The 20th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, October 30th-31st 2025

DEFENSE RESOURCE PLANNING CHALLENGES IN THE CURRENT SECURITY ENVIRONMENT

Nino GIORGOBIANI
Ministry of National Defense, Georgia

Abstract:
Modern defense resource planning faces unprecedented challenges driven by rapid technological change, shifting geopolitical dynamics, and evolving societal norms. This paper examines four critical dimensions shaping defense planning in the 21st century: human capital, economic constraints, technological integration, and logistical complexity. It highlights how traditional military structures and planning models are increasingly misaligned with the demands of contemporary security environments, including hybrid warfare, cyber threats, and multi-domain operations. The analysis emphasizes the urgent need for adaptive, agile, and innovation-driven strategies to ensure military readiness and strategic advantage. By exploring these interconnected challenges, the paper offers insights into how defense institutions can evolve to meet future security demands in a complex and uncertain global landscape.

Keywords: *reusource plannig; challenges; oportunities; readiness; strategic advantage.*

Introduction

The 21st-century era of rapid technological development and world power shifting changed our understanding of war, security and their dimensions. Defence and security are not only superiority in the land, sea and air domains it is beyond that. In today's globalization and technological rapid expansion multiplied security and defence dimensions, each represented a domain where conflict can unfold. These warfare domains are interconnected and often used simultaneously in hybrid strategies. This contemporary security environment is marked by complexity, unpredictability, and rapid changes, which demands strategic foresight, adaptability, and resilience from Defence organisations. Rising tensions among major powers, regional conflicts, and the resurgence of great-power competition mark the current international landscape. Conflicts such as the Russia-Ukraine war, Indo-Pacific tensions, and Middle East instability strain existing defence postures and create unpredictable scenarios that require rapid response capabilities. Defence resource planning is the process of aligning available assets—human, financial, technological, and material—with strategic objectives to ensure military effectiveness. Defence planners must anticipate diverse scenarios—from conventional warfare to grey-zone operations—and allocate resources flexibly. However, in an era of constrained budgets, cyber warfare, and global supply chain disruptions, this process has become increasingly difficult.

This paper examines the primary challenges in defence resource planning and management, focusing on human capital, economic constraints, technological integration and logistical complexities. As hybrid threats become more prevalent and strategic uncertainty increases, traditional resource planning models must adapt to ensure operational readiness and strategic advantage.

1. Human Capital

Skilled human resources are central to defence effectiveness, particularly in domains like cyber, data analysis, and unmanned systems. However, many militaries struggle to recruit and retain the talent necessary to operate and innovate within these domains. Defence organizations compete with the private sector for high-tech talent, often offering less attractive career paths and compensation. Moreover, outdated personnel policies and rigid hierarchies hinder agility and innovation. According to several studies, military recruitment across numerous nations is increasingly caught up by four major factors, demographic shifts, societal attitudes, technological advancements and cultural factors.

1.1. Demographic Shifts

- Health Issues: Many potential recruits are disqualified due to physical or mental health concerns. In the U.S., for example, obesity, drug use, and mental health diagnoses disqualify over 75% of youth aged 17–24.
- Educational Deficiencies: Declining literacy, numeracy, and overall academic performance reduce the number of candidates eligible for roles requiring basic or technical proficiency.
- Aging Populations: In countries like Japan and Germany, shrinking youth populations due to low birth rates are limiting the military-age demographic.
- Urbanization: More youth in urban areas are disconnected from military culture, which is often more prevalent in rural or traditional communities.

1.2. Societal Attitudes

- Erosion of National Identity: Many younger citizens express a weaker sense of national duty or patriotic motivation to serve, especially in Western democracies.
- Perceived Irrelevance: Some view the military as outdated or disconnected from modern, tech-driven career aspirations.
- Public Trust Deficit: High-profile incidents of misconduct, the politicization of the military, or controversial deployments have led to growing public scepticism and reluctance to support military service.
- Competing Civilian Opportunities: Skilled candidates are more likely to choose lucrative private-sector jobs over military careers, especially in fields like engineering or IT.

1.3. Technological Advancements

- Changing Warfare Landscape: Modern conflicts increasingly involve cyber warfare, unmanned systems (drones), space operations, and AI-based surveillance—requiring highly technical personnel.
- Skill Shortages: Armed forces must now compete with the tech industry for experts in cybersecurity, coding, machine learning, and data science.

- Training Gaps: Traditional military training pipelines are often too slow or outdated to produce cyber-ready professionals at the pace needed.
- Integration Challenges: Adapting command structures and recruitment models to accommodate tech-savvy specialists without traditional military backgrounds remains difficult.

1.4. Cultural Factors

- Workplace Environment: Reports of hazing, sexual harassment, racism, and toxic leadership have damaged the reputation of military service as a safe or equitable career.
- Inclusion and Diversity: Many militaries are struggling to attract recruits from minority or underrepresented communities due to historical exclusion or lack of targeted outreach.
- Retention Issues: Even when individuals join, many leave early due to dissatisfaction with career progression, work-life balance, or family support systems.
- Generational Expectations: Younger recruits often seek flexibility, purpose-driven work, and respectful leadership—expectations that clash with hierarchical, rigid military cultures.

In conclusion, as a new generation joins the military ranks, defence structures face challenges related to technological expectations, work-life balance, diversity, purpose, and communication styles. By adapting to these challenges, the military can create an environment that attracts and retains this generation of service members. Embracing technology, promoting inclusion, and fostering a culture of purpose will not only enhance recruitment efforts but also ensure a more resilient and effective defence force for the future.

2. Economic constrains

National defence spending has traditionally occupied a central place in government budgeting, often justified by the imperative of maintaining security, sovereignty, and geopolitical influence. However, contemporary economic realities have introduced significant constraints to defence budgets, especially after the end of the Cold War European countries significantly decried defence spending. These constraints are shaped by a combination of competing domestic priorities, global economic volatility, and the increasing financial demands of technological modernization. It has to be underlined that the COVID-19 pandemic left most governments with unprecedented debt levels due to stimulus packages, emergency spending, and revenue losses. This financial squeeze complicates medium- and long-term planning in the defence sector, particularly for states with smaller economies or weaker fiscal foundations.

Modern warfare increasingly demands advanced technologies, including cyber defence systems, hypersonic missiles, space-based sensors, and autonomous platforms. The costs associated with these systems are immense, often surpassing traditional weapons platforms in both acquisition and lifecycle maintenance.

These economic constraints have several implications for defence strategy and operational readiness such are:

- **Capability Gaps:** Nations may struggle to maintain full-spectrum capabilities, leading to over-reliance on allies or contractors.
- **Delayed Modernization:** Lagging in technological adoption may reduce deterrence and operational effectiveness.
- **Reduced Global Influence:** Budget limitations may hinder a country's ability to project power or participate meaningfully in multinational operations.

- **Vulnerability to Asymmetric Threats:** Adversaries may exploit gaps created by fiscal constraints, especially in areas like cyber and space.

Economic constraints have become a defining feature of contemporary defence budgeting. While national security remains a paramount concern, it must now be balanced against a complex array of domestic and international economic pressures. Only after Russia's full-scale invasion of Ukraine, some European countries start to reprioritize the defence budget and allocate more funds to it (Fig.1). To navigate this environment, governments must pursue smarter, more efficient approaches to defence spending—emphasizing cost-effective innovation, collaborative development, and transparent procurement practices. Only through such reforms can defence establishments remain capable and credible in an increasingly unpredictable world.

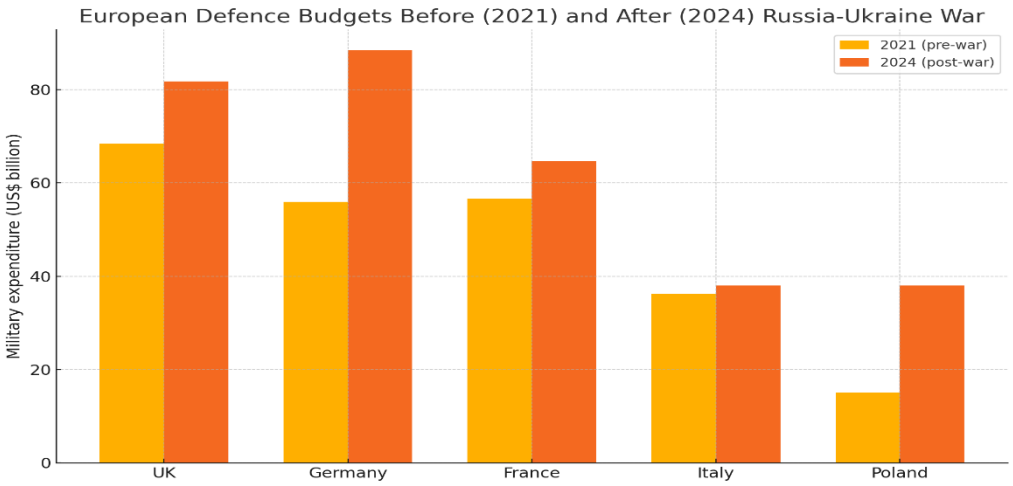

Fig.1 (comparing military outlays before Russia's full-scale invasion of Ukraine (calendar year 2021) with the most recent post-war data available (calendar year 2024)

3. Technological integration

Defence organizations worldwide are undergoing a profound transformation driven by rapid technological advancement. The emergence of artificial intelligence (AI), machine learning, big data analytics, and autonomous systems has the potential to redefine warfare, command structures, and defence strategies. However, the pace of innovation often surpasses the military's ability to adapt, constrained by legacy infrastructure, institutional inertia, and regulatory gaps. In this chapter, we will overview the technological, operational, and ethical challenges military organisations face and the reforms necessary to remain agile and responsible in a rapidly evolving security environment.

3.1. Legacy Systems vs. Modern Requirements

Many defence forces continue to rely on decades-old systems originally built for old conventional-style conflicts. These legacy platforms are the tanks, fighter jets, communication networks, and missile defence systems which are facing a lack the flexibility and digital architecture to accommodate next-generation technologies.

I will outline three key problems that are more commonly faced by defence forces:

- Outdated hardware and software often lack interfaces and abilities for integrating new components or software-based upgrades.
- Economical restraints and slow procurement cycles mean that by the time new systems are fielded, they may already be outdated.
- Reliance on proprietary or closed systems complicates interoperability between allied forces and different branches within the same military.

These technological holdups weaken strategic responsiveness and reduce effectiveness in modern multi-domain operations that require seamless coordination between land, sea, air, space, and cyber environments.

3.2. Integration Challenges: AI, Big Data, and Autonomy

Emerging technologies offer transformative capabilities but are difficult to implement into traditional defence structures. Integration of modern technological assets within military structures requires doctrinal changes, reassessment of standing operational procedures and a more hasty decision-making process. From these complex challenges, I would like to outline some of them:

Artificial Intelligence (AI) can enhance threat detection, autonomous navigation, decision support, and predictive maintenance conversely AI systems which require massive, high-quality datasets and computing power resources are not always available or secure for defence settings.

Big Data Analytics offers real-time battlefield insights, logistics optimization, and cyber threat anticipation for military operations, but integrating disparate data sources from legacy systems and ensuring data integrity under combat conditions is highly complex.

Autonomous Systems such are drones, unmanned ground vehicles, and robotic swarms offer cost-effective, risk-mitigated and prompt force projection, however full autonomy raises questions of command and control, as well as the system's ability to distinguish combatants from civilians under the laws of armed conflict.

3.3. Legal and Ethical Considerations

The deployment of advanced technologies in warfare introduces unprecedented ethical and legal challenges that cannot be resolved solely through technical solutions and requires legal and ethical frameworks, such as legal accountability and ethical implications:

Legal Accountability challenges are:

- Current international humanitarian law (IHL) and rules of engagement are not fully equipped to address scenarios involving autonomous lethal weapons or AI-based targeting.
- Who is responsible when an autonomous system makes a fatal error? Legal frameworks lag behind technological capability.

Ethical Implications arise from the following issues:

- Autonomous weapons raise moral concerns about delegating life-or-death decisions to machines.

- Issues of bias in AI models could lead to disproportionate or unlawful targeting based on flawed data or algorithmic discrimination.

To overcome these challenges defense organizations must establish oversight bodies and compliance protocols to ensure emerging technologies respect human rights, minimize civilian harm, and comply with the Geneva Conventions. The accelerating pace of technological change is reshaping the nature of defence and security. While emerging technologies offer unmatched opportunities to enhance capability, they also introduce serious integration, legal, and moral risks. Navigating this disruption demands a holistic approach—modernizing infrastructure, securing digital ecosystems, and embedding ethical and legal safeguards into every stage of development and deployment. Only then can defence institutions maintain both technological superiority and strategic legitimacy in an evolving world. However nowadays, we have witnessed the effectiveness of drones in Russian - the Russian-Ukraine war and understand that unmanned vehicles are the future of combat advantages.

3.4. Interoperability and Cybersecurity Risks

As defence systems become more digitally connected, interoperability and cybersecurity emerge as dual imperatives. On one hand, cross-platform compatibility is critical in coalition operations (NATO or UN missions), without common data standards or open systems architecture, joint operations become fragmented and inefficient but in another hand. Integrated digital systems expand the attack surface for adversaries and vulnerabilities in AI algorithms, communication protocols, and remote control systems can be exploited to disrupt operations or steal sensitive information.

4. Logistical complexities in Modern Defense

In an era of global interdependence and rising geopolitical uncertainty, defence logistics has become a critical strategic domain. Once a back-office function, logistics now plays a frontline role in military readiness, resilience, and global power projection. Defence supply chains are increasingly strained by the dual pressures of technological dependency and systemic vulnerability—exacerbated by events such as the COVID-19 pandemic, the Russia-Ukraine war, and tensions over Taiwan and the South China Sea. This chapter will be focused on the mounting complexity of defence logistics, highlighting the risks posed by supply chain fragility, geopolitical realignment, and sustainability mandates.

4.1. Globalization and the Fragile Defense Supply Chain

Modern military equipment like fighter jets, precision-guided munitions, and cyber-defence platforms depend on components sourced from dozens of countries, including adversarial or politically unstable regions. This globalization of production creates strategic exposure such as semiconductors and microchips which are produced in East Asian countries (notably Taiwan and South Korea) or Rare Earth Elements (REEs) which are critical for guidance systems, stealth coatings, and electric vehicles mainly produced in China (over 70% of the global supply). Disruption in this region, due to conflict or blockade, would paralyze global defence electronics.

As well currently we have recent supply chain shocks due to COVID-19: the world has been exposed to the fragility of just-in-time logistics and overreliance on single-source suppliers. Disrupted access to critical materials like titanium and nickel due to the Russia-Ukraine War forced NATO countries to rapidly reassess munitions stockpiles. Additionally increasing the use of economic weapons (chip bans on China or Russia) adds uncertainty to global procurement.

4.2. Geopolitical Realignment and Strategic Stockpiling

Defence ministries are rethinking logistics from a geopolitical risk lens, countries like the U.S., Germany, and Australia are investing in domestic manufacturing of critical components from drones to ammunition. Furthermore, EU's Joint Procurement of Ammunition and NATO's Strategic Airlift Capability seek to pool logistics and ensure shared access during crises. However, these measures come at a high cost and are often constrained by national-level fragmentation, bureaucratic inertia, and the long lead times required for industrial ramp-up.

4.3. Environmental Sustainability in Defense Logistics

Militaries are among the largest institutional consumers of fossil fuels, primarily for vehicles, aircraft, and naval fleets. According to some estimates, if the U.S. Department of Defense were a country, it would be the 47th largest emitter in the world. Within global climate commitments, militaries are under increasing pressure to reduce their carbon footprint, leading to a push for:

Electric and hybrid military vehicles
Alternative fuels (biofuels for naval ships and aircraft)
Energy-efficient logistics hubs and bases
Circular economy approaches (reuse and recycling of components)

This shift requires long-term investment, new procurement standards, and close collaboration with the commercial sector. It also raises tactical questions about fuel reliability, supply chains in hostile environments, and technology performance under combat conditions.

The age of smooth, just-in-time defence logistics is over. In its place, militaries must operate in an environment of perpetual disruption from pandemics and wars to climate shocks and political fragmentation. To succeed, defence logistics must evolve into a strategic capability that balances speed, security, sustainability, and sovereignty. This evolution will not be easy but it is essential for operational credibility and global stability in the 21st century.

Conclusion

The contemporary defence landscape is shaped by a web of interdependent, rapidly evolving challenges. Resource planning, once a primarily budgetary and logistical function, has become a multidimensional strategic imperative which is essential to national resilience, international influence, and military effectiveness. At the core of this complexity lies a fragile balance between human capital, fiscal resources, technological adaptation, and logistics infrastructure which now must operate as a tightly integrated ecosystem.

These factors are not fragmented they are deeply knotted, creating feedback loops that amplify risk. For example, fiscal austerity may delay technical integration, which in turn undermines the recruitment of high-skill talent, which then weakens the effectiveness of modern platforms. Similarly, logistics vulnerabilities can erode deterrence credibility, affecting alliance dynamics and procurement diplomacy. In response, defence institutions must adopt a systems-thinking approach to resource planning, one that accounts for strategic interdependencies, long-term resilience, and cross-domain innovation. This involves the following measures:

- Redesigning institutional structures to break down silos between operational planning, acquisition, and research communities.
- Fostering dual-use ecosystems that blend commercial innovation with defence needs, ensuring agility and affordability.
- Embedding adaptive planning models that can simulate uncertainty, manage risk portfolios, and respond dynamically to geopolitical shocks.

- Reframing sustainability and ethical oversight not as external constraints, but as core strategic competencies necessary for legitimacy and endurance.

Ultimately, the future of national security will be defined less by raw military power and more by the intelligence, agility, and cohesion with which nations manage their defence resources. Success will favour those who can integrate foresight with flexibility by building security architectures that are not only strong, but smart, sustainable, and socially accountable.

References:

[1]. Defense Innovation Board. (2022). AI principles: Recommendations on the ethical use of artificial intelligence by the Department of Defense. https://media.defense.gov/2022/Jul/01/AI-Principles-Report.pdf

[2]. Kavanaugh, J. (2021). The talent war: How tech industry is outcompeting defense for cyber talent. Defense One. https://www.defenseone.com

[3]. NATO Review. (2022). Securing the supply chain: NATO's new logistical imperative. https://www.nato.int/review

[4]. Stockholm International Peace Research Institute. (2023). Trends in world military expenditure 2023. https://sipri.org

[5]. Kelly, J. (2025, April 3). Entitlement, identity politics, lack of pride blamed for slump in ADF recruitment. *The Australian*. https://www.theaustralian.com.au/nation/defence/entitlement-identity-politics-lack-of-pride-blamed-for-slump-in-adf-recruitment/news-story/7c0b8f62f1f7c036f983ab75a5756487

[6]. Miller, J. (2025, May 24). 'Crazy' data rules hit German plans to boost army reserve. *Financial Times*. https://www.ft.com/content/db0d9cc0-8d63-4107-ad62-3452fcd181ae

[7]. Helm, T. (2025, June 1). British Army will not be increased in size this parliament, John Healey says. *The Guardian*. https://www.theguardian.com/uk-news/2025/jun/01/british-army-will-not-be-increased-in-size-this-parliament-john-healey-says