authority of elected leaders, rather than be coming an autonomous actor in the political process.

However, security policies often involve sensitive information, discreet operations and plans that can not be made public without affecting their effectiveness. **The challenge of democratic governance** lies precisely in finding a balance between the **necessity of secrecy** – indispensable for protecting operations and sources – and the **democratic requirements of oversight and control**. The experience of mature democracies shows that this balance can be achieved through independent oversight institutions, specialised parliamentary committees, regular public reporting and a culture of integrity within security institutions.

This ethical approachis also relevant for **extending the concept of security** beyond the military domain. While national defence, public order and civil protection can be onsidered pure public goods provided by the state, areas such as cyber, energy, health or food security have the features of mixed goods, requiring the involvement of the private sector and civil society. At the global level, phenomena such as climate change, international terrorism or financial instability represent global public goods whose efficient provision depends on the cooperation of international institutions such as NATO, the European Union or the United Nations.

Thus, we can outline a **conceptual framework** that reflects this diversity: national security (pure public good) encompasses defence, public order and civil protection; extended security (mixed goods) includes areas such as cyber, energy, health and food; global security (global public good) refers to climate, international terrorism and financial stability. The instruments through which these levels are managed range from public policies and budgetary resources to mechanisms of cooperation and institutional partnerships.

Finally, the **theoretical foundations** presented in this first chapter provide an interpretative framework necessary for analysing the practical dimensions of security. They show that moving from conceptualisation to reality involves observing how economic resources and available infrastructures shape defence strategies, and how recent transformations – such as the COVID-19 pandemic or the conflict in Ukraine – have shaped security policies. The next chapter illustrates these relationships through relevant examples and case studies, preparing the ground for public policy recommendations.

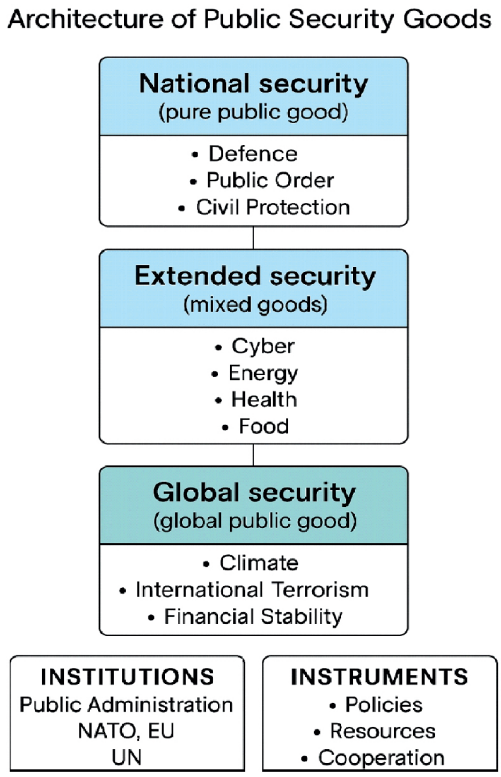

Figure 1: Architecture of Public Security Goods

As shown in *Table 1*, the types of public goods relevant to security can be described in a continuous manner so as to highlight the transition from the national to the global level and the nature of the instruments used.

Table 1: Types of Public Goods Relevant for Security

Type	Characteristics	Examples in Security	Policy Implications
Pure public good	Non-excludable, non-rival	Territorial defence	Collective budgetary funding
Global public good	Transnational	Climate stability, counterterrorism	International cooperation
Club good	Excludable, non-rival until congestion	Common capabilities in an alliance	Contributions and access rules
Common-pool good	Non-excludable, rival	Electromagnetic space, spectrum	Usage rules, monitoring

At the **national level**, security is structured around pure public goods provided by the state: defence, public order and civil protection. These areas are non-excludable and non-rival: the protection offered by the army, police or emergency services extends to the entire population regardless of individual contribution. Public administration is responsible for planning, financing and coordinating these functions, there by ensuring a minimum guaranteed level of security for all citizens.

As the concept of security **expands**, domains with the characteristics of mixed goods emerge, where effective provision requires collaboration between the public and private sectors. Cybersecurity, energy security, public health and food security are relevant examples. In these cases, non-excludability is no longer absolute, and rivalry may arise under conditions of crisis or overload. Therefore, governance is based on public-private partnerships, regulation, common standards and coordinated investments to maintain access to and the functionality of these essential goods.

At the **global level**, security takes on the haracteristics of a global public good. Phenomena such as climate change, international terrorism or financial instability can not be effectively managed by a single state. They simultaneously affect multiple regions and generations and require sustained multilateral cooperation. International institutions – NATO, the European Union and the United Nations – become platforms through which states coordinate their policies, mobilise resources and create common norms for the provision of these global goods. The instruments used range from treaties and international agreements to joint programmes, pooled funding and stabilisation missions.

This narrative presentation allows a gradual understanding of the types of public goods relevant to security, highlighting the continuity between the national, extended and global levels and clarifying the role of public administration and international institutions in their provision.

The Relationship between Public Administration and National/International Security

Public administration represents the institutional infrastructure through which the state exercises its essential functions, including the provision of security as a public good. At the national level, the administration plays the role of designing policies, mobilising resources and coordinating the institutions responsible for defence, public order and civil protection. This role is not purely technical but involves making strategic decisions that affect the balance between freedom and security, transparency and secrecy, and social costs and benefits (Rothstein, 2011).

In a consolidated democracy, public administration acts as an **intermediary between political decision-makers and citizens**, ensuring that security policies reflect both public will and the international commitments undertaken by the state. It is responsible for formulating national defence strategies, managing risks and implementing international standards. For example, in Romania, the Ministry of National Defence and the Ministry of Internal Affairs act on the basis of government plans approved by Parliament and coordinated with NATO and EU strategies (Government of Romania, 2022).

At the international level, **security can no longer be provided unilaterally**. Transnational threats – terrorism, organised crime, cyberattacks, climate change – require cooperation between states and institutions. National administrations thus become key actors in **global governance networks**, contributing data, expertise and resources to collective security mechanisms (Keohane, Nye, 2001). Participation in organisations such as NATO, the European Union or the United Nations involves not only assuming formal obligations but also adapting internal administrative structures to cooperate effectively with external partners.

This bidirectional relationship between public administration and national/international security entails a series of challenges. First, **resource allocation**: administrations must balance defence expenditure with domestic social and economic needs. Second, **inter-institutional coordination**: modern security covers multiple dimensions – military, economic, health, cyber – that require collaboration between ministries, agencies and the private sector. Third, **democratic legitimacy**: the involvement of the administration in international security mechanisms must be transparent and comply with the rule of law and parliamentary oversight (Born et al., 2003).

Therefore, public administration is not merely an executor of political decisions in security matters but a **strategic actor** that shapes defence policy, coordinates the implementation of international obligations and mediates the relationship between state and citizen. In the context of contemporary transformations, the success of security policies depends on the capacity of administrations to integrate national and international perspectives, anticipate risks and build systemic resilience through coherent policies and durable partnerships.

ECONOMY AND MILITARY STRATEGY IN THE CONTEMPORARY CONTEXT

Where as the first chapter provided the theoretical framework of security as a public good and the instruments through which it can be delivered, this chapter focuses on the **practical dimensions** of the interaction between the economy and military strategy. In the 21st century, economic resources are no longer merely the basis for financing military capabilities but have become a strategic element in their own right, directly influencing national resilience and the cohesion of international alliances.

This section analyses several complementary directions: **economic resources as the foundation of military power**; budgetary policies and NATO's **2% of GDP** defence spending benchmark; and the transformative effects of recent crises. **The COVID-19 pandemic** highlighted systemic vulnerabilities and redefined population health as a strategic element, while the **conflict in Ukraine** brought to the forefront issues of energy security, logistics and doctrinal adaptation. It will also address the **interdependence between the economy and military strategy**, investments in technology, the defence industry and digitalisation, as well as the **role of the European Union and NATO** in managing security-related public goods.

Through this approach, the chapter offers an integrated picture of how current economic realities and geopolitical challenges shape defence strategies and security governance in Romania, in the Euro-Atlantic space and globally.

Economic Resources as the Foundation of Military Power

A state's ability to build, maintain and modernise its armed forces fundamentally depends on the **economic resources** it can mobilise. Since the classic works of international relations, military power has been considered inseparable from economic power, which provides the material basis for financing equipment, training personnel, technological development and the logistical support of operations (Kennedy, 1987). A state with a solid economy can allocate more consistent resources to defence without compromising social welfare, thereby increasing both its deterrence capacity and its resilience to crises.

Traditionally, the **defence budget** reflects a state's strategic priorities and the extent to which it can transform economic potential into military power. NATO states agreed at the 2014 Wales Summit to allocate at least **2% of GDP** to defence by 2024, precisely to ensure the sustainability of collective capabilities (NATO, 2023). This target is not merely an accounting indicator but also a political signal of the willingness to contribute to common security and to avoid the

"free rider" phenomenon described by Olson (1965). Romania, for example, has managed to reach and maintain this level of funding since 2017, which has allowed the accelerated modernisation of its armed forces and more active participation in international missions (Government of Romania, 2022).

Economic resources, however, are not limited to annual budgets. **The structure of the economy** and its **critical infrastructures** directly influence mobilisation capacity in times of crisis. A diversified industrial base, robust supply chains and a skilled workforce enable the rapid production of necessary equipment and long-term logistical support. Lessons from the two World Wars show that states capable of converting civilian industries into war industries held a decisive advantage (Tooze, 2006). Today, this logic underpins the emphasis on **dual-use capabilities** and on public-private partnerships for the development of technologies with simultaneous civilian and military applications (Edwards, 2018).

At the same time, **macroeconomic stability** is a prerequisite for sustainable defence financing. Excessive budget deficits or financial crises can drastically reduce available resources and limit investments in strategic capabilities. The COVID-19 pandemic highlighted this vulnerability: massive spending on public health and economic support competed with defence allocations, while supply-chain disruptions affected military procurement programmes (SIPRI, 2021). These developments confirm that economic resilience is an integral part of national resilience.

Economic resources also form the basis for **investment in research and development**. In the age of emerging technologies – artificial intelligence, autonomous drones, biotechnology, cyber security – military competitiveness depends on states' ability to finance innovation and integrate results into doctrine and equipment (Gilli, Gilli, 2019). Countries with dynamic technological ecosystems and institutions that facilitate collaboration between universities, industry and the armed forces are better positioned to maintain their strategic advantage.

Finally, economic resources have a **geopolitical** dimension. States with large economies can use aid, credits and investments to build alliances, support partners and project stability in key regions. The financial and logistical support provided to Ukraine by NATO and EU states after 2022 illustrates how collective economic power can be transformed into strategic effect, strengthening the defence of a third state and deterring aggression (European Council, 2023).

Therefore, economic resources are not just a contextual factor but a **structural foundation of military power.** Public administrations must manage this relationship in an integrated manner, balancing domestic social needs with security commitments,

and short-term spending with long-term capability development. The ability to mobilise economic resources efficiently ultimately makes the difference between a declarative defence strategy and a credible one.

Budgetary Policies and National Defence (the Example of 2% of GDP for NATO)

Budgetary policies in the field of defence represent the central instrument through which states transform strategic objectives into concrete capabilities. By allocating financial resources, governments determine not only the level of military preparedness but also the direction of force development and the degree of interoperability with allies. Unlike other public policies, defence budgets have a dual meaning: they are both indicators of internal priorities and external signals of the credibility of security commitments (Smith, 2019).

Within **NATO**, the budgetary dimension has become a criterion of solidarity and equitable burden sharing. At the 2014 Wales Summit, member states pledged to allocate at least **2% of GDP** to defence by 2024, of which at least 20% was to be devoted to major equipment and research & development (NATO, 2023). This commitment has been reiterated at subsequent summits, reflecting consensus that the effective deterrence of contemporary threats requires constant and predictable investment.

For many European states, reaching this threshold has represented a significant change in public policy. Romania, for example, adopted in 2015 a national political agreement committing to increase the defence budget to 2% of GDP starting in 2017 and to maintain this level in the long term (Government of Romania, 2022). This decision enabled the launch of programmes to modernise aviation, air defence and communications, while simultaneously strengthening Romania's credibility within the Alliance.

However, defence budget policy cannot be viewed in isolation. It must be correlated with **fiscal sustainability** and the needs of other public sectors. Massive military expenditures, unaccompanied by economic growth or structural reforms, can generate social tensions and unsustainable budget deficits (Băhnăreanu, 2009). For this reason, governments seek a **balance** between investments in defence and those in civil infrastructure, health or education, thus ensuring political legitimacy and citizen support for security policy.

In addition, budgetary allocation does not automatically guarantee efficient use of funds. **Transparency and accountability** in the execution of the defence budget are essential to avoid waste, corruption and delays in procurement programmes.

In this sense, public audit, regular reports to Parliament and civil society involvement can contribute to improving the performance of defence spending and maintaining public trust (Born et al., 2003).

In the context of recent crises such as the COVID-19 pandemic and the conflict in Ukraine, defence budget policies have acquired an additional dimension: that of **multidimensional resilience**. States have begun integrating into defence planning investments in strategic stockpiles, critical infrastructure and dual-use capabilities, as well as increasing budgets for research in emerging domains from cyber security to biotechnology (SIPRI, 2021). Thus, the 2% of GDP threshold becomes not only a financial target but also a benchmark for the structural transformation of defence policies and for strengthening collective security.

At the NATO Summit in The Hague in June 2025, the Alliance's members adopted a historic decision to increase defence spending: NATO states committed to raise spending—including related security elements – to **5% of GDP** by **2035**. Of this amount, **3.5% of GDP** will be dedicated to core military expenditures (equipment, personnel, operations, maintenance) and **1.5%** to *"defence-related"* activities – critical infrastructure, digital infrastructure, resilience (reserves, logistics, innovation, etc.). The decision was approved through a joint investment plan *("The Hague Investment Plan"*) and provides for intermediate assessments, especially in 2029, to monitor progress and adjust trajectories according to the strategic environment.

The implications of this decision are multiple and unfold at the economic, political and strategic levels. Economically, raising spending to 5% of GDP will put pressure on national budgets, especially for states with deficits, high debt or substantial economies with low productivity; however, simulations show that, if implemented gradually, it can generate positive effects through investment in infrastructure, stimulation of the defence industrial sector, job creation and technological innovation (Janes, 2025). Politically, the decision is a strong signal of unity and determination in the face of the Russian threat but carries a risk of domestic opposition in fiscally vulnerable states or those with strong social priorities. NATO's strategy will need to clarify what is concretely included in the *"defence-related"* component to avoid the use of these expenditures as a form of creative accounting, since effectiveness is not determined only by percentages but by how resources are directed to relevant, interoperable capabilities adapted to current threats.

Romania, which in 2024 allocated approximately **2.2% of GDP** to defence, plans to increase this percentage towards **5%** in the context of NATO's 2025 commitment. According to an **Erste Group** report from 2025, scenarios exist in which Romania

could reach 5% of GDP by 2028 through gradual growth depending on economic performance, revenue increases and the willingness to reallocate budgetary spending (Erste Group, 2025; Romania Insider, 2025).

The fiscal impact of such an increase is significant. Romania is already facing a large government deficit, estimated at over **8.6% of GDP** in 2024. Raising defence spending to 5% of GDP would require an additional budgetary effort, probably in the form of higher fiscal revenues, reductions in other areas of expenditure or the use of EU/externally provided exceptional funds. Economists and financial institutions warn that without fiscal consolidation Romania risks increased public debt and additional pressure on fiscal credibility.

In conclusion, budgetary policies are more than simple accounting allocations; they reflect a state's political will, administrative capacity and strategic vision. Achieving and maintaining an adequate level of defence financing is a necessary but not sufficient condition for an effective security policy. It must be accompanied by rigorous planning, transparency and international cooperation to transform financial resources into real and credible capabilities.

The Impact of the COVID-19 Pandemic on Security

The COVID-19 pandemic represented the most severe test of the resilience of national security systems since the end of the Cold War. Although at first glance a health crisis seems separate from the military domain, the experience of recent years has shown that population health, the functioning of logistics chains and the response capacity of public institutions are **strategic** elements with a direct impact on national and international security (WHO, 2021). COVID-19 demonstrated that economic and social vulnerabilities can be exploited by state or non-state actors and that security must be redefined to include non-military dimensions.

First, the pandemic triggered unprecedented **resource crises**. Public budgets came under enormous pressure due to spending on health, economic support and social protection measures. In many states, defence allocations stagnated or were postponed, affecting procurement programmes and military exercises (SIPRI, 2021). At the same time, travel restrictions and transport blockages disrupted supply chains for the defence industry, delaying the delivery of equipment and limiting the maintenance of existing capabilities (OECD, 2020).

Second, the pandemic highlighted **population health as a strategic element**. The preparedness of the medical system, testing and vaccination capacity, stockpiles of medical materials and inter-institutional cooperation became indicators of national resilience. Armed forces were called upon to support vaccination logistics, transport medical equipment and maintain public order under restrictive conditions,

confirming the interdependence between civil and military security (MAPN, 2021). In theoretical terms, this reflects an extension of the concept of the public good: protecting collective health becomes a precondition for the functioning of security institutions and for national defence.

Third, the pandemic accelerated the **digitalisation and doctrinal transformation** of security institutions. Telework, online communication and data management became essential for the continuity of critical functions. At the same time, cyber-threats increased, exploiting vulnerabilities generated by massive use of digital platforms. This led governments to invest more in cyber security and resilient digital infrastructures, adding a new dimension to defence budgets (ENISA, 2021).

At the international level, the pandemic underscored the need for **multilateral cooperation**. The unequal distribution of vaccines, competition for medical equipment and the use of trade restrictions generated geopolitical tensions, while revisionist actors attempted to exploit these weaknesses to undermine the cohesion of Western alliances (EUISS, 2021). At the same time, NATO and the EU developed mechanisms for coordination and mutual support, demonstrating that international institutions can function as providers of global public goods in the field of health and security.

In conclusion, the impact of the COVID-19 pandemic on security has been **multidimensional**. It has shown that traditional military power is insufficient without functioning critical infrastructures, a healthy population and a resilient economy. The main lesson for public administrations is the need to integrate public health, logistics and cyber security into strategic planning, as well as to strengthen international partnerships for managing global public goods. In this sense, the pandemic was not only a crisis but also a catalyst for the transformation of security governance.

Lessons from the War in Ukraine: Energy Security, Logistics and Strategic Adaptation

Russia's full-scale invasion of Ukraine in February 2022 represented the largest conventional war on the European continent since 1945 and generated systemic effects on the Euro-Atlantic security architecture. At the same time, it provided a *"laboratory"* for understanding the relationship between economics and military strategy, revealing a series of **key lessons** for public administrations and international institutions (Chivvis, 2023).

Energy security is one of the central lessons. Before the invasion, Europe's dependence on Russian gas seemed manageable through long-term commercial contracts. The war demonstrated, however, that energy infrastructure can be

weaponised. Reduced deliveries of gas, attacks on critical infrastructures and price volatility prompted the European Union to accelerate plans to diversify sources, create strategic reserves and invest in renewable energy and interconnection infrastructures (European Commission, 2023). Energy security is no longer an isolated economic issue but a core component of strategic resilience and the ability to sustain a defence effort.

A second key aspect concerns **military logistics**. The war in Ukraine has shown that continuous supply of ammunition, fuel, equipment and spare parts is as important as technological superiority. Lack of logistical coordination can undermine operational advantages, while railway networks, depots and transport corridors become strategic targets. NATO and the EU have launched initiatives to improve military mobility, simplify customs procedures and modernise critical infrastructure so that troops and equipment can be moved quickly on the eastern flank (NATO, 2023b). This lesson is particularly relevant for Romania and the Baltic States, which constitute key areas for deterrence.

The third lesson involves **strategic and doctrinal adaptation**. The conflict has highlighted the role of emerging technologies, from commercial drones used for military purposes to information warfare and cyber-attacks against critical infrastructures. This obliges public administrations and armed forces to integrate technological innovation more rapidly, develop dual-use capabilities and invest in protecting the cyber domain and communications (IISS, 2023). At the same time, international cooperation in training and equipment transfer has shown that alliances can act as force multipliers when there is political will and effective coordination mechanisms.

On the economic plane, the conflict demonstrated that **financial and trade sanctions** can be used as instruments of deterrence and strategic coercion. Freezing foreign reserves, restricting technology exports and excluding Russian banks from international payment systems have undermined Moscow's ability to finance its war effort, showing that economic interdependence can be transformed from a vulnerability into a foreign-policy tool (CFR, 2022).

In conclusion, the war in Ukraine confirms that security in the twenty-first century is **multidimensional**, and the success of defence strategies depends on integrating energy, logistics, economic and technological dimensions. For public administrations in NATO and EU member states, the lessons of the war imply the need for more comprehensive planning, strengthening the resilience of critical infrastructures and accelerating investment in emerging capabilities, alongside deepening international cooperation.

Economic – Military Strategy Interdependence: Technology, Defence Industry and Digitalisation

Amid the accelerated transformations of the security environment, **the interdependence between the economy and military strategy** has become more visible than ever. On the one hand, the economy provides the resources, infrastructure and human capital necessary to build and modernise military capabilities. On the other, defence strategies and security investments generate multiplier effects on the economy, stimulating innovation, the development of critical infrastructure and the creation of jobs (Băhnăreanu, 2009).

A central domain of this interdependence is **investment in technology**. Progress in artificial intelligence, autonomous systems, advanced sensors or encrypted communications is redefining how military operations are conceived. States that invest consistently in research and development and in the technological transfer between the civil and military sectors enhance their ability to maintain a competitive edge (Gilli and Gilli, 2019). In the United States, the *"innovation ecosystem"* model has generated technology companies collaborating with the Pentagon; in Europe, the European Defence Fund supports joint research projects for emerging technologies with dual-use applications (European Commission, 2022).

The defence industry is another pillar of this relationship. It acts as an **interface between the economy and strategy**, transforming financial resources allocated to defence into equipment, services and real capabilities. A solid industrial base enables states not only to meet their own needs but also to export strategic products, thus strengthening their international influence. In the context of the war in Ukraine, the importance of secure supply chains and the ability to ramp up ammunition production became evident, prompting the European Union to adopt measures to stimulate production and coordinate joint procurement (European Defence Agency, 2023).

An emerging element of the economy – strategy interdependence is **digitalisation**. Digital technologies – big data, cloud computing, artificial intelligence – are transforming planning, command and logistics processes within defence institutions. Armed forces are investing in digital platforms for resource management, simulations and virtual exercises, while public administrations are developing dashboards and integrated systems for evaluating security policies (NATO, 2023c). This transformation is not only technical but also organisational, requiring new skills and new models of data governance.

Alongside the obvious advantages, the interdependence between the economy and military strategy also raises **challenges**. Massive investments in emerging

technologies can create critical dependencies on foreign suppliers, while the transfer of dual-use technology involves risks of proliferation and cyber security. Moreover, robust **inter-institutional coordination** is necessary to avoid duplication and to ensure the efficient use of resources. Public administrations must therefore develop support policies for the defence industries, mechanisms for information sharing and training programmes for strategic leadership and risk analysis (OECD, 2022).

In conclusion, the interdependence between the economy and military strategy is not merely a passive phenomenon but can be **actively shaped** through coherent public policies, public – private partnerships and smart investments in technology and digitalisation. Such an approach can turn defence spending from a necessary cost into a driver of innovation and national resilience, thereby consolidating security as a public good.

CONCLUSIONS AND RECOMMENDATIONS

The analysis presented in the first two chapters highlights the complex nature of security as a public good, both at the national and global level. Starting from its theoretical foundations – non-excludability, non-rivalry, the free-rider problem and the role of public policies – it becomes clear that security can no longer be approached merely as a military function of the state, but rather as a **multidimensional** ecosystem in which health, energy, cyber resilience and financial stability are essential components. Within this framework, public administration acts as the orchestrator of resources and partnerships, while international institutions such as NATO and the European Union operate as providers and coordinators of global public goods.

The practical dimension of the analysis shows that **economic resources** constitute the foundation of military power. Budget allocations for defence – exemplified by the 2% of GDP benchmark assumed within NATO – are not just accounting figures but the expression of political will and long-term security strategy. The COVID-19 pandemic demonstrated that national security is inseparable from public health and the functioning of supply chains, while the conflict in Ukraine showed that energy security and military mobility are as important as technological modernisation. Investments in industry, critical infrastructures and digitalisation can turn defence spending from a burden into a driver of innovation and economic resilience.

Based on these findings, several complementary recommendations emerge:

- **Establish a national framework for policy evaluation** in the field of defence and resilience, to monitor the impact of programmes and allow rapid

adjustments to changes in the strategic environment. Such a framework would integrate performance indicators, independent audits and public reporting, strengthening transparency and accountability of decision-makers.

- **Integrate data from NATO, SIPRI, the World Bank or Eurostat into public dashboards enabling international** comparisons and supporting evidence-based decision-making. These tools would facilitate understanding of the distribution of defence effort, spending trends and structural vulnerabilities.
- **Develop public – private partnerships for dual-use capabilities and secure supply chains**. In an interdependent economy, the private sector holds a significant share of critical infrastructures and technological know-how. Public policies should stimulate collaboration and innovation in areas such as cyber security, ammunition production, energy and communications.
- **Launch training programmes for strategic leadership, risk analysis and data governance** within public administration and the security sector. Qualified human resources are the key element that can transform financial investments into real capacity for reaction and planning.
- **Implement integrated plans for military mobility and critical infrastructure interoperable with Euro-Atlantic standards**, ensuring that crisis responses are rapid and coordinated. Lessons from the conflict in Ukraine show that transport, storage and communication infrastructure can be decisive factors in deterring aggression.

These recommendations should not be seen as isolated initiatives but as part of an **adaptive governance strategy** connecting economic, defence and social policies. A public administration oriented towards resilience, transparency and partnership can transform current challenges – pandemics, conflicts, energy crises – into opportunities for strengthening collective security. In this way, security remains a public good, but one delivered through smart public policies, international cooperation and the active involvement of all relevant actors.

BIBLIOGRAPHY:

1. Băhnăreanu, C. (2009), *The Influence of the Economic Factor in Achieving Security*. Bucharest: "Carol I" National Defence University Publishing House.
2. Born, H., Fluri, P., Johnsson, A. (2003). *Handbook on Parliamentary Oversight of the Security Sector*. Geneva: DCAF – Geneva Centre for the Democratic Control of Armed Forces.
3. Buchanan, J.M. (1965). *'An Economic Theory of Clubs'*, in *Economica*, vol. 32, no. 125, pp. 1-14.

4. CFR (Council on Foreign Relations) (2022). *'Sanctions on Russia: Impacts and Effectiveness',* https://www.cfr.org/backgrounder/sanctions-russia-ukraine-war, retrieved on 5 September 2025.
5. Chivvis, C. (2023). *'Lessons from the Ukraine War for U.S. Strategy in Europe'*, in Foreign Policy Research Institute, March, https://www.fpri.org/article/2023/03/lessons-from-the-ukraine-war-for-u-s-strategy-in-europe, retrieved on 22 September 2025.
6. Dunn, W.N. (2017). *Public Policy Analysis: An Integrated Approac*h. 6th edn. New York/Abingdon: Routledge.
7. ENISA (European Union Agency for Cybersecurity) (2021). *ENISA Threat Landscape 2021,* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021, retrieved on 2 September 2025.
8. Erste Group (2025). '*Romania: A New Era of Defense Expenditure'*, https://www.erstegroup.com/en/research/report/en/SR436222, retrieved on 2 September 2025.
9. EUISS (European Union Institute for Security Studies) (2021). *Pandemic geopolitics: COVID-19 and the international order*, https://www.iss.europa.eu/content/pandemic-geopolitics-covid-19-and-international-order, retrieved on 9 September 2025.
10. European Commission (2022). *'European Defence Fund: 61 collaborative defence research and development projects selected'*, https://ec.europa.eu/defence-industry-space/european-defence-fund, retrieved on 8 September 2025.
11. European Commission (2023). *'REPowerEU Plan: Affordable, Secure and Sustainable Energy for Europe'*, https://commission.europa.eu/repowereu-plan, retrieved on 8 September 2025.
12. European Council (2023). *'EU support for Ukraine: military assistance and macro-financial aid'*, https://www.consilium.europa.eu/en/policies/eu-support-ukraine/, retrieved on 18 September 2025.
13. European Defence Agency (2023). *'Supporting Ammunition Production and Joint Procurement in the EU'*, https://eda.europa.eu/news-and-events/news, retrieved on 18 September 2025.
14. Gilli, A., Gilli, M. (2019). *'Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage*', International Security, vol. 43, no. 3, pp. 141-189.
15. Global Firepower (GFP) (n.d.). *'2023 Military Strength Ranking',* http://www.globalfirepower.com/countries-listing.asp, retrieved on 16 September 2025.
16. Government of Romania (2022). *Government Programme 2021-2024.* Chapter: Defence and Public Order. Bucharest: Government of Romania.
17. IISS (International Institute for Strategic Studies) (2023). *The Military Balance 2023*. London: Routledge.
18. Janes (2025). *'White paper assessing NATO's 5% defence spending plan',* https://www.janes.com/osint-insights/defence-and-national-security-analysis/nato-spending-plan-assessment-white-paper, retrieved on 20 September 2025.
19. Kaul, I., Conceição, P., Le Goulven, K., Mendoza, R.U. (eds.) (2003). *Providing Global Public Goods: Managing Globalization*. New York: Oxford University Press.
20. Kennedy, P. (1987). *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000*. New York: Random House.

21. Keohane, R.O., Nye, J.S. (2001). *Power and Interdependence*, 3rd edn. New York: Longman.
22. MoND (Ministry of National Defence – Romania) (2007-2023). '*Budget. Information regarding the Budget of the Ministry of National Defence*', http://www.mapn.ro/buget/index.php, retrieved on 8 September 2025.
23. MoND (Ministry of National Defence – Romania) (2021). *Report on the Involvement of the Romanian Army in Managing the COVID-19 Pandemic*. Bucharest: MoND.
24. Monitorul Apărării (2021). *'NATO report on military spending in 2020. Only 11 countries meet the recommendation to increase the defence budget'*, 17 March, https://monitorulapararii.ro/raport-nato-despre-cheltuielile-militare-in-2020-doar-11-tari-respecta-recomandarea-de-a-creste-bugetul-apararii-1-36008, retrieved on 20 September 2025.
25. Musgrave, R.A. (1959). *The Theory of Public Finance: A Study in Public Economy*. New York: McGraw-Hill.
26. NATO (2023-a). '*Defence Expenditure of NATO Countries (2014-2023)',* https://www.nato.int/cps/en/natohq/news_220195.htm, retrieved on 14 September 2025.
27. NATO (2023-b). *'Improving NATO Military Mobility: Projects and Funding'*, https://www.nato.int/cps/en/natohq/topics_152817.htm, retrieved on 14 September 2025.
28. NATO (2023-c). *'NATO Digital Transformation and Emerging Technologies'*, https://www.nato.int/cps/en/natohq/topics_184303.htm, retrieved on 14 September 2025.
29. NATO (2025). *'The Hague Summit Declaration'*, 25 June, https://www.nato.int/cps/en/natohq/official_texts_236705.htm, retrieved on 14 September 2025.
30. OECD (Organisation for Economic Co-operation and Development) (2020). *'COVID-19 and Global Supply Chains: Disruptions and Policy Responses'*, https://www.oecd.org/coronavirus/policy-responses/covid-19-and-global-supply-chains-disruptions-and-policy-responses, retrieved on 18 September 2025.
31. OECD (Organisation for Economic Co-operation and Development) (2022). *Industrial Policy for the Defence Sector: Ensuring Resilient Supply Chains*. Paris: OECD.
32. Olson, M. (1965). *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge, MA: Harvard University Press.
33. Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action.* Cambridge: Cambridge University Press.
34. Romania Insider (2025). '*Romania adheres to 5%-of-GDP defence spending target',* 3 June, https://www.romania-insider.com/romania-defence-budget-june-2025, retrieved on 13 September 2025.
35. Rothstein, B. (2011). *The Quality of Government: Corruption, Social Trust, and Inequality in International Perspectiv*e. Chicago: University of Chicago Press.
36. Samuelson, P.A. (1954). *'The Pure Theory of Public Expenditure'*, in *The Review of Economics and Statistics*, vol. 36, no. 4, pp. 387-389.
37. SIPRI (Stockholm International Peace Research Institute) (2021). *'World Military Spending Rises to Almost $2 Trillion in 2020'*, https://www.sipri.org/media/press-release/2021/world-military-spending-rises-almost-2-trillion-2020, retrieved on 5 September 2025.

38. SIPRI (Stockholm International Peace Research Institute) (2023). *SIPRI Military Expenditure Database*, https://www.sipri.org/databases/milex, retrieved on 14 September 2025.
39. Smith, R. (2019). *Defence Economics*, 3rd edn. London: Routledge.
40. Tooze, A. (2006). *The Wages of Destruction: The Making and Breaking of the Nazi Economy*. London: Allen Lane.
41. United Nations (UN) (2004). *'A More Secure World – Our Shared Responsibility – Report of the High-level Panel on Threats, Challenges and Change'*, 2 December, https://www.un.org/peacebuilding/content/more-secure-world-our-shared-responsibility-%E2%80%93-report-high-level-panel-threats-challenges-and, retrieved on 21 September 2025.
42. WHO (World Health Organization) (2021). *World Health Statistics 2021: Monitoring Health for the SDGs*. Geneva: WHO.