BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

No. 2/ 2024

ISSN 2284-936X
eISSN 2284-9378

Publication founded in 1937

SCIENTIFIC PUBLICATION HIGHLY ACKNOWLEDGED IN THE FIELD OF "MILITARY SCIENCES, INFORMATION AND PUBLIC ORDER" OF THE NATIONAL COUNCIL FOR ATTESTATION OF ACADEMIC DEGREES, DIPLOMAS AND CERTIFICATES, INDEXED IN INTERNATIONAL DATABASES EBSCO, CEEOL, GOOGLE SCHOLAR, INDEX COPERNICUS, PROQUEST, DOAJ, ERIH PLUS, CROSSREF

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, 2024

The articles published in the Bulletin of "Carol I" National Defence University, ISSN 2284-936X, L 2284-936X, are also found – title, author, abstract, content and bibliography – in the Romanian version of the journal, ISSN 1584-1928.

Content

No. 2/2024

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Forward defense – concept, plan, and action for solving russian aggression at Nato's easternd border

Prof. Iulian CHIFU, Ph.D.*

*"Carol I" National Defence University
e-mail: keafuyul@gmail.com

Abstract

Forward defense is not a new concept. It is rather traditional, coming from the Cold War and implying, originally, the nuclear posture and strategy. Following the issuance of the Madrid NATO Strategic Concept and Vilnius statement that not an inch of the Alliance's territory will fall under the control of the opponents, a new approach to forward defense is needed to cope with the multiple shifts in the security environment: Russian war of aggression, the change of technological generation, dilemmas of resources and capabilities, limits and multiple challenges from the international environment with superposed simultaneous crises. The perspective of possible attacks on NATO territory – in the next 2-3-5-8 years – requires a review of the concept and, consequently, of the political decisions, strategic planning, enforcement of those decisions, and development of forces and capabilities on the ground. Combining nuclear flexible capabilities, a strategy of massive retaliation with conventional forces and deterrence by reinforcement, deterrence by denial, forward presence, rapid projection capabilities, resolution, effective decision-making, and forward posture, we could build a new, updated doctrine of forward defense. However, the debate has to consider what is theoretically developed, technically feasible, politically acceptable, financially sustainable, and strategically credible in the „new forward defense" for granting inviolability of allied territory. The basic limitation is to define and refine forward defense without a reconsideration beyond existing means.

Keywords:

forward defense; deterrence; defense by denial; extra-territorial engagement; strategic depth; forward posture.

Article info
Received: 15 May 2024; Revised: 3 June 2024; Accepted: 7 June 2024; Available online: 5 July 2024

Citation: Chifu, I. 2024. "Forward defense – concept, plan, and action for solving russian aggression at Nato's easternd border." *Bulletin of "Carol I" National Defence University*, 13(2): 7-20. https://doi.org/10.53477/2284-9378-24-16

The concept of forward defense has roots in the history, geopolitics, and diverse levels of ambitions in historic times. The first type was developed by the naval powers, island states, and remote grand powers considering the need to face the enemy outside of their territory, in the grand seas and oceans of the globe. Be it the US, UK, *Türkiye*, Australia, or Singapore, all states had a share in the debate and introduced forward defense in their respective strategic and security documents. In some cases, the forward defense was just a piece or chapter of the post-imperial syndrome or of the neo-imperial strategies, nostalgic dreams of greatness, or newly discovered opportunities for projecting interests in its region, as the case is with the Soviet Union, Russia (Chifu & Ţuţuianu 2017) or Iran.

UK had a sea, naval, and projection of power type of forward defense during its times of colonial global presence, which transposes today, in a limited version, in its military relation with Europe, the EU, and France, in particular. The US began forward defense thinking with naval forward defense, first outside its territorial waters, then it developed a global forward defense of its interests, and created a theory of protecting its citizens all over the world (US Department of State – Bureau of Consular Affairs, n.d.) and access to needed resources (US Department of Commerce 2020), wherever they are situated, balancing regional powers (creating neo-realism as a theoretical approach, in the process) and linking its security with the security of Europe during the two World Wars and NATO foundation. The last decade brought the debate about fair burden sharing of costs for common defense inside the alliance (defense pledge) (NATO 2024) and responsibilities in Europe's neighborhood. Discussing forward defense, the US moved to assume forward presence, then deterrence, and forward posture, discussing nowadays the credibility of an enforced forward posture and the needs of global coalitions and alliances, in a variable geometry.

Türkiye begins introducing the logic of "forward defense" with Mavi Vatan - Turkish naval doctrine. Davudoglu's Neo-Ottomanism and zero problems with the neighbors was also a "forward defense" strategic theory, mainly based on a perception of common culture and on the systematic use of soft power, which became after 2009, and especially after the 15th of July 2016 attempted coup, a hard power pillar of Turkish forward policy (Taspinar 2008). As was the case with the Organization of Turkic States (OTS), formerly called the Turkic Council or the Cooperation Council of Turkic Speaking States. Here, the discussion about legitimate cultural ties, soft power approach, alliance, and forward defense and offensive aims is open and a number of states have different approaches, even rating those developments as direct threats – Greece, Cyprus, and Iran. Still, the novelty regarding that approach is also the defense beyond the national territory (Areteos 2020).

The Soviet Union and Russia embraced a theory of the needed space, strategic depth and buffer zones, coming from Ekaterina the Great and the burndown of Moscow by the Tartars. That led to Russian classical geopolitics and the institutionalization of the Kozakhs, free people, farmers, and fighters, defenders of the borders of the

empire. But this translated easier into imperial, post-imperial and neo-imperial ambitions of aggression, violence, and occupation when the Soviets introduced the spheres of influence, transformed by Russia into the sphere of strategic interest – with concepts and actions from limited sovereignty of neighbor communist states (Romaniecki 2016) to frozen conflicts and Russian presence in the post-Soviet space (Chifu & Țuțuianu 2017) as post-imperial approaches and annexation of territories by military force since 2008 in Georgia, as neo-imperialist aims. Russia proved that nonaligned, neutral states and buffer zones in its proximity become just grey zones not yet occupied by Russia.

For sure, this is not a genuine, acceptable forward defense, according to international law and the rules-based order. However, an excess of interpretation and wishful thinking transformed into reality once there was no opposition to Russia's offensive acts. Ukraine fell under this alleged forward defense approach (in fact space geopolitics). Putin's statements related to the need for a buffer zone inside Ukraine to defend Russia's interests (President of Russia 2024), as well as Lavrov's statements that this buffer zone inside Ukraine is as large as the new long-range reach of the weapons transferred to Ukraine (Ministry of Foreign Affairs of the Russian Federation 2024) are showing both this territorial neo-imperial approach, as are indicating the 2021 ultimatums/proposals drafting Russia's view of the New Security of Europe (Ministry of Foreign Affairs of the Russian Federation 2021).

Information warfare plays its role in this Russian approach to forward defense, especially in the post-Soviet space, by changing the environment into a friendly pro-Russian one – challenged by independent states as neo-imperialism (Chifu & Simons 2023). In fact, Russia rejected the buffer zones, transforming them into future controlled zones of Russia. Widening and occupying those regions was an attempt to close this new Fulda Gap in Eastern Europe, which led to the full-scale, high-intensity, long-term war of aggression in Ukraine. This happened once the space and territorial approach proved no longer valid after Ukraine hit oil refineries, oil depots, military bases, and logistical infrastructure 1,500 kilometers deep into Russian territory using civilian-industrial drones.

An interesting approach to forward defense could be found in Iran's strategy. Prompted by the needs of the Iran-Iraqi war, it shifted to religious Shia motivation for support towards minorities in Sunni states and moved to an ideological projection of the Revolutions and challenges to kingdoms and caliphates here on Earth. Rivalries and politics against the Israeli state and opportunities on the ground in Syria and Iraq, as well as in Yemen, raised the stakes to forward defense by proxies. The 13th April attack unveiled the direct confrontation and showed the limits of the military capabilities of Iran. Moreover, the leadership of Iran is aware of the limits and rejection in the society of those investments in proxies, so reconsidering that form of forward defense, prompted by opportunistic means, is on its way.

Methodology

In order to reach the aim of the study, a concept theoretically developed, technically feasible, politically acceptable, financially sustainable, and strategically credible „new forward defense", and the applicability of such a concept in granting the inviolability of allied territory, we used comparative studies, an epistemological approach to the concept, content analysis, and extensive study of the security and strategic documents of different countries.

Forward defense: the concept

Forward defense is a concept with a clear definition but a significant need for constant adaptation to technological and strategic evolution, as well as to the specific applicability, resource availability, and capability gap within a given strategic environment. It does not fundamentally alter the conceptual basis of defense, as it primarily concerns the defense of a state's territory as close as possible to the source of threat and as far as possible from its own territory. However, the complex relationship with one's own territory, especially in cases of limited strategic depth, and the maritime component, including territorial waters and exclusive economic zones, alongside land borders, pose constant challenges. Additionally, the acceptability and resource availability to confront threats far from borders remain significant considerations, as does the ongoing technological evolution of capabilities and deterrence strategies.

The concept is tight and in a complex relation with the concepts of forward presence, deterrence, projection of power, forward posture, and credibility – both in terms of perception and concrete actions proving will, resolution, and factual applicability. Also, it changes with the technological generation. But the greatest change came with the rise of the historical distance from the use of nuclear weapons and today's nuclear ways of deterrence, the credibility of nuclear deterrence, and the lack of acceptability of its use in concrete wars. If the classic strategic and tactical nuclear deterrence is still here (credibility disputable, still), the acceptability of the use of sub-tactical and theatre small nuclear weapons is a recently opened subject by Russia (Tetrais 2018; Colas, 2023).

How to perform forward defense at sea begins to be challenged by the new hybrid approaches of China in the South China Sea, with harassment and water cannon shooting on vessels in international, territorial, or disputed waters of the Philippines. Forward defense is no longer achievable without allies and coalitions, based on common values or common interests alike. The forward defense is confronted with the conceptual debates about defending the country by defending allies and how far such an effort should go when forward defense is the defense of allies (Chifu & Simons 2017). Now, the new generation of forward defense is debating actions beyond the borders. Far away, outside of the territory. A real lesson learned from

Russia's war of aggression in Ukraine when we can see how difficult and painful it is to regain a territory after losing it, in such a way as to avoid that even an inch of the territory might fall under the control of an adversary.

The concept undoubtedly stems from empirical analysis and practical military needs. Therefore, this flexibility in interpretations and methods of enforcement—altering, nuancing, or adapting the concept—affirms its degree of universality. For instance, Washington's preferred option of "forward defense" in critical regions like East Asia is preparing to counter threats when and where they materialize rather than responding directly long after aggression has occurred or responding indirectly by imposing costs in other theatres by clearly and credibly signaling that the United States will oppose an adversary's aims and come to the assistance of its allies (Montgomery 2017). Forward defense, in this case, covers both deterrence and assurance as well as granting stability in the regions where it matters most.

Australia has a forward defense concept linked to its strategic geography that "dictates that we should plan on more pro-active operations which focus on defeating attacks in our maritime and air approaches before they reach Australian territory. (…), it is about being prepared to contribute actively to our objective of a secure Australia in a secure region" (Parliament of Australia 1997a). The idea of action outside the territory is recent also in Australia's Strategic Policy 1997 which conceded that the defense of Australia might involve operations forward of Australia's shoreline, emphasizing the pursuit of security interests external to territorial Australia (National Library of Australia 1997, 31-36).

Australia not only recognizes the relation of forward defense with the local geographic environment, relativizes the concept to this context and explicitly introduces requirements of defense outside of the territory – and on the territory of allies in the region, outside of the naval concept acceptable as an insular country – but it also regards the added value of this forward pro-active actions beyond its territory even though resources and capabilities do not fit a level of ambition to defend widely against any threat. It is notable that structuring of forces for significant operations in Eurasia under forward defense, even though Australia's forces were not decisive, they could be used and seen as a means of procuring future goodwill and security from major allies (Parliament of Australia 1997b).

The observation about capabilities comes also in the Turkish approach to forward defense. Analysts of those documents note that "without the cumulative growth in the defense industry over the last four decades, a pronounced shift to the current hard power approach would not have been possible. (…) The growth over time of an indigenous defense industry and, equally if not more important, the sense of power that it has reinforced in Ankara generates an aggressive stance and readiness for military action in multiple spheres" (Sinem 2020).
Another case is Singapore's defense policy from 1965 to the early 1980s, defined as forward defense, with Singapore's Armed Forces (SAF), focused on acquiring the

capability to conduct an offensive military campaign within Malaysia in the event of threats to Singapore's security or the continuity of its water supply from Malaysia (Yaacob 2022). That introduces a debate about the thin line between defensive and offensive actions and whether this approach to forward defense does not have an offensive side. In this context, the case of Iran's forward defense is an interesting one: Tehran's logic behind forward defense is "preempting the penetration of symmetric and asymmetric threats inside Iran's borders" (Barzegar, n.d.). The application of power in Iran's wider security zone can be seen as an offensive action, even though the concept has evolved over the last 40 years since Iran's practical military needs during the Iran-Iraq War led to the forward defense concept based on the proxy model and has also proven its utility.

When ISIS carried out its first attacks in Tehran in June 2017, Iran claimed that if it had not militarily intervened in Syria and Iraq, it would have had to confront a far greater ISIS threat inside its borders. But in this case, the concept of forward defense on a large scale is viewed as part of a grand strategy to expand its influence, being rather offensive than defensive, even though the concept and its application were, in the beginning, a contextual one coming from happening, not planning (Vatanka 2021a). This is because Tehran's reliance on forward defense and depending on foreign militias is mostly by choice in all the versions of geopolitical forward defense from Yemen to Syria to Libya. Nowadays, the political and military elite in Tehran have begun to rethink the concept and the sustainability of the forward defense doctrine (Vatanka 2021b), considering the gap between costs and benefits and the internal development needs.

Epistemological analysis proved that the concept is indeed very stable and the definition is clear and with an identity that recommended it for a concept of its own. The idea of applicability and concrete practical definition linked to regional or local situations and security environment is an acceptable variation and does not induce difficulties in the conceptual structure of forward defense. How this forward defense is reached and where – inside its own border as close as possible to the contact line, in front of the coastal line, in territorial waters or economic exclusive zones – in the case of the Navy – or outside the national territory, in what legal conditions, depending on the region, this is to be developed and covered by nuances and interpretations that do not relativize the concept. The same goes with the content of forward defense and its interpretations of some actions falling under the offensive realm in the process: we are coming back to the epistemological debate about the line between defensive and offensive actions in military studies, which is a classical one.

NATO's history on forward defense. Before the war came back to Europe

Forward defense is not a new concept in the transatlantic allied framework. In the first Strategic Concept of 1949, the forward defense was about deterrence by

punishment through the threat of American atomic weapons (Monaghan 2022). The original aim was to create a powerful deterrent to any nation or group of nations threatening the peace, independence, and stability of the North Atlantic family of nations (NATO 1950a) and deterrence by denial through positioning adequate forces to defend allied territory against invasion. NATO's denial strategy was one of forward defense designed to "arrest the enemy advance as far to the East as possible" and active opposition to peacetime aggression "by all measures short of war" (NATO 1950a). It is true, we were close to the Hiroshima and Nagasaki use of nuclear weapons, before the first Soviet nuclear test (29 August 1949). Therefore, the conceptual base was using the supreme weapons syndrome and relied only on this basis and on the then-present memory and impact of the use of this nuclear weapon.

It was with NATO's second strategic concept, in 1952 that a proper "forward strategy" for the defense of Europe was established, considering "to hold the enemy as far to the East in Germany as is feasible, using all offensive and defensive means available to deny or limit his freedom of action to the maximum extent" (NATO 1952). In 1957, we were discussing about forward deployed forces, with strategic bombers force in the forefront (NATO 1957). And in 1958, U.S. general Lauris Norstad, then Supreme Allied Commander Europe stated the aim of defending "as far forward as possible in order to maintain the integrity of the NATO area"- including Scandinavia (NATO 1957; NATO 1952). It was the first out-of-area-like mission, with forward defense accepting activities beyond NATO's territory.

In 1968, the forward defense had still an important nuclear component. We were after the Cuba crisis and the shift was from massive retaliation – the forward deterrent up to date – to flexible response. The threat of punishment through an overwhelming nuclear response to Soviet invasion or nuclear use was still in the Strategic Concept, with "massive retaliation" plus a forward-deployed "shield" force that NATO could rapidly reinforce. Moreover, in order to bolster the credibility of NATO shield forces, the fourth concept emphasized "rapid augmentation of its forward posture" through "appropriate echeloning in depth in suitable tactical locations," logistic support, tactical mobility, supplementing local forces with those of allies, and a fully trained, equipped, and ready NATO reserve force (US Department of State 1962).

In 1991, despite the existing nuclear threat from the Soviet Union, the strategic concept introduced a reduced forward presence. In fact, NATO's post–Cold War strategic concepts placed a new emphasis on the ability to project power out of the area through expeditionary operations. That was the new instrument for forward defense. For example, to meet the "significantly reduced level" of forces now assigned to NATO's Eastern Front, American forces based in Europe were reduced from 330,000 to 100,000 troops (Kugler & Binnendijk 2008, 45). If during the Cold War, "NATO's guiding operational paradigm was Forward Defense, from Northern Norway, across West Germany, to eastern Turkey, in the post-Cold War era the operational paradigm became NATO's capacity to conduct expeditionary operations of varying purpose and scale" (Palmer 2016).

In 2010, the forward defense force was replaced by a smaller forward presence through the concept of deterrence by reinforcement. Only in 2014, after the return of the change of European borders by military means, did NATO return to deterrence. "We, the Heads of State and Government of the member countries of the North Atlantic Alliance have gathered in Wales at a pivotal moment in Euro-Atlantic security. Russia's aggressive actions against Ukraine have fundamentally challenged our vision of a Europe whole, free, and at peace" (NATO 2014).

At this moment, some were even discussing the fact that the changes in NATO membership also created new areas for forward defense, most of which must now be fulfilled by former members of the Warsaw Pact. Those sources stated that aside from Poland, several of those countries were making very mixed efforts to develop military forces that are modern and interoperable with the forces of older NATO states, and these changes altered the major regions where NATO must conduct forward defense (Cordesman & Hwang 2021a) claiming that forward defense was, practically, impossible to enforce for practical reasons.

NATO's forward defense debate before and after Russia's war of aggression

The approach and interpretation of the forward defense concept in practice, in NATO's framework, was rather conservative and restrained. It came from the strict and conservative views at the European level and the consensus process of decision. The first reference mentioned that, in order to strengthen its deterrence credibility, NATO should also officially end its self-imposed restrictions on the permanent deployment of troops on the Eastern Flank (Wojciech 2022).

Leon Panetta found another condition on forward defense: America leading at the international stage - engaging other nations and building capable coalitions. So, more than ever, Americans must go abroad to remain secure at home, with a ready and well-trained military, forward-positioned and equipped with the most modern and advanced weapons and systems available. A typical American forward defense, in a NATO context, as well, but recognizing, at the same time, the limits of the capabilities: "the threats we confront are simply too numerous and complex for Americans to address alone. We simply lack the resources to defend our country and our citizens sufficiently against revisionist powers, rogue states, and terrorist organizations simultaneously" (Panetta 2020). Therefore, the solution to forward defense was a system of coalitions and alliances with a variable geometry.

The years after 1991 till the war led to a period of a sharp decline in US forces in Europe. In the period before 2014 and the beginning of the Russian war with Ukraine, U.S. troop numbers dropped from 222,500 to approximately 40,500. It is also estimated that the total troop strength for the entire U.S. European Command

(USEUCOM) deployed in Europe dropped from 283,100 to 66,998 (Cordesman & Hwang 2021b). Most European states in NATO cut their forces, had far lower rates of modernization, and cut back sharply on sustainability. The new allied states came with an added value but also created new burdens for forward defense. In this framework, forward defense shifted more conceptually to US total forces it could project into a forward combat zone, be it in cyber, space, precision and long-range conventional strike, deployable land-based air defenses, all becoming the subject of new U.S. force development programs (Cordesman & Hwang 2021b).

A new impetus to the development of the forward defense concept came with the war, in February 2022, when defense beyond the allied territory became once again interesting and subject of debate. The reinsurance and deterrence measures initiated since 2014 were insufficient for the allies of the Eastern Flank, especially for the Baltic space who lack a geographic space of retreat because they are small and narrow so a Russian attack scenario could have become a fait accompli. Even the shift from increased forward presence and deterrence to greater defense capability, decided by the Allies back in 2014 with the Readiness Action Plan (RAP), was no longer enough for the purpose that allied territory not to fall into Russian hands in the first place (Matlé 2023). So, NATO continued to evolve its military strategy away from a "forward presence" to a "forward defense" posture at the summit in Madrid, with brigade-strong forces that would be a central component of NATO's new strategy.

Ceding NATO territory to Russian forces, with the view to eventually retake it, leaves the citizens of those NATO and EU countries vulnerable, and all war crimes in Ukraine are proof of that (Bergmann & Svendsen 2023). NATO shifted from its Enhanced Forward Presence with multinational battlegroups to more permanent forward defense across the Eastern Flank, with 300,000 troops on high alert, a massive uptick from the 40,000 troops comprising the alliance's quick reaction force, the NATO Response Force, before Madrid Summit. That became the argument and capabilities needed for defending every inch of NATO territory, requiring NATO forces to have a high degree of combat readiness to fight a conventional war (Cancian & Monaghan 2023).

From forward presence and deterrence to forward posture and the new forward defense at NATO's borders

The United States assumed that it could no longer rely for the forward defense of its allies primarily on rapidly projecting power at the time of need to defend allies and partners in the Western Pacific and Europe against Chinese or Russian aggression. Combat-credible U.S. forward posture in the Western Pacific and Europe can offset the United States' time-distance disadvantage, so the interest moved to build a forward posture to "deny a quick and cheap Chinese or Russian victory while buying time for the full weight of U.S. power to be brought to bear" (Fabian 2020).

The Pentagon introduced the criteria of credibility – for their own citizen, for the allied countries, and the adversaries alike – of its US forward posture. Coming back to three main lines: (1) it must be sufficiently lethal and resilient to fight outnumbered on highly contested battlefields from the start of a conflict; (2) it should be integrated with the forces of allies and partners to form a cohesive, combined defensive posture; and (3) it must receive rapid reinforcement and resupply in the event of a war (Fabian 2020). On the contrary, any withdrawal of U.S. forces for any reasons – from costs, non-observance of the Defense Pledge, a China-First policy in DC, would jeopardize U.S. national security interests and represents unexpected messages for the authoritarian regimes in China, Russia, Iran, North Korea, and elsewhere.

The solutions in Europe of such a forward posture combat-credible would mean extending the U.S. military to fit into an operational concept of deterrence by denial, an enhanced military presence, of approximately 100,000 American personnel in Europe, based on the current 5+2 model that maintains five total brigade combat teams (BCTs), including the two additional BCTs deployed after Russia's invasion (one rotational armored brigade combat team and one rotational infantry brigade combat team in Romania) in addition to the pre-war units (a forward-stationed IBCT and Stryker brigade combat team based in Italy and Germany, respectively, and one rotational ABCT as part of Operation Atlantic Resolve) (Jones, Daniels, Doxsee, Fata, & McInnis 2024). This posture would maintain the seven fighter squadrons currently forward deployed and add a persistent rotational deployment of fifth-generation aircraft to NATO's Eastern Flank.

"What we are looking for from NATO in this next phase is long-term planning for how it will contain Russia post-Ukraine and provide resilience and reassurance to countries that cannot do that on their own. That could be permanent basing or it could be rapid readiness - being able to deploy quickly, instead of being stuck in a big base in one place. That is all up for development, which I think is incredibly important" (Wallace 2022).

This led to NATO's defense and deterrence reset in Madrid, but that should be moved ahead in Washington DC with planning against Russian "Maximum Intentions" (NATO 1950b). This could mean coming back to NATO, coming back to its strategy of the sword and the shield in its 1957 form, a combination of strategic nuclear forces to deter attack through the threat of massive retaliation, alongside the forward defense of NATO's Eastern front through the basing of significant forces as far East as possible. That could explain, partially, Putin's return to the nuclear rhetoric and saber rattling, however, based more on reaffirming a symbolic return to its last argument of superpower, after the degradation of its conventional forces in Ukraine.

Some ideas for the new forward defense content could be also brought from Australia's recent documents. The 2020 Defence Strategic Update states: 'The

capacity to conduct cooperative defense activities with countries in the region is fundamental to our ability to shape our strategic environment'. The 2023 Defence Strategic Review takes this concept further, stating: 'To protect (Australia's) strategic interests, we must contribute to the maintenance of a regional balance of power in the Indo-Pacific that is favorable to our interests' and 'We must posture for the protection of Australia and for integrated defense and deterrence effects in our immediate region'.

In this case, 'forward presence' is defined as the presence of formed units or sub-units beyond the main domestic raise-train-sustain areas. This definition encompasses a long presence; open-ended rotational deployment; and the permanent stationing of forward presence forces. Forward presence can support many different objectives, including defense diplomacy or direct assistance for political influence; capacity building to increase self-help; and demonstration of commitments. In this paper, we focused on what is arguably the most difficult and demanding – and, for Australia, also the most unfamiliar – form of forward presence: the deployment of armed forces to signal a deterrence commitment (Australian Army Research Centre 2023).

The success factors for forward presence as a deterrence posture are rating forward presence under the conditions of deterring by denial and defending beyond the national territory, a conceptual framework that identifies 'forward defense', which seeks to deter by denying the adversary, its intended objective, albeit within a broader national strategy for reinforcement and potential escalation (Australian Army Research Centren 2023).

From our perspective, the new concept of forward defense should clearly address the need for contiguous zones where deterrence by denial is reinforced by additional instruments. The NATO Eastern Flank has already witnessed breaches and threats stemming from the war of aggression in Ukraine, such as drones entering the airspace and debris from missiles or artillery causing destruction upon impact. This might entail establishing no-fly zones in proximity to Alliance territory, with the agreement of sovereign states where possible, and authorization to intercept any military aircraft crossing a designated line outside Alliance territory to prevent it from reaching NATO's territory or harming Alliance citizens. Additionally, integrated ballistic and air defense with partner states should be established to protect allied territory and citizens, alongside those of sovereign states. A transparent doctrine of forward defense should be publicly communicated to warn, prevent, and deter any transgressions in this regard.

References

Areteos, E. 2020. "Mavi Vatan and Forward Defense. The Sinuous Journey of a Republican and Imperial Hybridization." Diplomatic Academy, University of Nicosia: https://www.unic.ac.cy/da/wp-content/uploads/sites/11/2020/07/Mavi-Vatan-and-Forward-Defence-Evangelos-Areteos.pdf

Australian Army Research Centre. 2023. *Forward Presence for Deterrence. Implications for the Australian Army.* Occasional Paper No. 15. https://researchcentre.army.gov.au/sites/default/files/op_15_-_forward_presence_for_deterrence.pdf

Barzegar, K. n.d. *The Assassination of Qassem Soleimani Institutionalized Anti-American Sentiment in Iran.* Middle East Political and Economic Institute – MEPEI. https://mepei.com/the-assassination-of-qassem-soleimani-institutionalizes-anti-american-senti.

Bergmann, M., & Svendsen, O. 2023. *The Transatlantic Strategic Landscape in Transforming European Defense. A New Focus on Integration.* Center for Strategic and International Studies (CSIS). https://www.jstor.org/stable/resrep51361.5

Cancian, M. F., & Monaghan, S. 2023. *Made in Madrid NATO's Commitments to Strengthen Defense and Deterrence in Repel, Don't Expel. Strengthening NATO's Defense and Deterrence in the Baltic States.* Center for Strategic and International Studies (CSIS). https://www.jstor.org/stable/resrep52042.8.

Chifu, I., & Simons, G. 2017. *The Changing Face of Warfare in the 21st Century.* London and New York: Routledge.

Chifu, I., & Simons, G. 2023. *Rethinking warfare in the 21st Century. The influence and effects of the Politics, Information and Communication Mix.* Cambridge University Press.

Chifu, I., & Țuțuianu, S. 2017. *Torn Between East and West: Europe's Border States.* London and New York: Routledge.

Colas, B. 2023. "A Rational Choice." *Æther: A Journal of Strategic Airpower & Spacepower, 2*(2), pp. 18-30.

Cordesman, A. H., & Hwang, G. 2021a. *Expand Upon the NATO 2030 Strategy and Work in the NATO 2021 Summit in Brussels to Develop Clear National Forces Plans to Address the Major Weaknesses in National Military Forces and National Contributions to NATO*. In *StrengtheEuropean Deterrence and Defense: NATO, NOT European Defense Autonomy, Is the Answer* (pp. 16-26). Center for Strategic and International Studies (CSIS). https://www.jstor.org/stable/resrep35122.6

Cordesman, A. H., & Hwang, G. 2021b. *Have the U.S. Clearly and Decisively Make Its Continued Commitment to NATO, Europe, and Extended Deterrence Clear in Strengthening European Deterrence and Defense.* In *NATO, NOT European Defense Autonomy, Is the Answer.* Center for Strategic and International Studies (CSIS). https://www.jstor.org/stable/resrep35122.5

Fabian, B. 2020. *Overcoming the Tyranny of Time: The Role of U.S. Forward Posture in Deterrence and Defense.* https://www.cnas.org/publications/commentary/overcoming-the-tyranny-of-time-the-role-of-u-s-forward-posture-in-deterrence-and-defense

Jones, S. G., Daniels, S. P., Doxsee, C., Fata, D., & McInnis, K. 2024. *Alternative options - Forward defence. Strengthening U.S. force posture in Europe.* Center for Strategic and International Studies (CSIS). https://www.jstor.org/stable/resrep58186.10

Kugler, R. L., & Binnendijk, H. 2008. *Toward a New Transatlantic Compact.* Center for Technology and National Security Policy, National Defense University. https://apps.dtic.mil/sti/pdfs/ADA486328.pdf

Matlé, A. 2023. *From "Forward – Presence" to – "Forward Defense". Germany Must Strengthen – NATO's Northeastern Flank in Lithuania.* German Council on Forward Relations, DGAP. https://dgap.org/en/research/publications/forward-presence-forward-defense

Ministry of Foreign Affairs of the Russian Federation. 2021. *Press release on Russian draft documents on legal security guarantees from the United States and NATO*. https://www.mid.ru/en/forward_ policy/news/1790809/

Ministry of Foreign Affairs of the Russian Federation. 2024. *Forward Minister Sergey Lavrov's remarks and answers to media questions following a UN Security Council meeting on Ukraine and an open debate on "The situation in the Middle East, including the Palestinian question*. https://mid.ru/en/forward_policy/news/1927568/

Monaghan, S. 2022. *Resetting NATO's Defense and Deterrence. The Sword and the Shield Redux.* Center for Strategic and International Studies (CSIS). https://www.jstor.org/stable/resrep41893

Montgomery, E. B. 2017. *Reinforcing the Front Line: U.S. Defense Strategy and the Rise of China. Centre for Strategic and Budgetary Assessments.* https://csbaonline.org/research/publications/reinforcing-the-front-line-u.s.-defense-strategy-and-the-rise-of-china

National Library of Australia. 1997. *Australia's Strategic Policy*. https://catalogue.nla.gov.au/catalog/1699161

NATO. 1950a. *North Atlantic Defense Committee Decision on D.C. 13. A Report by the Military Committee on North Atlantic Treaty Organization on Medium Term Plan.* https://www.nato.int/docu/stratdoc/eng/a500328d.pdf

—. 1950b. *North Atlantic Military Committee Decision on M.C. 14 Strategic Guidance for the North Atlantic Regional Planning.* https://www.nato.int/docu/stratdoc/eng/a500328c.pdf

—. 1952. *North Atlantic Military Committee Decision on M.C. 14/1. A Report by the Standing Group on Strategic Guidance.* https://www.nato.int/docu/stratdoc/eng/a521209a.pdf

—. 1957. *Final Decision on MC 48/2, A Report by the Military Committee on Measures to Implement the Strategic Concept.* https:// www.nato.int/docu/stratdoc/eng/a570523b.pdf

—. 2014. *Wales Summit Declaration*. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

—. 2024. *Funding NATO*. https://www.nato.int/cps/en/natohq/topics_67655.htm#:~:text=At%20the%202023%20Vilnius%20Summit,of%20GDP%20annually%20on%20defence

Palmer, D. A. 2016. *The Framework Nations' Concept and NATO: Game-Changer for a New Strategic Era or Missed Opportunity?* Reasearch Division - NATO Defence College. Reasearch Paper No. 132. https://www. ndc.nato.int/news/news.php?icode=965

Panetta, L. 2020. *Defending Forward. Securing America by Projecting Military Power Abroad.* Foundation for Defense of Democracies: https://www.fdd.org/analysis/2020/12/15/defending-forward/

Parliament of Australia. 1997a. *The Suitability of the Australian Army for Peacetime, Peacekeeping and War*. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Completed_Inquiries/jfadt/army/issues

—. 1997b. *Australia's Defense Strategy*. https___aphref.aph.gov.au_house_committee_jfadt_army_armych_3.pdf

President of Russia. 2024. *Presidential address to the Federal Assembly*. http://www.en.kremlin.ru/events/president/transcripts/messages/73585

Romaniecki, L. 2016. *Sources of the Brezhnev Doctrine of Limited Sovereignty and Intervention.* Cambridge University Press. https://www.cambridge.org/core/journals/israel-law-review/article/abs/sources-of-the-brezhnev-doctrine-of-limited-sovereignty-and-intervention/8BDA7DB7C09CE79EFEB1F5AFE3CC905C

Sinem, A. 2020. Understanding Turkey's Increasingly Militaristic Forward Policy. *MENA Politics Newsletter, 3*(1).

Taspinar, Ö. 2008. *Turkey's Middle East Policies: Between Neo-Ottomanism and Kemalism. Carnegie Papers.* https://carnegieendowment.org/2008/10/07/turkey-s-middle-east-policies-between-neo-ottomanism-and-kemalism-pub-22209

Tetrais, B. 2018. Russia's Nuclear Policy: Worrying for the Wrong Reasons. *Survival, 60*(2), 33-44. doi:10.1080/00396338.2018.1448560

US Department of Commerce. 2020. *A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals*. https://www.commerce.gov/sites/default/files/2020-01/Critical_Minerals_Strategy_Final.pdf

US Department of State - Bureau of Consular Affairs. n.d.. *International Travel*. https://travel.state.gov/content/travel/en/international-travel.html

US Department of State. 1962. Address by Secretary of Defense McNamara at the Ministerial Meeting of the North Atlantic Council. Document 82, Foreign Relations of the United States 1961-1963, Vol.VIII, National Security Policy.

Vatanka, A. 2021a. *Conclusion: Is "Forward Defense" A Sustainable Military Doctrine in Whither the IRGC of the 2020s? Is Iran's Proxy Warfare Strategy of Forward Defense Sustainable?* New America. https://www.jstor.org/stable/resrep28480.6

—. 2021b. *Soleimani Ascendant: The Origins of Iran's "Forward Defense" in Whither the IRGC of the 2020s? Is Iran's Proxy Warfare Strategy of Forward Defense Sustainable?* New America. https://www.jstor.org/stable/resrep28480.5

Wallace, B. 2022. *NATO and International Security.* U.K. Parliament, Hansard. https://hansard.parliament.uk/commons/2022-05-19/debates/D190232B-3733-4708-B5AA-3EF5A40C2A24/NATOAndInternationalSecurity

Wojciech, L. 2022. *Forward Defence: a New Approach to NATO's Defence and Deterrence Policy.* PISM paper no 2 (210). https://www.pism.pl/publications/forward-defence-a-new-approach-to-natos-defence-and-deterrence-policy

Yaacob, A. R. 2022. Towards a 'Forward Defence' for Singapore: Revisiting the Strategy of the Singapore Armed Forces 1971-1978. *British Journal for Military History, 8* (3). https://journals.gold.ac.uk/index.php/bjmh//article/view/1650

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Leveraging of role-play games in military training cadets within the ongoing conflict in Ukraine

Ph.D. (Economics), Associate Professor Kira HORIACHEVA*
Doctor (Pedagogy), Professor Vadym RYZHYKOV**

*Military Institute of the Taras Shevchenko National University of Kyiv
e-mail: horyachevakira@gmail.com
**Military Institute of the Taras Shevchenko National University of Kyiv
e-mail: vadr66@ukr.net

Abstract

In the realm of professional military education, innovative pedagogical methodologies are pivotal for fostering strategic thinking and adaptive leadership qualities among cadets. This paper delves into the effectiveness of role-play games as a means of experiential learning within military training, with a particular emphasis on the Ukrainian defense and security sector amidst the ongoing conflict. Drawing from insights gleaned from research papers and practical applications this study examines how role-playing games intersect with cadet training. By analyzing various approaches and practical examples, we aim to illuminate the potential of role-play games in enhancing strategic mindsets and decision-making skills among future military leaders. Understanding the dynamics of incorporating role-playing into military pedagogy is crucial for optimizing the educational experience of cadets and preparing them to navigate the complexities of contemporary warfare effectively.

Keywords:

professional military education; role-playing game; experiential learning; war in Ukraine; defense and security sector; cadet training.

Article info
Received: 22 April 2024; Revised: 28 May 2024; Accepted: 3 June 2024; Available online: 5 July 2024

Citation: Horiacheva, K. and V. Ryzhykov 2024. "Leveraging of role-play games in military training cadets within the ongoing conflict in Ukraine". *Bulletin of "Carol I" National Defence University*, 13(2): 21-29. https://doi.org/10.53477/2284-9378-24-17

Military professional education stands as a cornerstone in shaping the next generation of military leaders, particularly in regions embroiled in conflict like Ukraine. Amidst the ongoing war, it is imperative to explore innovative pedagogical strategies that equip cadets with the necessary skills to navigate the complexities of modern warfare. This paper explores the integration of role-play games as a pedagogical tool within professional military education, focusing on their potential to cultivate strategic mindsets and adaptive decision-making abilities among cadets. This exploration aims to bridge theoretical frameworks with real-world implementation. By examining the intersection of role-playing games with cadet training, we seek to elucidate their role in enhancing experiential learning and preparing future military leaders for the multifaceted challenges they will face in their careers. Understanding the implications of incorporating role-playing methodology into military professional education is essential for ensuring the readiness and effectiveness of defense forces in conflict-affected regions like Ukraine. Against the backdrop of the ongoing war in Ukraine, the integration of innovative teaching methodologies is imperative for ensuring the readiness and effectiveness of the Armed Forces.

Theoretical Framework

Role-play games serve as a dynamic and immersive method for experiential learning within military training contexts, drawing upon principles of experiential learning and cognitive psychology. According to Dewey (Dewey 1938), experiential learning involves active engagement with real-world situations, enabling learners to construct meaning and develop critical skills through reflection and experience. Role-play games provide a structured yet flexible framework for participants to engage in simulated scenarios, allowing for active experimentation and learning by doing.
Cognitive psychology offers insights into the cognitive processes involved in role-playing and its effectiveness as a learning tool. Bandura's social cognitive theory (Bandura 1977) posits that individuals learn through observation, imitation, and modeling. In the context of role-play games, participants observe and interact with each other, modeling behaviors and decision-making strategies that are conducive to effective leadership and problem-solving.

Moreover, role-play games facilitate the development of critical thinking skills essential for military leadership roles. By immersing participants in dynamic and interactive scenarios, role-play games require them to analyze information, evaluate alternatives, and make decisions under pressure. This process mirrors the cognitive demands of real-world military operations, helping participants refine their decision-making abilities in a safe and controlled environment.

Situational awareness, another crucial aspect of military leadership, is enhanced through participation in role-play games (Horiacheva, et al. 2023). By simulating

complex and evolving scenarios, role-play games challenge participants to maintain awareness of their surroundings, anticipate potential threats, and adapt their strategies accordingly. This heightened awareness translates into improved performance in real-world situations, where split-second decisions can have significant consequences.

Collaborative problem-solving is also fostered within the context of role-play games. Participants must work together to achieve common goals, communicate effectively, and coordinate their actions to overcome obstacles. This collaborative approach mirrors the teamwork and cooperation required in military operations, where success often depends on the ability of individuals to work together towards a shared objective.

Overall, the theoretical underpinnings of role-play games in military training highlight their effectiveness in facilitating experiential learning and developing critical skills essential for military leadership roles. By immersing participants in dynamic scenarios, role-play games offer a unique opportunity for hands-on learning and skill development, preparing future military leaders to navigate the complexities of modern warfare effectively.

Furthermore, insights from the aforementioned sources underscore the importance of incorporating role-play games into military training curricula as a means of enhancing the readiness and effectiveness of defense forces. As the nature of warfare continues to evolve, innovative pedagogical approaches like role-play games will play an increasingly crucial role in preparing cadets for the multifaceted challenges they will encounter in their military careers.

Role-Play Games in Military Training

Role-play games serve as a valuable pedagogical tool in professional military education, offering cadets hands-on experience and opportunities for skill development in a controlled environment. Drawing upon insights from the aforementioned sources, this section delves into the practical application of role-play games within cadet training programs, highlighting their versatility and effectiveness in simulating real-world scenarios (Yao and Huang 2021).

One of the primary benefits of role-play games is their ability to simulate diverse and complex scenarios encountered in military operations. By creating immersive environments that mirror the challenges of tactical operations, diplomatic negotiations, and humanitarian missions, role-play games provide cadets with a platform to apply theoretical knowledge in practical settings. This experiential learning approach enables cadets to develop critical skills such as decision-making, problem-solving, and leadership under realistic conditions.

Moreover, role-play games offer cadets the opportunity to receive immediate feedback and guidance from instructors and peers. Through debriefing sessions and post-game discussions, cadets can reflect on their performance, identify areas for improvement, and refine their strategies for future scenarios. This feedback loop fosters a culture of continuous learning and improvement, ensuring that cadets are better prepared to handle the complexities of real-world military operations.

Incorporating role-play games into cadet training programs also enhances the development of practical skills and strategic acumen. By actively participating in simulated scenarios, cadets gain hands-on experience in applying military tactics, conducting risk assessments, and making mission-critical decisions. This practical experience not only reinforces theoretical concepts but also instills confidence and competence in cadets as they transition to operational roles within the military.

Furthermore, role-play games promote collaboration and teamwork among cadets, essential qualities for effective military leadership. By working together to achieve common objectives, cadets learn to communicate effectively, coordinate their actions, and leverage each other's strengths to overcome challenges. This collaborative approach mirrors the dynamics of real-world military operations, where success often depends on the ability of individuals to work cohesively as part of a team (Bumbuc 2020).

The integration of role-play games into cadet training programs is also conducive to fostering creativity and innovation (Vartanian, et al. 2022). By encouraging cadets to think outside the box and explore unconventional solutions to complex problems, role-play games stimulate intellectual curiosity and promote a culture of innovation within the military. This innovative mindset is essential for adapting to evolving threats and maintaining a competitive edge in today's dynamic security environment.

Overall, role-play games play a vital role in enhancing the effectiveness of cadet training programs by providing experiential learning opportunities, fostering practical skills development, and promoting collaboration and innovation. As military education continues to evolve to meet the challenges of modern warfare, the incorporation of role-play games offers a promising approach for preparing cadets to excel in their future roles as military leaders. By leveraging the insights and experiences gained from role-play games, cadets can better navigate the complexities of contemporary military operations and contribute to the success of their respective defense forces.

Practical Example

The implementation of role-play games in cadet training within Ukrainian military institutes has demonstrated notable success, particularly within the context of the

ongoing conflict in Ukraine. This practical example exemplifies the effectiveness and versatility of role-play games in preparing cadets for the multifaceted challenges of contemporary conflict environments (NATO 2021). Drawing upon insights from the provided sources, this section delves into specific examples of scenario-based exercises and their impact on cadet training.

Such an example is the integration of role-play games into the "Military Psychology and Pedagogy (Military Leadership)" course within the young officer master's degree education program at the Military Institute (Ministry of Defence of Ukraine 2023). This course is designed to equip cadets with the psychological and pedagogical skills necessary for effective military leadership. As part of this course, cadets engage in practical role-play exercises that simulate real-world scenarios encountered in military operations.

One practical session within this course focuses on addressing asymmetric warfare tactics, a prevalent challenge faced by the Ukrainian military in the context of the ongoing conflict. Cadets are divided into teams and tasked with developing strategic responses to simulated asymmetric threats, such as guerrilla warfare tactics and cyber-attacks. Through role-play scenarios, cadets are challenged to think critically, adapt to dynamic situations, and collaborate with their peers to devise effective countermeasures.

Another practical session centers on counterinsurgency operations, a key aspect of modern warfare in conflict-affected regions like Ukraine. Cadets are immersed in simulated scenarios that replicate the complexities of counterinsurgency campaigns, including engaging with local populations, conducting intelligence-gathering operations, and implementing stabilization efforts. Role-play games provide cadets with hands-on experience in navigating the intricacies of counterinsurgency operations, allowing them to develop practical skills and strategies for addressing insurgency threats effectively.

Additionally, cadets participate in role-play exercises focused on crisis management strategies, preparing them to respond to emergencies and crises in high-pressure environments. These scenarios simulate various crisis situations, such as natural disasters, terrorist attacks, or civil unrest, requiring cadets to make quick and informed decisions to mitigate risks and ensure the safety and security of personnel and assets.

The integration of role-play games into cadet training within the "Military Psychology and Pedagogy (Military Leadership)" course underscores their effectiveness in enhancing experiential learning and skill development. By immersing cadets in realistic scenarios, role-play games provide invaluable opportunities for practical application of theoretical knowledge, fostering critical thinking, decision-making, and teamwork skills essential for military leadership roles.

In conclusion, this practical example demonstrates the significant impact of role-play games on cadet training within Ukrainian military institutes, particularly in preparing cadets for the challenges of contemporary conflict environments. Through practical sessions integrated into the "Military Psychology and Pedagogy (Military Leadership)" course, cadets gain valuable hands-on experience and develop essential skills for effective military leadership. The incorporation of role-play games into cadet training programs exemplifies a proactive approach to preparing future military leaders to navigate the complexities of modern warfare effectively.

Implications for Professional Military Education

The integration of role-play games into the curriculum of military training institutions holds significant implications for professional military education. Drawing upon insights from the provided sources, this section explores the multifaceted benefits of incorporating role-play games and their impact on the preparedness of future military leaders for the realities of modern warfare.

One of the primary implications of integrating role-play games into professional military education is the enhancement of experiential learning opportunities. By immersing cadets in dynamic and realistic scenarios, role-play games provide a hands-on approach to learning that complements traditional classroom instruction. This experiential learning methodology enables cadets to apply theoretical knowledge in practical contexts, fostering the development of critical thinking, decision-making, and problem-solving skills essential for effective military leadership (Ryzhykov 2021).

Moreover, role-play games facilitate the development of strategic mindsets among cadets, preparing them to navigate the complexities of modern warfare with agility and adaptability. Through simulated scenarios that replicate real-world challenges, cadets gain valuable insights into strategic planning, operational decision-making, and risk assessment. This strategic perspective enables cadets to anticipate and respond effectively to evolving threats and uncertainties, enhancing the readiness and resilience of future military leaders.

Another implication of integrating role-play games into professional military education is the cultivation of adaptive leadership qualities. By participating in role-play exercises that require them to assume leadership roles and make decisions under pressure, cadets develop confidence, resilience, and interpersonal skills essential for effective leadership in dynamic and high-stakes environments. This experiential approach to leadership development fosters a culture of innovation and agility within the military, enabling leaders to respond effectively to changing circumstances and emerging challenges (Iskandarov and Gawliczek 2018).
Furthermore, role-play games promote cross-functional collaboration and teamwork

among cadets, reflecting the importance of collective action in military operations. By working together to achieve common objectives, cadets learn to communicate effectively, leverage each other's strengths, and coordinate their actions to achieve mission success. This collaborative approach fosters a sense of camaraderie and mutual trust among cadets, enhancing unit cohesion and operational effectiveness.

In conclusion, the integration of role-play games into professional military education represents a proactive approach to preparing future military leaders for the realities of modern warfare. By providing experiential learning opportunities, fostering strategic mindsets, cultivating adaptive leadership qualities, and promoting cross-functional collaboration, role-play games enhance the readiness and resilience of cadets to meet the challenges of contemporary security environments. As military education continues to evolve to meet the demands of the 21st century, the incorporation of role-play games offers a promising avenue for enhancing the effectiveness of professional military education and ensuring the success of defense forces in an increasingly complex and unpredictable world.

The integration of role-play games into professional military education offers significant advantages in preparing cadets for the challenges of contemporary warfare. Table no. 1 visually represents the main advantages of using role-play games in military training and their impact on the development of skills and qualities of future military leaders. Building upon the insights this conclusion synthesizes the overarching implications of incorporating role-play games into military training curricula within the context of the ongoing conflict in Ukraine.

TABLE 1 Advantages of using role-play games in military training

Advantages of Using Role-Play Games in Military Training	
Development of Strategic Thinking	Role-play games contribute to the formation of strategic skills and decision-making abilities in uncertain conditions
Experiential Learning	Participation in role-play games provides cadets with practical skills and experience, complementing theoretical learning
Preparation for Real Scenarios	Role-play games allow for the simulation of real military operation scenarios, helping cadets adapt to actual conditions
Development of Leadership Qualities	Engaging in role-play games promotes the development of leadership skills such as command, organization, and decision-making
Promotion of Teamwork	Role-play games foster the formation of teamwork and communication skills necessary for successful task execution within a team

Conclusions

In conclusion, role-play games serve as a multifaceted tool for fostering strategic mindsets among cadets, enabling them to develop the cognitive flexibility and forward-thinking necessary for effective military leadership. By immersing cadets in dynamic and realistic scenarios, role-play games encourage strategic thinking, scenario planning, and decision-making, preparing cadets to navigate complex and unpredictable operational environments with confidence and competence.
Furthermore, the integration of role-play games enhances experiential learning within professional military education, complementing traditional classroom instruction with hands-on, practical experiences.
As Ukraine continues to confront security challenges amidst the ongoing war, the importance of innovative pedagogical methodologies cannot be overstated.

In essence, role-play games offer a valuable avenue for bridging theory and practice within professional military education, empowering cadets to apply theoretical knowledge in practical contexts and develop the critical skills and competencies required for effective military leadership. As military education continues to evolve, the integration of role-play games serves as a testament to the commitment of military institutions to provide cadets with the highest caliber of training and preparation for the challenges of contemporary conflict environments.

References

Bandura, Albert. 1977. *Social Learning Theory.* Englewwood Cliffs: NJ: Prentice-Hall.

Bumbuc, Stefania. 2020. "Using the Role-Play Method in Military Pedagogy." *Land Forces Academy Review* 25 (4): 317-324. doi:10.2478/raft-2020-0038.

Dewey, John. 1938. *Experience and Education.* New York: Macmillan Company.

Farhad, Manjoo. 2017. *Snap Makes a Bet on the Cultural Supremacy of the Camera.* New York Times.

Horiacheva, Kira, Anatily Yurkov, Andrii Savchenko, Nataliia Snapkova, and Dmytro Kilderov. 2023. "Formation of Military Leadership Throught the Lens of History." *Cuestiones Politicas* 41 (78): 554-563.

Iskandarov, Khayal, and Piotr Gawliczek. 2018. "NATO's role in improving professional military education with a focus on the south Caucasus countries." *The Quarterly Journal* 18 (3-4): 35-44.

LaSalle, Peter. 2017. *Conundrum:A Story about Reading.* New England Review.

Manjoo, Farhad. 2017. *Snap Makes a Bet on the Cultural Supremacy of the Camera.* New York Times.

Ministry of Defence of Ukraine. 2023. *Educational and pedagogical sciences.* Kyiv: National Defence University of Ukraine. https://nuou.org.ua/assets/documents/onp_011_en.pdf.

NATO. 2021. "NATO Science presents: Training by gaming." Brussels: NATO Headquarters. https://www.nato.int/cps/en/natohq/news_180639.htm.

Ryzhykov, Vadym. 2021. "Changes in Training Methods in the Armed Forces of Ukraine Servicemen According to the World's Current Practices of Military Education." *Security Challenges of Europe* pp. 62-70.

Vartanian, Oshin, Cathy Boscarino, Jerzy Jarmasz, and Vlad Zotov. 2022. "Training-Related Stress and Performance in the Military." In *Handbook of Military Sciences*, pp. 1-21. SpringerLink.

Yao, Kai, and Shaoluo Huang. 2021. "Simulation Technology and Analysis of Military Simulation Training." *Journal of Physics: Conference Series.* 1746(1):012020. doi:10.1088/1742-6596/1746/1/012020.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

The mixed system of complementing the armed forces – a requirement for the Republic of Moldova

Ion COROPCEAN, Ph.D.*

*Agency for Science and Military Memory, Republic of Moldova
e-mail: ion.coropcean@gmail.com

Abstract

Military service is a complex social and legal phenomenon that is at the basis of the completion and functioning of the armed forces. Depending on the completion system, the armed forces may be composed of conscripts, volunteers and/or professional military personnel. Contract-based military service significantly contributes to strengthening the armed forces' operational capabilities. Conscript military service is the main form for the military training of citizens who are later included in the reserve to ensure the mobilization of the army. The mixed system of complementing the armed forces organized in the Republic of Moldova responds to the interests of the military construction in the new security conditions after the start of the war in Ukraine.

Keywords:
the system of complementing the armed forces; mixed system; military service; type of army; professionalization of the army; reserve of the armed forces.

Article info
Received: 9 May 2024; Revised: 3 June 2024; Accepted: 13 June 2024; Available online: 5 July 2024

Citation: Coropcean, I. 2024. "The mixed system of complementing the armed forces – a requirement for the Republic of Moldova". *Bulletin of "Carol I" National Defence University*, 13(2): 30-43. https://doi.org/10.53477/2284-9378-24-18

An important task of military policy in the Republic of Moldova is the organization of military construction in sufficient volume to ensure the military security of the state. Traditionally, military construction consists of economic, scientific, technical, social, political, and military measures. The main elements of military construction are the armed forces. In this context, military service, as a subject of military policy, ensures the effective functionality of the armed forces and contributes to the development of each military member's required capabilities. (Coropcean, Juc and Manolache 2019, 64).

Types of armies and their complement system

Currently, we distinguish among the following types of armies: *mass army; professional army, and mixed army.* Each type of army is characterized by a method of complementing military personnel and organizing military service. In our opinion, the type of army holds primacy, within which a part is a method of complementing and organizing military service. This is determined by the criterion of volunteering or recruiting military personnel for a predetermined term (soldiers and graduates).

Thus, as a general feature of *the mass army*, we will mention the fact that a significant part of the military personnel, i.e. the military for a pre-determined term, perform the mandatory military service, arriving in the army through conscription. *Conscription,* is a way of recruiting an important part of the army's forces (it is about conscripts or ordinary soldiers), translated into the obligation of all citizens of the country, who meet the conditions provided by law, to perform military training. Among the arguments brought by researchers in favor of conscription are: the emergence and development of the feeling of defending the country; strengthening the link between the military institution and the nation it belongs to; and decreasing costs as there are lower costs for conscription than for professional military personnel; ensuring the necessary and sufficient human reserves in case of war.

The professional army is expressed through voluntary employment in the military institution of the entire military force, all of whom have professional training specific to the positions and functions for which they are assigned. The acceptance or rejection of applicants is done according to complex criteria and, as a rule, through competition. This type of army is specific to developed industrial states, which can massively endow themselves with modern military equipment. We will note that the emergence and evolution of the professional army proves to be an adequate response to the changes produced in the security environment at both national and international levels.

The mixed army represents the military institution in which both ordinary soldiers, from conscription, and volunteers meet, in addition to career military (officers, warrant officers, and non-commissioned officers). The proportion in which

one recruitment method or another is used depends on an extended spectrum of economic, political, social, demographic, and military factors, and trends of evolution of the national, regional, and global security environment. Such a type of army is also found in states with a high level of economic development, which may or may not belong to a political-military alliance (Duțu, Moştoflei and Sarcinschi 2003, 3-4).

In the specialized literature at the beginning of the 2000s, reference is made to the advantages and disadvantages of military service based on conscription, in comparison with the professional one, starting from the natural approach of the factors (internal and international) that determine the transition from the mass army to the mixed army or by professionals. The professionalization of the army is a very sensitive political issue with major implications for the management and structure of the armed forces, and the process of making such a decision involves the analysis of several factors.

Among the international factors that stand out, we could mention: the diminishing or even the apparent absence of the danger represented by a massive external military attack on any European state; the disappearance of interstate wars, at least in Europe, and the intensification of intrastate wars of ethnic or religious origin; the emergence and manifestation on the international level in terms of defense and security, in addition to traditional actors (states), of non-state actors (political-military and other organizations); the emergence and manifestation of new dangers and security threats: international terrorism, the proliferation of weapons of mass destruction and their specific vectors, organized crime, regional conflicts; illegal migration; the transformation of the political-military organization of which the respective state is a member.

Among the internal factors that determined the transformations within the army, the following can be found: *the psychosocial factor*: the evolution of mentalities in society, especially those aimed at the "spirit of defense" and the military-citizen connection. An important role seems to have been played by the gaps manifested during conscription as a method of recruiting the military (ranked and soldiers) and the lack of legitimacy in the eyes of the population of compulsory military service; *the technological factor:* the increase in the degree of technicalization of armaments and the introduction of new technologies, especially of information and communications, require well-trained and specialized soldiers in top fields; *the economic factor:* more and more European states, after 1990, started to decrease the budgets for defense, given the new geostrategic and geopolitical context; *the military factor*: the evolution of contemporary conflicts resulting in the quasi-disappearance of mass confrontations in favor of punctual, "targeted" and multifaceted international crises related to a certain form of external aspects of the professionalization of the army, the internal ones being much more important (Duțu 2008, 118-120).
In this framework of analysis, the Romanian researcher A. Sarcinschi emphasizes that in the establishment of a professional army, it is necessary to clearly define how the military

personnel employed on a contract basis will be selected, trained, and professionally improved (Sarcinschi 2005, 36) highlighting the importance of developing a recruitment and professional training methodology for this category of soldiers.

The professionalization of the National Army – between intentions and reality

We will mention that during this period the professionalization of the Romanian Army represented an objective necessity and was successfully achieved. At the same time, at the level of the political leadership of the Republic of Moldova, a clear option was not formulated regarding the type of army that we were going to build. In the absence of a state policy based on feasible calculations and foresight regarding the military security of the state in general and how to complement the armed forces and organize the military service in particular, almost every government and defense minister came up with their own approach on the model of completing and organizing the military service. Thus, in recent years, the aspects of completing the army have seen an oscillation from one form to another.

This includes the intention to professionalize the Moldovan army by adopting Government Decision No. 601 of 27.06.2018 regarding the approval of the Program "Professional Army 2018-2021" (Government of the Republic of Moldova 2018). The purpose of the program was to identify the areas of development of the National Army and to order them according to the allocated resources. The main effort was focused on two aspects of major importance for the army.

The first aspect highlighted the importance and role of the military (individual) within the national defense system. The focus of attention was on the quality of the human dimension, implicitly the selection, equipping, training, and provision of social facilities, which becomes imperative in the context of the diminishing attractiveness of military service and the increased ebb of personnel. *The second aspect* of the Program concerned the structural reform of the National Army. The need for this reform was imposed by the evolution of the environment, security, and defense systems at the international level.

According to the vision outlined in the Program, *"professionalization"* implies deep transformations at the level of organization, equipping with modern equipment, armaments and combat techniques, training, and the activity of the military body. Complementarily, professionalization was supposed to intensify the communication relations between the army and society (the political class, civil society, state institutions, etc.), increasing its involvement and presence in various compartments of social life. The implementation of the Program was supposed to be carried out in stages, during the years 2018-2021, in accordance with the budget allocations, the additional resources available, and those provided by external partners. Among the

areas of implementation were:

- *The transition from military term service to service by contract by the year 2021*.
- *Perfecting the process of combat training and mobilization.* The efforts were to be oriented towards the standardization of the training process and the gradual provision of military units with modern weapons and equipment. Also here, efforts were to be undertaken to replace obsolete military equipment, including through external assistance. Additionally, it was expected to initiate the process of revising the army mobilization system.
- *Revision of the salary system for the military and improvement of the social package.* In this chapter, the possibility of moving to unitary pay for all force structures within the national security and defense system was to be identified. Additionally, it was planned to extend the benefits of the social package for the military of the National Army.
- *The efficiency and development of the logistic system*. In the initial phase of this direction, the organizational structure and the command-and-control component of the system were revised. At the same time, a feasibility study was carried out regarding the reconsideration of the method of insurance with military uniforms of the military by contract, as well as insurance with food ration.
- *Modernization of the military and social infrastructure.* This measure was aimed at the renovation and gradual construction of some infrastructure objects (barracks, canteens, sports and housing complexes, etc.). Also here, the continuous realization of the Public-Private Partnership projects, which involved the provision of service housing for the contract military, was foreseen.
- *The review of the security service and guarding the military objectives of the National Army.* This measure has an innovative character at the national level, based on the practice of the armies of the Western states, and aims to make the military service more efficient by reducing the number of personnel involved in guarding activities and ensuring daily life.
- *The development of cooperation relations with external partners.* Efforts were focused on streamlining cooperation within the Defense Capacity Building Initiative (DCBI). At the same time, it was foreseen to establish the positions of advisers (military attachés) within the embassies of the Republic of Moldova in the partner states (USA, Romania, and Ukraine).

The program, however, did not achieve its proposed objectives. We will identify several causes: considering the importance of the defense sector in ensuring the security and sustainable development of the state, the Program was not the expression of the consensus decision of the political class through its approval by the Parliament, being rather a decision of a party, which did not have continuity; the issue of financing the Program was not a priority of the political leadership

and the Government of the Republic of Moldova; the society was not sufficiently informed and prepared for the transition to the professional army. Thus, the delays in the implementation of the Program made the Republic of Moldova repeat the same experience that Ukraine, Georgia (Global Legal Monitor 2023), Latvia (Capital 2024), Lithuania (Capital 2015), but also other states went through. However, the Program was a good platform that the Ministry of Defense used effectively in rethinking the importance of the system of complementing the army by organizing the military service and its multilateral assurance.

Those issues exposed regarding the policies of complementing the armed forces and organizing the military service allow us to identify new concepts of organization and operation, which correspond to the current security architecture and the new challenges to the international and national security environment. The war in Ukraine demonstrated that the mixed complementation system of the armed forces, where alongside the military service by contract compulsory military service is also organized, remains a necessity that ensures the functionality of the armed forces in the context of the new security conditions.

The system of complementing the armed forces through the lens of the war in Ukraine

We will note that before the start of the war in Ukraine, on February 1, 2022, the President of Ukraine signed Decree no. 36/2022 "On the priority measures for strengthening the state's defense capacity, increasing the attractiveness of military service in the Armed Forces of Ukraine and the gradual transition to the principles of a professional army." We consider that an additional argument for this decision was the previous unsuccessful attempt of Ukraine to switch starting from January 1, 2014, to the professional army (President of Ukraine 2013).

One of the elements foreseen for the year 2022 was the transition to a system of intensive military training and the cancellation of conscription for military service. From January 1, 2024, it was proposed to introduce short-term intensive training for citizens, 3-4 months, gradually increasing the number of those involved and maintaining their skills through regular training (President of Ukraine 2022). This approach preserved the system of training citizens for the defense of the homeland and the formation of a trained reserve with a necessary number of specialists. We will mention that this fact was not taken into consideration by the Moldovan authorities with the intention of professionalizing the National Army in the "Professional Army 2018-2021" Program.

The aggression of the Russian Federation on February 24, 2022, prevented the implementation of the mentioned decree; thus, Ukraine entered the war having mixed military service to complement the army. However, the term-military is not involved in combat actions. In the context of the declaration of general mobilization

in Ukraine, incorporation during the war was not carried out. All vacancies in the Armed Forces and other military formations are filled by the mobilized reservists (Interfax 2022). Ukraine has learned its lesson regarding the importance of the system of complementing the armed forces. In the new mobilization law, basic military service is introduced instead of military service. It is to be organized for citizens aged between 18 and 25 years. They will be able to independently choose the period of service until they reach the age of 24. Basic military service in wartime will last up to 3 months, of which at least 1 month will be devoted to basic training and up to 2 months will be for professional training, and in peacetime the duration will be up to 5 months, respectively 3 months will last for basic training and 2 months for professional training (Euronews 2024). In this context, previously organized military term service was the main source that allowed the formation of the required number of trained reservists of the Ukrainian army, and the introduction of basic military service will ensure the possibility of training reservists for the future.

We will mention that the characteristics and trends of evolution of the national, regional, and global security environment since the end of the 20th century, which influenced the transition to a professional army in Eastern European countries, changed radically with the invasion of the Russian Federation in Ukraine. Both states resorted to the mobilization of reservists, who initially ensured the transfer of military units to the states at war, and later to restore and supplement the losses suffered as a result of combat actions, the formation of new combat units to ensure the rotation of front-line units. The availability of human resources trained and prepared for mobilization is one of the key indicators of the state's military potential (Diplomatic Dictionary 2024). After two years of war, the Armed Forces of Ukraine urgently needed new reservists called up, and for this purpose, amendments were adapted to the mobilization law which expanded the categories of citizens that could be mobilized, including by lowering the age for mobilization from 27 years to 25 years (Parliament of Ukraine 2024). The new provisions of the law will ensure the possibility of rotating approximately 300,000 soldiers on the battlefield out of the nearly 500,000 people who could be mobilized (Forbes 2024).

The importance of the reserve, prepared in time, in the war in Ukraine, led to the reevaluation of the role and place of compulsory military service which is the main form of military training of the citizens and, respectively, of the formation of the reserve for the mobilization of the army. After Russia annexed Crimea in 2014 and the military invasion of Ukraine on February 24, 2022, several states revised their system of complementing the armed forces, advocating a mixed system. The Lithuanian government enacted a law that all men between the ages of 18 and 25 would be conscripted for compulsory military service in the army. Likewise, in Latvia all men between the ages of 18 and 27 will have to undergo 11 months of military training, starting in 2024. In Sweden, compulsory military service was reintroduced in 2018, as not enough were found volunteers for military service (DW 2023). Denmark extended the term of compulsory military service from 4 to 11

months and intends to introduce, from 2026, compulsory conscription for women as well, after it was implemented in Norway and Sweden (Defense Romania 2024).

The actuality of the mixed system of complementation for the National Army

The war in Ukraine required a comprehensive analysis of the security sector in the Republic of Moldova. The national security strategy, recently adopted, defines the threats, risks, and vulnerabilities that affect or may affect national security. Among the vulnerabilities in the field of military security and national defense that are or can be exploited by internal and external malignant actors, the strategy highlights the low support for the country's defense among the population (Parliament of the Republic of Moldova 2023).

In this context, we will note that the institution of compulsory military service, in addition to the formation of the reserve prepared for mobilization, also acts as an educational factor, in a civic-national spirit, on those who have been active within its structures, thus functioning as an instrument socialization and strengthening of support for the country's defense among the population. Thus, both the conducted studies and the data provided by the opinion poll entitled "L'opinion publique et l'Europe de la Defense" (Duțu and Sarcinschi 2004, 8-10) state that the military institution has the purpose, among other things, to:

- *prepare young people for life, accustoming them to discipline and order*: performing military service, they learn to conform freely, voluntarily, and consciously to a set of norms and rules specific to military activity and life, but with positive consequences for their future conduct;
- *transmit to young people specific traditional values:* the instructive-educational activities that young people take part in during military service help them assimilate and internalize traditional values – honor, pride in being a citizen of their state, justice, discipline, loyalty, responsibility;
- *contribute to the socialization and maturation of young people*: the socialization process that young people start in the family continues in school (primary socialization), then it is continued in the army, where they learn, internalize, and integrate essential socio-cultural elements into the personality structure, based on which they can act coherently within society;
- *help to integrate young people into society*: during military service, young people assimilate values (specific to the military environment, but also common to any democratic society), norms, and rules, that will shape their behavior from a psychosocial point of view (consensus, conformity, solidarity, effectiveness, and traditions) and professionally. These accumulations allow an easier integration into the civilian social environment when they are transferred to the reserve.

The exercise of these social functions acts directly on the qualitative content of the army's mission to defend the sovereignty, territorial integrity, and independence of

the state. If the young soldiers are trained and educated according to the demands of social functions, they will be able to perform all the tasks received in the coordination of the defense of the country. The military service approached as a life experience, continues to have an important contribution to the formation of the social perception of the population on the role, utility, and legitimacy of the army in society.

Thus, the mixed system of complementing the armed forces represents the model in which the armed forces are supplemented by both professional military personnel and conscripts who have been recruited through compulsory military service. In this vein, we emphasize that for the Republic of Moldova the preservation of compulsory military service, through its educational effects, is an essential factor in reducing vulnerability in the field of security and national defense determined by the low support for the country's defense among the population, reflected in the National Security Strategy.

Currently, the National Army is going through an extensive transformation process, a situation that implies the transition from a certain perspective from compulsory (mixed) military service in all military units, to the system of completing some military units only with contract soldiers. In this process, according to the regulations established at the national level, the role, place, and importance of the military profession expands, the emphasis being placed on the number of soldiers and sergeants employed on a contract basis. However, the National Army is currently facing the substantial problem of the reduced capacity to maintain/complete the workforce of sergeants and soldiers employed by contract.

We will highlight the main problems of complementing the number of sergeants and soldiers engaged in military service by contract: the alternative of better-paid jobs; diminishing the social status of the defender of the country; lack of motivation of young people for military service; disinformation attacks and manipulation of public opinion on the military establishment; the material and technical resources needed to carry out daily activities are below the corresponding quality level and others.

The Russian Federation's aggression against Ukraine has generated a very strong change in the view of Moldovan citizens towards the National Army and defense issues. Traditionally, the military enjoyed positive attitudes from the general public. If in previous years trust in the army, exposed in the Barometer of Public Opinion, had constantly varied between 40% and 50%, then in the survey of 2022, this indicator has dropped to 27%. Another important aspect can be found in the answers to the question about citizens' willingness to join the armed forces in the event of military aggression against the Republic of Moldova. The willingness of men to enlist in the army in the event of aggression is 41%, while among citizens with military training, the percentage of those who declare themselves willing to participate in the defense of the country is 48.5%. Thus, in the event of aggression, Moldovans will not flee the country but will defend themselves, ensuring the capabilities of mobilizing the

armed forces. This indicator, however, does not come close to similar provisions in Ukraine, Poland, Finland, and the Baltic States, where there is patriotic education and a cutting-edge state information policy regarding the dangers emanating from Russia (Albu et. all 2022, 17).

We believe that the initiation and implementation of a campaign to promote the positive image of military service in the National Army is of major importance. There is a need for a system/program of military-patriotic education of the young generation and the formation and promotion of security and defense culture, as well as the culture of memory in society. Patriotic education should be seen as a systematic activity of the state authorities, the army, the school, civil society, and the family for the formation in citizens of high patriotic consciousness, feelings of loyalty to the homeland, readiness to fulfill civic duty and constitutional duties to protect the interests of the homeland. We will note that Government Decision No. 1263 of 24.12.1998 regarding the approval of the concept of military-patriotic education of the youth (Government of the Republic of Moldova 1998) was repealed in 2012, without an adequate replacement for the new security requirements.

At the same time, the actions to increase the attractiveness, the quality of the military service, and the guarantees of social protection of the military by ensuring an appropriate social package for the employees are opportune. In this context, in 2023, the Government of the Republic of Moldova approved an increase in the salary of the term-military from 150 to 500 lei per month, and the right to a food ration for the contract-based military was introduced once a day (at lunch), per diem of the National Army soldiers deployed in a peace support mission in the Security Zone was increased, the salary principles for the corps of sergeants and soldiers were adjusted in accordance with international practices.

At the same time, the Ministry of Defense started some programs for the development and equipping of the National Army with modern weapons. This became possible thanks to the support of external partners, as well as the support of the defense sector by the political leadership in the current security conditions, which allowed the increase of the budget intended for defense, which for the year 2024 constitutes - 0.55% of GDP (Ministry of Defense of the Republic of Moldova 2023). The social protection actions of the military, on the one hand, and the development and equipment of the army, on the other hand, represent a factor of strengthening citizens' confidence in the army's ability to carry out its constitutional mission and respectively increase support for the defense of the country among the population.

Keeping the mixed system of complementing the armed forces offers the possibility of preparing the reserve of the armed forces at the expense of the soldiers who are released after completing the military service. The armed forces of Romania faced the problem of the insufficiency of the prepared reserve, after the abolition of compulsory military service in 2007. In order to return to normality, in 2015, the

Law on the Status of Voluntary Reservists was adopted, which provides for an initial training period for citizens who have not completed active military service for the accumulation of basic military knowledge, after which the annual call for training takes place for 15 calendar days (Parliament of Romania 2015). At the same time, considering the lessons of the war in Ukraine, the Ministry of National Defense has prepared for 2024 a draft law on voluntary military training for women and men that will regulate the possibility of those who wish to have military training, having an age between 18 and 35 years, to undergo training for a period of up to four months, with certain incentives for this (Free Europe 2024).

We believe that this example should be taken into consideration by the Ministry of Defense of the Republic of Moldova in the context of the opportunity to continue to keep the mixed system of complementing the army. Moreover, national legislation does not limit the proportion, a fact that allows for gradual professionalization. The need to improve the legislation in force regarding the training of the military reserve also remains current.

Conclusions

Taking into account the changes in the international and regional security environment, after the National Security Strategy was adopted, in the Republic of Moldova there is a complex process of designing the strategic framework for defense planning, which includes the elaboration of a set of strategic documents such as the National Strategy of Defense and Military Strategy.

We will note that at this stage of the practical implementation of the political decisions, it is recommended that the Ministry of Defense ensure the planning of the construction and development of the National Army not only through the prism of streamlining the structure, organization, management, training, efficient use, equipment, deployment but also by keeping the mixed system of complementing the army. In the National Defense Strategy, it is recommended to mention that the mixed system of complementing the National Army is the main method by which the Republic of Moldova can prepare its citizens and its own reserve of armed forces for the defense of its homeland. In perspective, the professionalization of the army can be examined through the lens of the existence of updated external/internal conditions, on a broad platform of political support and multilateral assurance of the process, the launch of a system for organizing the military training of young people/citizens to create reserves, as well as the establishment of voluntary military service in reserve.

At the same time, defense is a joint effort that involves both military and civilian institutions, and, last but not least, the responsibility of the citizen. There is a need for a strong security culture, promoted in a sustained manner among the population and political decision-makers, for the formation and consolidation of knowledge

and information regarding national security values and needs, the knowledge of which attracts the development and promotion of behaviors necessary for the defense of the state in the face of internal or external dangers. Thus, the meaning of the Constitution (art. 57) will be understood correctly (Parliament of the Republic of Moldova 1994), by which it is mentioned that the defense of the homeland is a right and a sacred duty of every citizen which is primarily achieved through military service in the armed forces.

References

Albu, N., E. Mîrzac, M. Potoroacă, V. Pașa, A. Grămada, V. Juc and V. Catarji. 2022. Public receptions on the security and defense system of the Republic of Moldova, Chisinau.

Capital. 2015. "Introducing Europe: Lithuania Temporarily Returns to Conscription". https://www.capital.ro/se-introduce-in-europa-lituania-revine-temporar-serviciul-militar-obligatoriu.html

___. 2024. "They will necessarily go to the army". https://www.capital.ro/vor-merge-obligatoriu-in-armata-decizie-pentru-barbatii-intre-18-si-27-de-ani-ordin-oficial.html.

Coropcean, I., V. Juc. and C. Manolache. 2019. Military service in the Republic of Moldova: political-legal approach. Monograph. Chisinau, "Andrei Lupan Scientific Library (Institute)".

Defense Romania. 2024. "The Nordics Set the Tone: Denmark Introduces Compulsory Military Service for Women, Too". https://www.defenseromania.ro/nordul-europei-da-tonul-danemarca-introduce-serviciul-militar-obligatoriu-si-pentru-femei-stagiul-militar-obligatoriu-creste-la-11-luni_627380.html.

Diplomatic dictionary. 2024. "The State's Military Potential." [The state's military potential]. http://diplomaticdictionary.com/dictionary/.

Duțu, P., C. Moștoflei and A. Sarcinschi. 2003. The professionalization of the Romanian Army in the context of integration into NATO. Bucharest: Center for Strategic Defense and Security Studies.

Duțu, P. and A. Sarcinschi. 2004. Social, psychosocial and legal determinations of the Romanian Army missions. Bucharest: Publishing House of the "Carol I" National Defence University.

Duțu, P. 2008. Phenomena and defining processes for the evolution of the National Army. Bucharest: Publishing House of the "Carol I" National Defence University.

DW. 2023. "Europe: Is conscription back?". https://amp.dw.com/ro/ne-%C3%AToarcem-la-serviciul-militar-obligatoriu/a-65884583.

Free Europe. 2024. Project: voluntary military internship for women and men between 18 and 35 years old, available at https://romania.europalibera.org/a/ministerul-apararii-legislatie-comisii-parlament-intalnire /32807942.html.

Euronews. 2024. "Ukraine: Parliament Adopts Law on Mobilization". https://ru.euronews.com/2024/04/11/ukraine-conscripts.

Forbes. 2024. "В поиске 500.000 новобранцев." [Looking for 500,000 recruits]. https://forbes.ua/ru/war-in-ukraine/u-poshukakh-500-000-novikh-rekrutiv-ft-otsinyue-shansi-ukraini-mobilizuvati-piv-milyona-cholovikiv-dlya-viyni-proti-tomatoes-13032024-19830.

Global Legal Monitor. 2023. "Georgia: New Defense Code Establishes System of Mandatory Military Service". https://www.loc.gov/item/global-legal-monitor/2023-12-28/georgia-new-defense-code-establishes-system-of-mandatory-military-service/.

The Government of the Republic of Moldova. 1998. "Government's decision regarding the approval of the conception the military-patriotic education of the youth". https://www.legis.md/cautare/getResults?doc_id=77261&lang=ro.

___. 2018. "Government Decision no. 601 of 27.06.2018 regarding the approval of the "Professional Army 2018-2021". https://www.legis.md/cautare/getResults?doc_id=108729&lang=ro.

Interfax. 2022. "The spring call for emergency service in 2022 will not be held in Ukraine - General Staff of the Armed Forces of Ukraine." [The spring call for conscription in 2022 will not be held in Ukraine - General Staff of the Armed Forces of Ukraine]. https://ua.interfax.com.ua/news/general/822114.html.

Ministry of Defense of the Republic of Moldova. 2023. "The Minister of Defense presented the achievements of the institution in the plenary session of the Parliament". https://www.army.md/index.php/spiritual/inf/12319116423?lng=2&action=show&cat=122&obj=8572.

The Parliament of the Republic of Moldova. 1994. "The Constitution of the Republic of Moldova". https://www.legis.md/cautare/getResults?doc_id= 128016&l ang = ro.

___. 2023. "Parliament decision no. 391/2023 on the approval of the National Security Strategy of the Republic of Moldova". https://www.legis.md/cautare/getResults?doc_id=141253&lang=ro.

The Romanian Parliament. 2015. "Law no. 270/2015 of November 10, 2015 regarding the Statute of voluntary reservists". https://www.mapn.ro/rezervisti_voluntari/documente/270_din_2015.pdf.

Parliament of Ukraine. 2024. "Закон України Про внееся змені до часть бесплатных октів України гаје одинідный очень оченье онлайні обліку, mobilizacija та віннуго облику." [The Law of Ukraine On amendments to some legislative acts of Ukraine regarding certain issues of military service, mobilization, and military registration]. https://zakon.rada.gov.ua/laws/show/3633-IX#Text.

President of Ukraine. 2013. "Decree of the President of Ukraine №562/2013 Про строки проведення чергових призовів, чергові призови громадян України на строкову військову службу до внутрішніх військ Міністерства внутрішніх справ України та звільнення в запас військовослужбовців у 2014 роцію." [Decree of the President of Ukraine No. 562/2013 On the terms of regular conscriptions, regular conscriptions of citizens of Ukraine for temporary military service in the internal troops of the Ministry of Internal Affairs of Ukraine and the release of servicemen into the reserve in 2014]. https://www.president.gov.ua/documents/5622013-15707.

__. 2022. "Decree of the President of Ukraine №36/2022 Про першочергові заходи щодо зміцнення обороноздатності держави, підвищення привабливості військової служби у Збройних Силах України та поступового переходу до засад професійної армії." [Decree of the President of Ukraine No. 36/2022 On priority measures to strengthen the state's defense capabilities, increase the attractiveness of military service in the Armed Forces of Ukraine, and gradual transition to the basics of a professional army]. https://www.president.gov.ua/documents/362022-41285.

Sarcinschi, A. 2005. The impact of the professionalization of the Romanian Army on its relations with the society in which it exists. Bucharest: Publishing House of the "Carol I" National Defense University.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Counterintelligence Risks in Crew Management and Recruitment: The Role of Profiling and Screening in Shipping Companies

Anastasios–Nikolaos KANELLOPOULOS, Ph.D. Candidate*

*Athens University of Economics and Business
e-mail: ankanell@aueb.gr

Abstract

This paper examines the critical role of profiling screening in countering security threats within the maritime industry, focusing on crew management and recruitment processes. In light of the industry's susceptibility to espionage, terrorism, and sabotage, effective counterintelligence measures are imperative. By scrutinizing the vulnerabilities and best practices associated with profiling screening, shipping companies can fortify their security defenses, mitigate insider threats, and ensure the safety of their assets and personnel.

Keywords:
Counterintelligence; shipping companies; Shipping Crew Management; Profiling; Screening.

Article info
Received: 8 April 2024; Revised: 7 May 2024; Accepted: 3 June 2024; Available online: 5 July 2024

Citation: Kanellopoulos, A.N. 2024. "Counterintelligence Risks in Crew Management and Recruitment: The Role of Profiling and Screening in Shipping Companies. *Bulletin of "Carol I" National Defence University*, 13(2): 44-59. https://doi.org/10.53477/2284-9378-24-19

This research embarks on a comprehensive literature review to explore the effectiveness and suitability of Counterintelligence (CI) profiling and screening processes within the realm of shipping companies. The primary objective of this study is to delve into various methodologies and best practices, aiming to assess their potential applicability within the unique operational landscape of shipping companies. CI processes serve as crucial components of security frameworks, especially in industries where there is a substantial risk of compromising sensitive information and assets. This significance is particularly pronounced in the maritime sector, characterized by its dynamic and often hazardous operating environment. Given the nature of maritime operations, which involve the transportation of valuable goods across international waters, the implementation of robust CI measures becomes imperative to safeguard the integrity and security of shipping operations. Consequently, this research seeks to scrutinize existing literature to identify key strategies, challenges, and best practices associated with CI profiling and screening, focusing specifically on their relevance and effectiveness within the maritime domain. By examining scholarly works and practical case studies, this study aims to offer valuable insights and recommendations to inform decision-making processes within shipping companies regarding the adoption and implementation of CI profiling and screening procedures. In doing so, this research endeavors to contribute to the enhancement of security protocols within the maritime industry, thereby ensuring the protection of vital assets and the mitigation of potential security risks.

General Crew Management and Recruitment Risks

Crew management within the realm of shipping companies entails the holistic supervision of seafarers across the entirety of their employment trajectory, spanning from initial recruitment to eventual retirement. This multifaceted endeavor involves the comprehensive administration of various facets of seafarers' employment, including but not limited to recruitment procedures, training initiatives, scheduling arrangements, welfare provisions, performance evaluations, and career advancement opportunities (Caesar and Fei 2018). Central to the mandate of shipping companies is the assurance that seafarers possess requisite qualifications, certifications, and competencies essential for the safe and proficient execution of their duties aboard vessels (Grammenos 2010). Furthermore, shipping companies shoulder the responsibility of addressing the distinctive exigencies and adversities encountered by seafarers, such as protracted periods of separation from familial environments, isolation, and exposure to potentially perilous working conditions (Auster and Choo 1994; Grammenos 2010; Giannakopoulou, Thalassinos and Stamatopoulos 2016).

Recruitment Risks: Recruitment risks within the maritime sector present formidable obstacles for shipping companies in their quest to identify and recruit qualified seafaring personnel. Among these challenges, one of the most prominent is the restricted availability of suitably qualified candidates for specific roles, stemming from

a confluence of factors including demographic shifts, skill scarcities, and evolving job specifications (Caesar and Fei 2018). Furthermore, the endeavor to entice proficient seafarers is compounded by heightened competition from alternative industries that offer enticing incentives and promising career pathways. Complicating matters further, inadequate recruitment channels exacerbate the situation, as shipping enterprises may encounter difficulties in effectively reaching potential candidates. Additionally, the constrained access to diverse talent pools inhibits endeavors to assemble inclusive and adaptable crews capable of fulfilling the multifaceted demands of the maritime sector. Another significant risk lies in the accuracy and completeness of the information furnished by candidates during the sourcing phase. Erroneous or incomplete data may lead to incongruities between job prerequisites and candidate proficiencies, ultimately impinging upon the caliber of hires and the overarching efficacy of crew management initiatives. Mitigating these recruitment risks necessitates the implementation of proactive strategies by shipping companies, including the diversification of recruitment channels, the augmentation of outreach endeavors, the refinement of candidate screening mechanisms, and the allocation of resources toward talent development programs. These measures are indispensable for facilitating the effective attraction, retention, and integration of proficient seafaring personnel within shipping enterprises (Barnea and Meshulach 2020).

Training and Familiarization Risks: Training and familiarization risks represent pivotal concerns within the maritime industry, exerting profound implications on the safety, efficacy, and proficiency of crew operations conducted aboard vessels. Among these risks, a noteworthy challenge arises from the provision of inadequate training and preparation for newly recruited crew members, a deficiency often attributed to constraints such as time limitations, resource constraints, or deficiencies in training curricula. Such inadequacies may render recruits ill-prepared to navigate the demands inherent to their roles, thereby compromising their safety and impeding the collective performance of the crew. Additionally, the dearth of familiarity with vessel-specific procedures and equipment poses further obstacles, potentially impeding crew members' adeptness in maneuvering onboard systems and adhering to established protocols (Estay 2020). Furthermore, deficient knowledge regarding safety protocols and emergency response procedures exacerbates these risks, potentially undermining the crew's capacity to effectively address emergent or perilous scenarios. Another salient concern pertains to the crew's challenges in assimilating novel technologies or systems onboard, which may encumber operational efficiency and productivity. Finally, deficient communication and coordination amongst crew members pose consequential risks, engendering instances of miscommunication, errors, and operational inefficiencies. To mitigate these training and familiarization risks, shipping companies must accord precedence to comprehensive training initiatives, allocate resources towards advanced simulation and training infrastructures, cultivate a culture of safety and perpetual learning, and foster effective communication and collaboration amongst crew members (Georgiadou, Mouzakitis and Askounis 2021). Through proactive

risk management endeavors, shipping companies can enhance crew preparedness, alleviate operational disruptions, and uphold unwavering standards of safety and operational excellence aboard their vessels (Cho and Lee 2016).

Retention Targets Risks: Retention targets risks in the maritime industry present notable obstacles for shipping companies, impeding their capacity to retain competent and seasoned seafarers. A primary concern lies in the challenge of meeting retention objectives due to substandard working conditions experienced onboard vessels. Factors such as prolonged periods away from home, demanding work environments, and limited access to amenities contribute to seafarer discontentment and heightened turnover rates. Furthermore, the dearth of opportunities for career advancement and progression pathways poses a substantial risk, compelling seafarers to seek employment elsewhere in pursuit of professional growth and personal development. Inadequate acknowledgment and rewards for high-performing seafarers exacerbate the retention predicament, fostering sentiments of undervaluation and unappreciation among crew members. Moreover, deficient feedback mechanisms and performance evaluation systems impede the company's ability to preemptively identify and rectify issues, engendering diminished morale and motivation within the crew. A notable risk factor pertains to the imbalance between work and personal life, with prolonged durations at sea exacting tolls on seafarers' mental and physical well-being, precipitating burnout and dwindling job satisfaction levels. To mitigate retention target risks, shipping companies must accord primacy to seafarer welfare, furnish competitive remuneration and benefits schemes, offer avenues for professional advancement and skill enrichment, institute robust performance assessment frameworks, and advocate for a harmonious work-life equilibrium. Through these concerted efforts, companies can ameliorate seafarer retention rates, bolster crew morale and efficiency, and fortify the enduring prosperity and viability of their endeavors (Cho and Lee 2016).

Counterintelligence Risks

The intersection of CI risks with the overarching complexities inherent in crew management and recruitment exacerbates the intricacies of security challenges encountered by shipping companies (Grammenos 2010; Cho and Lee 2016). This amalgamation encompasses a spectrum of threats stemming from state-sponsored espionage, activities of non-state actors, and the potential of insider threats, thereby presenting formidable hurdles to the organization's security infrastructure (Greene 1966; Wettering 2000; Johnson 2010; Alcaide and Llave 2020). Effectively addressing these risks necessitates a holistic comprehension of the landscape coupled with strategic mitigation measures, which take into account factors such as the constrained availability of suitable candidates, deficiencies in training protocols, obstacles in retention initiatives, and vulnerabilities within recruitment channels (Johnson 2010; Duvenage and Solms 2014; Caesar and Fei 2018; Kanellopoulos 2023).

By acknowledging the interconnected nature of these risks, shipping companies can bolster their defensive mechanisms, thereby safeguarding the integrity of their operations and assets (Catrantzos 2023).

State and Non-State Actor Threats

State-sponsored espionage poses a significant and tangible threat to the maritime industry, as evidenced by numerous real-life incidents. For example, the "Cloud Hopper" operation, attributed to China's Ministry of State Security, targeted managed service providers (MSPs) to access the networks of their clients, including shipping companies. This extensive cyber espionage campaign aimed to steal sensitive data, intellectual property, and trade secrets from various industries, including maritime. By compromising MSPs' networks, the Chinese government gained access to a vast array of companies, allowing them to gather valuable intelligence on maritime trade routes, cargo shipments, and port operations (Cybersecurity and Infrastructure Security Agency 2017).

In addition to state-sponsored espionage, non-state actors also pose a significant threat to the maritime industry, exploiting vulnerabilities within crew management and recruitment processes for illicit activities (Caesar and Fei 2018). For instance, criminal syndicates engage in drug smuggling operations, targeting shipping vessels by coercing or bribing crew members to facilitate the transportation of illegal narcotics across international borders. An example of this is the discovery of large quantities of drugs hidden aboard a container ship, revealing a sophisticated smuggling operation orchestrated by a criminal organization. Such incidents underscore the vulnerabilities within crew management systems and highlight the need for enhanced security measures to prevent criminal exploitation of maritime personnel (Europol 2023).

Moreover, terrorist organizations have shown their intent to exploit weaknesses in the maritime sector for strategic and ideological purposes. For example, the Somali-based terrorist group Al-Shabaab has targeted commercial Shipping vessels in piracy-prone regions like the Gulf of Aden and the Indian Ocean. The hijacking of MV Maersk Alabama by Somali pirates in 2009 highlighted the security risks faced by shipping companies operating in these areas (Kantharia 2019). Although piracy incidents have decreased in recent years due to improved maritime security measures, the threat of terrorist attacks or hijackings persists, necessitating ongoing vigilance and collaboration among industry stakeholders to effectively mitigate risks (Cho and Lee 2016).

Insider Threats

Malicious insiders and negligent insiders pose significant risks to shipping companies, often leading to substantial financial losses, reputational harm, and compromised security (BIMCO, et al. 2021; Gelles 2021; Kanellopoulos 2024). Real-life incidents provide concrete evidence of the severity of these threats and underscore the

necessity for robust countermeasures (Johnson 2010; Clark and Mitchell 2019). In 2016, a disgruntled IT contractor at Maersk Line, one of the world's largest shipping companies, orchestrated a devastating cyberattack that disrupted global operations and incurred substantial financial losses. The contractor, employed to manage Maersk's shipping systems, utilized his privileged access to implant the NotPetya malware into the company's network. This malicious act quickly spread across Maersk's infrastructure, bringing down essential systems worldwide. As a result of this cyberattack, Maersk was forced to shut down key operations, including container terminals, booking systems, and email communications, severely impacting global supply chains. The financial toll was immense, with Maersk estimating losses of over $300 million due to halted operations and recovery costs (Leovy 2017). The examples vividly illustrate how malicious insiders, motivated by personal grievances or financial incentives, can exploit their insider status to inflict significant harm on shipping companies (Catrantzos 2023).

Furthermore, negligent insiders, while not acting with malicious intent, can still pose serious security risks to organizations through their careless actions or failure to adhere to security protocols (Catrantzos 2023). In 2017, a significant data breach occurred at FedEx due to the negligent actions of an employee, highlighting the serious security risks posed by careless insiders. An employee at FedEx Office, the company's retail arm, inadvertently left unsecured customer information in a publicly accessible location. This information included scanned passports, driver's licenses, and other sensitive documents that customers had submitted for printing or copying services. The exposed documents were discovered by a customer who notified the media and raised concerns about the potential for identity theft and fraud. The incident attracted widespread attention and scrutiny, leading to investigations by regulatory authorities and damaging FedEx's reputation for data security. Upon investigation, it was revealed that the employee had failed to follow proper procedures for handling sensitive customer data, including securely storing and disposing of documents (Shaikh 2018). This oversight resulted in a breach of customer confidentiality and exposed individuals to significant privacy risks. This instance demonstrates how negligent insiders, due to their lack of awareness or disregard for security practices, can inadvertently create vulnerabilities that malicious actors exploit for nefarious purposes (BIMCO, et al. 2021; Gelles 2021; Catrantzos 2023; Kanellopoulos 2024).

Methods of Exploitation

The issue of falsified credentials poses a significant challenge in crew management and recruitment within shipping companies, where individuals may resort to deceptive practices to enhance their qualifications or experiences to secure employment (Clark and Mitchell 2019). This deception spans a spectrum from minor embellishments on resumes to outright fabrications of certifications or educational backgrounds. For example, an applicant might falsely claim to possess specialized maritime licenses or certifications crucial for certain roles, thereby misleading recruiters and potentially

jeopardizing the safety and security of operations (Estay 2020). In extreme cases, individuals with malicious intentions may resort to identity theft or the production of counterfeit documents to substantiate their false claims (Clark and Mitchell 2019).

Similarly, undisclosed affiliations present a notable risk factor as applicants may intentionally withhold information about their connections to external entities that could pose a threat to the organization (Cho and Lee 2016). For instance, an individual with affiliations to a foreign government, extremist group, or organized crime syndicate might conceal these associations during the recruitment process to avoid scrutiny or suspicion (ENISA 2024). However, such undisclosed affiliations could leave the company vulnerable to exploitation, as these individuals may be susceptible to coercion, blackmail, or recruitment by external actors seeking to exploit their insider status for espionage or sabotage purposes (Greene 1966; Gelles 2021; Catrantzos 2023).

Furthermore, social engineering tactics represent a sophisticated and covert threat to the security defenses of shipping companies. By leveraging human psychology and interpersonal relationships, threat actors can manipulate employees or recruiters into disclosing sensitive information, granting unauthorized access to systems, or unwittingly executing malicious actions (Clark and Mitchell 2019). For instance, attackers might impersonate trusted colleagues or authority figures to deceive employees into revealing login credentials, providing access to confidential databases, or initiating unauthorized transactions. Additionally, phishing attacks, characterized by deceptive emails or messages aimed at tricking recipients into divulging sensitive information or clicking on malicious links, remain a pervasive threat in the maritime industry (Clark and Mitchell 2019). These social engineering tactics underscore the imperative for robust cybersecurity measures, comprehensive employee training programs, and vigilant monitoring to detect and thwart potential threats before they manifest into actual harm (Duvenage, Jaquire and Solms 2018; Alcaide and Llave 2020; Ball 2021; Akpan, et al. 2022).

Counterintelligence Profiling and Screening in shipping companies

CI profiling and screening procedures within shipping companies represent a critical endeavor aimed at identifying and mitigating potential security risks (Cho and Lee 2016). This comprehensive approach involves a series of meticulously designed steps intended to scrutinize individuals' backgrounds, behaviors, and affiliations to enhance security measures effectively. The subsequent discussion will outline the essential steps involved in this profiling screening process (Prunckun 2019).

Information Gathering: The foundational stage of the profiling screening process entails comprehensive information gathering, which is fundamental for shipping

companies to develop a comprehensive understanding of potential candidates. This phase involves a systematic and exhaustive examination of various facets of the applicants' backgrounds and credentials. Personal history scrutiny encompasses a detailed review of past addresses, familial connections, and significant life events to glean insights into the individual's character and integrity (Clark and Mitchell 2019). Verification of educational background entails thorough validation of academic credentials, degrees earned, and institutions attended to ensure the authenticity of claimed qualifications. Scrutiny of employment records involves a meticulous assessment of past work experiences, job roles, and performance evaluations to gauge the candidates' professional competence and suitability for maritime positions. Furthermore, evaluating references provides valuable perspectives on the candidates' character, work ethic, and interpersonal capabilities, offering valuable insights into their past behavior and reliability. Through rigorous documentation and verification protocols, shipping companies aim to construct a comprehensive profile of each candidate, facilitating informed evaluations of their potential contributions to the organization and their alignment with the company's values and objectives (Grammenos 2010).

Background Checks: Background checks constitute a fundamental component of the screening process, serving as a critical mechanism for validating the accuracy and integrity of the information provided by applicants. Through rigorous scrutiny and verification procedures, shipping companies aim to corroborate the veracity of candidates' credentials and assertions, thereby ensuring transparency and reliability in the recruitment process (Caesar and Fei 2018). In alignment with principles from Occupational Psychology, the verification of credentials involves a comprehensive examination of academic qualifications, professional certifications, and licenses, thereby confirming the candidates' eligibility and proficiency for the roles they aspire to fulfill (Barrick and Mount 1991). This process aligns with the concept of the psychological profile of the job, which emphasizes the importance of matching the psychological requirements specific to a job with the qualifications and attributes of the applicants. Furthermore, scrutinizing employment history entails validating the accuracy of past job titles, responsibilities assumed, and duration of employment with previous employers, enabling shipping companies to evaluate the candidates' relevant experience and suitability for maritime positions (Morgeson and Humphrey 2006). This aspect corresponds to the Individual psychological profile of the person, which encompasses various psychological characteristics of the individual being assessed, including their work history and experiences (Judge and Bono 2001). Additionally, the investigation of any criminal records or legal issues serves to uncover potential red flags or inconsistencies in the candidates' background, thereby mitigating risks associated with the recruitment of individuals with a history of misconduct or legal entanglements (Cho and Lee 2016). Understanding the psychological aspects of such records can provide insights into an individual's propensity for ethical behavior and compliance with organizational norms, aligning with the principles of Occupational Psychology. Eventually, by

conducting thorough and diligent background checks informed by principles from Occupational Psychology, shipping companies can uphold the highest standards of integrity and diligence in their recruitment processes, thereby safeguarding against potential liabilities and preserving the security and reputation of the organization (Clark and Mitchell 2019; Gelles 2021).

Risk Assessment: Upon the conclusion of background checks, shipping companies undertake a comprehensive risk assessment aimed at systematically evaluating the potential security threats and vulnerabilities associated with each applicant (Cho and Lee 2016). This rigorous evaluation process involves a meticulous examination of various factors, including but not limited to, past behavior, affiliations, and any indicators of concern identified during the background verification process (BIMCO, et al. 2021). Through a thorough analysis of the applicant's historical conduct and associations, shipping companies endeavor to discern any discernible patterns or inclinations that may suggest a propensity toward unethical, illegal, or malicious behavior (Barnea and Meshulach 2020). Moreover, the assessment considers any affiliations or connections the individual may possess with entities or organizations that could pose a potential security risk to the shipping company's operations or assets (ENISA 2024). Additionally, the risk assessment scrutinizes any red flags or warning signs identified during the background check phase, such as discrepancies in the applicant's employment history or unresolved legal issues, to assess the severity of potential risks posed by the individual (Clark and Mitchell 2019). Through the implementation of this comprehensive risk assessment process, shipping companies can effectively identify and mitigate potential security threats, thereby bolstering the integrity and security of their crew management and recruitment practices (Caesar and Fei 2018).

Behavioral Analysis: Integrating behavioral analysis into profiling screening protocols constitutes a pivotal element in discerning potential security threats inherent in the recruitment processes of shipping companies. This facet of screening aligns with principles from Occupational Psychology, emphasizing the importance of understanding human behavior in organizational settings (Spector and Jex 1998). Through the lens of the psychological profile of the job, shipping companies aim to identify the psychological requirements specific to maritime roles and assess applicants' suitability based on their behavioral traits and characteristics (Barrick and Mount 1991). During this phase, a comprehensive evaluation is undertaken, encompassing both verbal and non-verbal cues exhibited by applicants throughout the recruitment process. Verbal cues may entail scrutinizing the language used, tone of voice, and responsiveness during interviews, while non-verbal cues encompass aspects such as body language, facial expressions, and overall demeanor (Morgeson and Humphrey 2006). This aligns with the concept of the Individual psychological profile of the person, which emphasizes the assessment of various psychological characteristics, including communication styles and interpersonal behaviors (Ones, Viswesvaran and Dilchert 2005). Furthermore, written communication,

including application materials and correspondence, undergoes scrutiny to discern any inconsistencies, discrepancies, or red flags that may signify potential security risks (Cho and Lee 2016). By leveraging behavioral analysis techniques informed by principles from Occupational Psychology, shipping companies can effectively identify subtle indicators of deception or malicious intent, thereby augmenting the reliability and integrity of their crew management and recruitment processes (Clark and Mitchell 2019; Gelles 2021).

Affiliation Verification: Affiliation verification represents a critical phase in the profiling screening process, designed to uphold the integrity and security of crew management and recruitment practices within shipping companies (Caesar and Fei 2018). This facet involves meticulous scrutiny and validation of applicants' associations with external entities, encompassing foreign governments, extremist organizations, or criminal networks. By rigorously assessing applicants' affiliations, shipping companies can evaluate the potential for loyalty conflicts or security threats that may jeopardize organizational interests or operations (Clark and Mitchell 2019). This verification process entails comprehensive inquiries, leveraging diverse sources of information, and scrutinizing applicants' backgrounds to accurately ascertain the nature and scope of their affiliations. Additionally, employing specialized investigative techniques and methodologies may be necessary to uncover any undisclosed or concealed connections that could pose security risks (ENISA 2024). Through diligent verification of applicants' affiliations, shipping companies can enhance their resilience against potential insider threats or external influences, thereby fostering a secure and conducive environment for crew management and recruitment activities (Gelles 2021; Catrantzos 2023).

Security Clearance Checks: Security clearance checks play a pivotal role in the profiling screening process, especially for positions requiring access to sensitive information or involvement in critical operations within shipping companies (Auster and Choo 1994). This rigorous procedure involves assessing individuals' eligibility to access classified data or engage in confidential activities based on a thorough evaluation of their background, trustworthiness, and allegiance to the organization (Barnea 2019). By subjecting applicants to comprehensive security clearance checks, shipping companies can determine the suitability and reliability of candidates for roles with heightened security responsibilities (ENISA 2024). This assessment delves into various aspects of the applicant's personal and professional history, including past affiliations, criminal records, financial stability, and overall integrity (Clark and Mitchell 2019). Additionally, security clearance checks may entail extensive interviews, background investigations, reference verifications, and character assessments to ascertain candidates' adherence to ethical standards and their ability to maintain confidentiality (ENISA 2024). Through meticulous scrutiny and adherence to established security protocols, shipping companies can effectively mitigate the risks associated with unauthorized access to sensitive information or potential breaches of security protocols (BIMCO, et al. 2021). By ensuring that

only individuals possessing the necessary qualifications, integrity, and loyalty are granted security clearances, organizations can enhance their resilience against internal threats and safeguard their critical assets from unauthorized disclosure or exploitation (Gelles 2021).

Continuous Monitoring: Continuous monitoring is an essential aspect of profiling screening, extending scrutiny beyond the initial hiring phase to encompass ongoing surveillance of employees' behavior and circumstances within shipping companies (Clark and Mitchell 2019). In line with principles from Occupational Psychology, this proactive approach acknowledges the dynamic nature of human behavior in organizational settings and emphasizes the importance of continuous assessment and adaptation (Spector and Jex 1998). Through systematic and vigilant monitoring mechanisms, such as surveillance systems, digital monitoring software, and periodic assessments, shipping companies can surveil employees' activities, communications, and interactions within the workplace environment (BIMCO, et al. 2021). This aligns with the concept of the psychological profile of the job, which emphasizes the identification of psychological requirements specific to maritime roles and the ongoing assessment of employees' alignment with these requirements (Morgeson and Humphrey 2006). Regular assessments and audits help identify potential red flags indicative of security vulnerabilities, such as sudden changes in behavior patterns, unauthorized access attempts, or suspicious communications (Gelles 2021). This corresponds to the Individual psychological profile of the person, which encompasses various psychological characteristics, including behavioral tendencies and communication styles (Ones, Viswesvaran and Dilchert 2005). Additionally, continuous monitoring facilitates the prompt identification and response to any deviations from established security protocols or compliance requirements, allowing organizations to intervene swiftly and mitigate potential threats before they escalate (ENISA 2024). By maintaining a vigilant stance and staying attuned to evolving security dynamics, shipping companies can bolster their resilience against internal threats and uphold the integrity and security of their operations and assets over the long term (Ball 2021).

Training and Awareness: Training and awareness initiatives are pivotal components in cultivating a culture of security and vigilance within shipping companies (Georgiadou, Mouzakitis and Askounis 2021). Through comprehensive training programs, employees acquire a deeper understanding of the importance of adhering to security protocols and remain alert to potential threats (ENISA 2024). These initiatives aim to equip staff with the requisite knowledge and skills to identify and respond effectively to suspicious activities or behaviors that could compromise the organization's security. Interactive workshops, seminars, and online modules are utilized to guide recognizing common indicators of security threats, such as anomalies in behavior patterns, unauthorized access attempts, or suspicious communications. Furthermore, training sessions offer practical advice on promptly and accurately reporting such incidents to designated authorities or security personnel for further investigation (ENISA 2024). By fostering a sense of ownership

and accountability for security among employees, these initiatives establish a robust frontline defense against both internal and external threats. Additionally, ongoing awareness campaigns and communication channels serve to reinforce key security messages and keep employees abreast of emerging risks or evolving security protocols. Through the cultivation of a culture of security consciousness and empowerment, shipping companies can bolster their resilience against potential threats and effectively safeguard their operations and assets (BIMCO, et al. 2021); (Georgiadou, Mouzakitis and Askounis 2021).

Adherence to Regulations: Ensuring adherence to regulations is fundamental to establishing robust security and CI practices within shipping companies. Organizations must rigorously comply with pertinent laws, regulations, and industry standards governing security protocols to uphold the integrity and credibility of their operations (Giannakopoulou, Thalassinos and Stamatopoulos 2016). By aligning profiling screening procedures with legal requirements and industry best practices, shipping companies manifest their dedication to maintaining security standards and mitigating potential risks proficiently (Cho and Lee 2016). This necessitates a comprehensive understanding and implementation of regulations such as the International Ship and Port Facility Security (ISPS) Code, which mandates stringent security measures for ships and port facilities globally (BIMCO, et al. 2021). Moreover, compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), ensures the lawful and ethical handling of sensitive information collected during screening processes (Auster and Choo 1994; Ronn 2016; Barnea 2019). shipping companies must also remain vigilant regarding evolving regulatory landscapes and adapt their security practices accordingly to effectively address emerging threats and regulatory modifications (ENISA 2024). By prioritizing compliance and regulatory adherence, organizations underscore their commitment to upholding the highest standards of security and integrity, thereby fostering trust and confidence among stakeholders and safeguarding the safety and security of maritime operations (Gelles 2021).

In conclusion, CI profiling and screening procedures in shipping companies encompass a thorough and methodical process aimed at evaluating the backgrounds, behaviors, and affiliations of individuals to mitigate security risks proficiently. Through adherence to these steps and the incorporation of robust security protocols, shipping companies can fortify their defenses against potential threats, thereby ensuring the protection of their operations and assets.

Potential Vulnerabilities in Counterintelligence Profiling and Screening

CI profiling and screening procedures in shipping companies are susceptible to significant vulnerabilities that necessitate careful attention and mitigation strategies.

A notable vulnerability arises from the reliance on potentially incomplete or inaccurate information during the screening process, which can lead to misguided assessments and compromise the overall efficacy of screening procedures (Kanellopoulos 2022). Additionally, biases present within the screening process pose another substantial vulnerability, as they may influence decision-making and result in unfair treatment or the overlooking of critical information (Lowenthal 2009); (Giannakopoulou, Thalassinos and Stamatopoulos 2016). Furthermore, the insufficient training of personnel responsible for conducting screenings constitutes another vulnerability, as it can diminish their proficiency and lead to oversight of crucial indicators or the failure to detect red flags effectively.

To address these vulnerabilities, the implementation of best practices in profiling screening is imperative. Leveraging multiple data sources for verification is paramount to enhance the accuracy and reliability of screening outcomes (Lowenthal 2009); (Barnea 2019). Cross-referencing information from various sources enables companies to validate applicant credentials more effectively and identify discrepancies (Auster and Choo 1994). Moreover, regular training and certification programs for screening personnel are essential to maintain competence and professionalism. Ongoing training ensures that personnel possess the requisite skills and knowledge to perform screenings accurately and impartially. Continuous evaluation and refinement of screening protocols are also crucial to address evolving threats and lessons learned from past experiences. Regular reviews and updates to screening procedures enable companies to adapt to emerging risks and bolster the effectiveness of their CI efforts (Clark and Mitchell 2019).

By prioritizing these best practices, shipping companies can mitigate vulnerabilities within their profiling screening processes and uphold the integrity and reliability of their security protocols. This proactive approach not only enhances the screening process's effectiveness but also contributes to overall organizational resilience against security threats in the maritime industry.

Conclusions

In summary, although CI profiling and screening procedures significantly contribute to enhancing security measures within shipping companies, they are susceptible to vulnerabilities that demand attention. Drawing from insights in Occupational Psychology, it is imperative to address challenges such as reliance on potentially inaccurate or incomplete information, biases in the screening process, and inadequate training of personnel to bolster the efficacy of these procedures.

By aligning with the psychological profile of the job, shipping companies can refine their screening processes by identifying and prioritizing the psychological requirements specific to maritime roles. This includes assessing the cognitive,

emotional, and behavioral attributes necessary for effective security screening (Barrick and Mount 1991).
Similarly, the individual psychological profile of the person plays a crucial role in ensuring the suitability of screening personnel. By considering factors such as personality traits, communication skills, and decision-making abilities, companies can select and train personnel who are well-equipped to handle the complexities of profiling screening (Judge and Bono 2001).

Nevertheless, by adopting best practices such as leveraging multiple data sources for verification, providing regular training and certification programs for screening personnel, and continuously evaluating and refining screening protocols, shipping companies can effectively mitigate these vulnerabilities (Barnea 2019).

Companies must remain vigilant and adaptable in the face of evolving threats, ensuring that their CI efforts remain robust and reliable (Kanellopoulos 2022). Through a proactive and comprehensive approach to profiling screening, shipping companies can fortify their security posture and mitigate potential breaches, thereby contributing to the overall safety and integrity of maritime operations.

References

Akpan, F., G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos. 2022. "Cybersecurity challenges in the Maritime Sector ." *Network* 2 (1): pp. 123–138. https://doi.org/10.3390/network2010009.

Alcaide, J.I., and R.G. Llave. 2020. "Critical infrastructures cybersecurity and the Maritime Sector ." *Transportation Research Procedia* 45: pp. 547–554. https://doi.org/10.1016/j.trpro.2020.03.058.

Auster, E., and C.W. Choo. 1994. "How senior managers acquire and use information in environmental scanning." *Information Processing & Management* 30 (5): pp. 607–618. https://doi.org/10.1016/0306-4573(94)90073-6.

Ball, K. 2021. "Electronic Monitoring and Surveillance in the Workplace." *Joint Research Center – European Commission.* https://publications.jrc.ec.europa.eu/repository/handle/JRC125716.

Barnea, A. 2019. "Big Data and Counterintelligence in Western countries ." *International Journal of Intelligence and Counterintelligence* 32 (3): pp. 433–447.

Barnea, A., and A. Meshulach. 2020. "Forecasting for Intelligence Analysis: Scenarios to abort strategic surprise." *International Journal of Intelligence and Counterintelligence* 34 (1): pp. 106–133.

Barrick, M.R., and M.K. Mount. 1991. "The Big Five personality dimensions and job performance: A meta-analysis." *Personnel Psychology* 44 (1): pp. 1-26.

BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo, Shipowners (INTERCARGO),

InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International, Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC). 2021. *The Guidelines on Cyber Security Onboard Ships.* https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pd.

Caesar, L.D., and J. Fei. 2018. "Recruitment and the image of the shipping industry." In *Managing Human Resources in the Shipping Industry*, pp. 18-36. Routledge. doi:10.4324/9781315740027-2.

Catrantzos, N. 2023. *Managing the Insider Threat No Dark Corners and the Rising Tide Menace.* CRC Press.

Cho, I., and K. Lee. 2016. "Advanced risk measurement approach to insider threats in Cyberspace." *Intelligent Automation & Soft Computing* 22 (3): pp. 405–413. https://doi.org/10.1080/10798587.2015.1121617.

Clark, R.M., and W. Mitchell. 2019. *Deception: Counterdeception and Counterintelligence.* Washington, DC: CQ Press.

Cybersecurity and Infrastructure Security Agency. 2017. *Awareness Briefing: Chinese Cyber Activity Targeting Managed Service Providers.* https://www.cisa.gov/sites/default/files/c3vp/Chinese-Cyber-Activity-Targeting-Managed-Service-Providers.pdf.

Duvenage, P., and S. Solms. 2014. *Putting Counterintelligence in Cyber Counterintelligence. 13th European Conference on Cyber Warfare and Security.* https://www.researchgate.net/publication/328732134_Putting_Counterintelligence_in_Cyber_Counterintelligence.

Duvenage, P., V. Jaquire, and S. Solms. 2018. "Towards a Literature Review on Cyber Counterintelligence ." *Journal of Information Warfare* 17 (4): pp. 284-297. https://www.jstor.org/stable/26783824.

ENISA. 2024. *Cyber Resilience Act Requirements Standards Mapping.* https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping .

Estay, D. 2020. *Cyber resilience for the shipping industry. CyberShip Project.* https://www.dendanskemaritimefond.dk/wp-content/uploads/2017/03/Cybership_Report_WP_5.pdf.

Europol. 2023. *New Modus Operandi: How organized crime infiltrates the ports of Europe .* https://www.europol.europa.eu/media-press/newsroom/news/new-modus-operandi-how-organised-crime-infiltrates-ports-of-europe.

Gelles, M. 2021. "Insider threat prevention, detection, and mitigation." In *International Handbook of Threat Assessment*, pp. 669–679. https://doi.org/10.1093/med-psych/9780190940164.003.0037.

Georgiadou, A., S. Mouzakitis, and D. Askounis. 2021. "Detecting insider threat via a cyber-security culture framework." *Journal of Computer Information Systems* 63 (4): pp. 706–716.

Giannakopoulou, E.N., E.I. Thalassinos, and T.V. Stamatopoulos. 2016. "Corporate governance in shipping: an overview." *Maritime Policy & Management* 43 (1): pp. 19-39.

Grammenos, T. 2010. *The Handbook of Maritime Economics and Business.* Edited by Lloyd's List.

Greene, R. 1966. *Business Intelligence and Espionage.* Homewood: Dow Jones- Irwin.

Johnson, L.K. 2010. *Handbook of Intelligence Studies.* London: Routledge.

Judge, T.A., and J.E. Bono. 2001. "Relationship of core self-evaluations traits—self-esteem, generalized self-efficacy, locus of control, and emotional stability—with job satisfaction and job performance: A meta-analysis." *Journal of Applied Psychology* 86 (1): pp. 80-92.

Kanellopoulos, A.N. 2022. "The Importance of Counterintelligence Culture in State Security." *Global Security and Intelligence* Note 5. https://www.buckingham.ac.uk/wp-content/uploads/2022/07/GSIN_5a.pdf.

__. 2023. "The Dimensions of Counterintelligence and Their Role in National Security." *Journal of European and American Intelligence Studies* 6 (2): pp. 85-104.

__. 2024. "Insider threat mitigation through human intelligence and counterintelligence: A case study in the shipping industry." *Defense and Security Studies* (5) 1: pp. 10-19. https://doi.org/10.37868/dss.v5.id261.

Kantharia, Raunek. 2019. *The Story of Maersk Alabama Container Vessel.* https://www.marineinsight.com/marine-piracy-marine/the-story-of-maersk-alabama-container-vessel/.

Leovy, J. 2017. "Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks." *Los Angeles Times.* https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html.

Lowenthal, M. 2009. *Intelligence: From secrets to policy.* Washington, DC: CQ Press.

Morgeson, F.P., and S.E. Humphrey. 2006. "The Work Design Questionnaire (WDQ): Developing and validating a comprehensive measure for assessing job design and the nature of work ." *Journal of Applied Psychology* 91 (6): pp. 1321-1339.

Ones, D.S., C. Viswesvaran, and S. Dilchert. 2005. "Cognitive ability in selection decisions." *Handbook of employee selection* 3: pp. 431–468.

Prunckun, H.W. 2019. *Counterintelligence theory and practice.* London: Rowman et Littlefield.

Ronn, K.V. 2016. "Intelligence ethics: A critical review and future perspectives." *International Journal of Intelligence and Counterintelligence* 29 (4): pp. 760–784. https://doi:10.1080/08850607.2016.1177399.

Shaikh, R. 2018. "More spills... thousands of passports, driver's licenses, & Photo ids of fedex customers exposed." *Wccftech.* https://wccftech.com/thousands-passports-fedex-exposed/.

Spector, P.E., and S.M. Jex. 1998. "Development of four self-report measures of job stressors and strain: Interpersonal Conflict at Work Scale, Organizational Constraints Scale, Quantitative Workload Inventory, and Physical Symptoms Inventory." *Journal of Occupational Health Psychology* 3 (4): pp. 356-367.

Wettering, F.L. 2000. "Counterintelligence: The broken triad." *International Journal of Intelligence and Counterintelligence* 13 (3): pp. 265–300.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Navigating organizational excellence: a comparative study and roadmap for streamlining defense infrastructure organizational model of Georgia

Ivan OKROMTCHEDLISHVILI, Ph.D.*
* Associate Professor, Sulkhan-Saba Orbeliani University, Tbilisi, Georgia
e-mail: iokro@yahoo.com

Abstract

In the face of evolving geopolitical dynamics and increasing security challenges, the efficacy of a nation's defense infrastructure is pivotal. This article conducts a comprehensive exploration of defense infrastructure organizational models, centering on the United Kingdom, France, Germany, Australia, and Latvia. Through a meticulous comparative analysis, the study delves into organizational structures, international operations, responsibilities, and strategic focuses of these nations' defense infrastructure entities. The goal is to glean insights applicable to Georgia's unique context, identifying key differences and commonalities to formulate a strategic roadmap for enhancing its defense infrastructure capabilities. The article examines each country's defense infrastructure model, highlighting distinctive features in organizational structure, international operations, responsibilities, and strategic focus. Drawing upon these insights, the study proposes tailored recommendations for Georgia, spanning organizational structure, international operations, responsibilities and focus, modernization and strategy, and integration of departmental efforts. Key entities within Georgia's defense infrastructure organizational model, such as the Department of Defense Sustainability, the J-4 Logistics Planning Department, and the Command for Logistics Support of the Troops, are illuminated to underscore their pivotal roles in fortifying the country's defense capabilities. Concluding with the identification of key areas for improvement in Georgia's defense infrastructure organization, the article outlines recommendations encompassing organizational structure, international operations, responsibilities and focus, modernization and strategy, and integration of departmental efforts. By aligning Georgia's defense infrastructure with international best practices, the nation can enhance security, contribute to regional stability, and actively participate in global security efforts. In essence, this article serves as a strategic guide for Georgia, offering a roadmap to fortify its defense infrastructure in a rapidly changing world. Through a synthesis of global insights and tailored recommendations, Georgia can position itself as a resilient and adaptable force, safeguarding national interests and contributing to a more secure global landscape.

Keywords:
defense infrastructure; organizational models; comparative analysis; Georgia; international operations; organizational structure; strategic focus; modernization.

Article info
Received: 26 March 2024; Revised: 17 April 2024; Accepted: 30 May 2024; Available online: 5 July 2024

Citation: Okromtchedlishvili, I. 2024. "Navigating organizational excellence: a comparative study and roadmap for streamlining defense infrastructure organizational model of Georgia". *Bulletin of "Carol I" National Defence University*, 13(2): 60-78. https://doi.org/10.53477/2284-9378-24-20

Introduction

In a time characterized by changing geopolitical environments and the rise of new security threats, the effectiveness of a nation's defense infrastructure is paramount. This article embarks on a comprehensive exploration of defense infrastructure organizational models, with a particular focus on the United Kingdom, France, Germany, Australia, and Latvia.
Through comparative analysis, we delve into the organizational structures, international operations, responsibilities, and strategic focuses of these nations' defense infrastructure entities: The Defense Infrastructure Organization (DIO) in the UK, the Defense Infrastructure Service (SID) in France, the Infrastructure, Environmental Protection, and Services (IUD) in Germany, the Infrastructure Division in Australia and the Logistics and Defense Investments Policy Department in Latvia.

This comparative study not only provides a nuanced understanding of each nation's approach but also aims to extract valuable insights applicable to Georgia's unique context. By identifying key differences and commonalities, we can discern areas for improvement and formulate a strategic blueprint for enhancing the defense infrastructure capabilities of Georgia.

The subsequent sections explore the intricacies of each country's defense infrastructure model, highlighting distinctive features in organizational structure, international operations, responsibilities, and strategic focus. Drawing upon these insights, the article then proposes recommendations tailored to Georgia's specific needs. The focus areas include organizational structure, international operations, responsibilities and focus, modernization and strategy, and integration of departmental efforts.

As we navigate through the current landscape of Georgia's defense infrastructure organization, we shed light on two key entities: The Department of Defense Sustainability and the J-4 Logistics Planning Department, both playing pivotal roles in fortifying the country's defense capabilities. Additionally, we delve into the Command for Logistics Support of the Troops, further underscoring the intricate relationship between effective infrastructure management and overall defense success.

The article concludes with an identification of key areas for improvement in Georgia's defense infrastructure organization. The recommendations span organizational structure, international operations, responsibilities and focus, modernization and strategy, and integration of departmental efforts. By aligning Georgia's defense infrastructure with international best practices and tailoring strategies to its specific needs, the nation can enhance its security, contribute to regional stability, and actively participate in global security efforts.

In essence, this article serves as a strategic guide for Georgia, offering a roadmap to fortify its defense infrastructure in a rapidly changing world. Through the synthesis of global insights and tailored recommendations, Georgia can position itself as a resilient and adaptable force, safeguarding national interests and contributing to a more secure global landscape.

1. Overview and Comparative Analyses of International Best Practices of Defense Infrastructure Organizational Models

The study employs a comparative approach to analyze the defense infrastructure organizational models of five nations: The United Kingdom, France, Germany, Australia, and Latvia. This method involves examining similarities and differences in organizational structures, international operations, responsibilities, and strategic focuses. Each nation's defense infrastructure model was studied as a case study, with a focus on understanding the nuances of their organizational structures, international operations, responsibilities, and strategic focuses. This method allowed for in-depth exploration and contextual understanding of each country's approach.

Information on the defense infrastructure organizational models of the selected nations was gathered, including organizational structures, international operations, responsibilities, and strategic focuses. The gathered data was compared and contrasted across the five nations to identify patterns, similarities, and differences in their defense infrastructure models. This analysis helped in understanding the various approaches and their effectiveness.
Key insights from the comparative analysis were extracted to provide a basis for formulating recommendations. Based on the identified insights, recommendations tailored to Georgia's specific needs in enhancing its defense infrastructure capabilities were developed. These recommendations address areas such as organizational structure, international operations, responsibilities and focus, modernization and strategy, and integration of departmental efforts.

1.1. United Kingdom: The Defense Infrastructure Organization (DIO)

The UK Ministry of Defense (MOD) possesses a varied land portfolio encompassing 220,000 hectares, equivalent to approximately 0.9% of the total landmass in the United Kingdom, with additional rights over an additional 204,000 hectares. This substantial landholding establishes the MOD as one of the foremost landowners in the country. Predominantly rural, exceeding 80% of the estate serves as venues for military training, with many areas carrying environmental designations necessitating specialized management. The built segment comprises naval bases, barracks, airfields, and other defense-related facilities. Furthermore, the MOD oversees 25 training estates situated across the globe (DIO 2017).
The establishment of the Defense Infrastructure Organization (DIO) in April 2011 marked a significant development within the Ministry of Defense (MOD), as it

unified the management of defense infrastructure under a single organization for the first time. The DIO, a part of the MOD, comprises around 5,000 professionals with diverse expertise, spanning town planning, digital content, estate surveying, airfield pavement management, accounting, forestry, specialized engineering, and various corporate head office functions (DIO 2017).
The DIO serves as the estate expert for defense, playing a crucial role in supporting the armed forces by planning, building, maintaining, and servicing infrastructure. The organization's responsibilities span a wide range of functions aimed at enabling defense personnel to live, work, train, and deploy effectively, both domestically and overseas.

Key responsibilities include planning and delivering major capital projects and lifecycle refurbishment initiatives to ensure the ongoing effectiveness and resilience of defense infrastructure. Additionally, the organization provides utility services to support various defense activities, ensuring the availability of essential resources for defense personnel.
Moreover, DIO manages soft facilities management aspects, such as cleaning and catering services, contributing to the overall well-being and efficiency of defense personnel. DIO is responsible for providing a safe place for defense personnel to train, emphasizing the importance of secure and effective training environments.

The organization also allocates Service Families Accommodation, recognizing the significance of providing suitable housing for military families. Furthermore, DIO procures and manages routine maintenance and reactive repair services to ensure the ongoing functionality and security of defense infrastructure.
Additionally, the organization maintains a central register of asset information, contributing to effective infrastructure planning and decision-making. DIO acts as the steward of the defense estate, overseeing and safeguarding the various elements of defense infrastructure.
Finally, DIO provides both physical and electronic security systems through its Security Services Group, emphasizing the importance of protecting defense assets (GOV UK n.d.).

DIO Strategy
The organization's strategy is outlined in its 2020-2030 report, focusing on becoming one cohesive team that provides excellent advice and outstanding delivery. The strategy addresses the evolving nature of global threats, including climate change and state aggressors, and highlights the need for resilience and transformation within the Defense Estate. Key areas of focus include implementing an asset management system, improving delivery to customers, and becoming an expert in sustainability, climate change, and the environment (GOV UK 2020).

Priorities and Modernization Efforts
DIO's priorities center around enhancing its capability to advise and deliver, with a specific focus on informed asset management and improved infrastructure planning.

The organization aims to modernize by embracing new technologies, utilizing digital systems more effectively, and optimizing the Infrastructure Management System (IMS). The emphasis on cross-cutting projects and continuous improvement across enabling functions like finance, commercial, people, and corporate services reflects a holistic approach to supporting DIO's customer capability needs.

The DIO plays a crucial role in overhauling accommodation services for UK Armed Forces families, marking a significant milestone with the introduction of new Future Defense Infrastructure Services (FDIS) contracts. These contracts, part of a £3 billion program, prioritize customer service and responsiveness, aiming to provide high-quality homes and community spaces for military families across the UK (Inside DIO Blog 2022).

In summary, the Defense Infrastructure Organization plays a vital role in ensuring the resilience, efficiency, and sustainability of defense infrastructure, with a commitment to ongoing modernization and transformation to meet evolving challenges.

1.2. France: The Defense Infrastructure Service (Service d'Infrastructure de la Défense/SID)

The Defense Infrastructure Service (Service d'Infrastructure de la Défense or SID) is a critical component of the Ministry of the Armed Forces in France, specializing in infrastructure and energy management. It serves as the ministerial reference for construction, property maintenance, control of non-stored energy, and administrative and technical management of assets.

The responsibilities and expertise of SID involve the management of one of the largest real estate portfolios in the French government. It is responsible for constructing, maintaining, and administering the entire real estate domain of the Ministry of the Armed Forces, both domestically and internationally.

The service supports the adaptation of infrastructure for the Armed Forces, directorates, and services across various locations. SID's operational contract entails meeting the infrastructure needs of the Armed Forces in diverse scenarios, including deterrence, external operations, and crisis prevention. SID oversees construction, renovation, and maintenance operations while focusing on cost control and adherence to deadlines.

The service actively manages and optimizes energy consumption in the ministry's real estate assets, incorporating sustainable development considerations into infrastructure projects. SID provides technical, administrative, and legal expertise to support the command of the Armed Forces, directorates, and services in their infrastructure-related needs.

The service actively contributes to local economic dynamism by supporting businesses and fostering partnerships in more than 210 municipalities. As the construction department of the ministry, SID conducts operations and acts as the contracting authority with service providers contributing to studies and construction.

SID has a territorial network close to the forces, addressing their needs through a decentralized structure. Key components include the Central Management in Versailles, the Center of Expertise for Defense Infrastructure Techniques (CETID), the National Defense Infrastructure Production Center (CNPID), seven SID establishments (ESID), and 51 Defense Infrastructure Support Units (USID). SID is an operational service involved in external operations to support French forces deployed abroad, managing infrastructure during deployment and long-term installation. Nine Defense Infrastructure Directorates, located overseas and abroad, execute SID missions to support sovereignty forces and prepositioned forces (MOAF n.d.).
In summary, SID plays a vital role in ensuring the construction, maintenance, and adaptability of defense infrastructure for the Ministry of the Armed Forces, both nationally and internationally, while actively contributing to local economic development.

1.3. Germany: Infrastructure, Environmental Protection, and Services (IUD)
The organizational unit known as Infrastructure, Environmental Protection, and Services (IUD – Infrastruktur, Umweltschutz und Dienstleistungen) plays a pivotal role within the Bundeswehr, serving as the largest civilian component with over 26,000 civilian and military positions. This unit is responsible for providing comprehensive services across the entire Bundeswehr, encompassing construction and maintenance of facilities, as well as statutory protective tasks such as occupational safety, environmental protection, and fire protection.

Key functions and responsibilities of the IUD include overseeing the construction and maintenance of approximately 1,500 military installations and more than 33,000 buildings, covering a vast area of over 260,000 hectares. It also provides statutory protective tasks that include occupational safety, environmental protection, and fire protection for the entire Bundeswehr.

IUD's service portfolio extends to catering and travel management, ensuring that these services are provided not only domestically but also for personnel serving abroad. The unit actively supports civilian operations abroad, playing a crucial role in ensuring the food supply and transportation services for service members deployed in theaters of operation.

The major organizational element comprises the Federal Office of Infrastructure, Environmental Protection, and Services (BAIUDBw) based in Bonn, the Bundeswehr Subsistence Office (VpflABw) in Oldenburg, Lower Saxony, and the Bundeswehr Firefighting and Fire Protection Centre (ZBrdSchBw) located in Sonthofen, Bavaria. Service provision at the regional level is facilitated by seven Centers of Expertise for Construction Management and six Centers of Expertise for Travel Management. Forty-two Service Centers (BwDLZ) located throughout Germany operate under the BAIUDBw, providing a comprehensive range of services. Seven Federal Republic of Germany Offices of Defense Administration abroad (BWVSt) in Belgium, France,

Italy, the Netherlands, Poland, the United Kingdom, and the United States cater to the needs of personnel serving abroad. Seven Field Offices of Defense Administration (EinsWVSt) are operated by BAIUDBw to provide support for service members deployed on operations (Bundeswehr n.d.).

In summary, the Infrastructure, Environmental Protection, and Services unit plays a crucial role in ensuring the effective functioning of the Bundeswehr by managing a diverse set of responsibilities, from construction and maintenance to protective tasks and support for operations abroad. The comprehensive service portfolio underscores its significance as a key organizational element within the Ministry of Defense.

1.4. Australia: The Infrastructure Division of the Security and Estate Group of the Department of Defense

The Infrastructure Division, operating as part of the Security and Estate Group, plays a pivotal role in Australia by managing the development, maintenance, and disposal of the Defense estate. This estate represents one of the largest real estate portfolios in the country, supporting over 90,000 personnel across all states and territories.

The division engages in comprehensive planning and construction activities, often projecting developments up to thirty years into the future.
The division is responsible for reviewing, developing, and constructing facilities and sites to effectively manage the Defense estate. It is involved in creating heritage and environment policies for all Defense properties in Australia, as well as those for Australian forces operating overseas.

The Capital Facilities and Infrastructure section of the division focuses on the planning and development of capital facilities and infrastructure essential to supporting Defense activities.
The Property Management section oversees the planning and management of divestment of surplus Defense properties, property acquisitions, leasing, and handling issues related to native title, offshore mining, and petroleum exploration.
The division is actively involved in initiatives related to the United States Force Posture and the Australia-Singapore Military Training Initiative (AGa n.d.).

Infrastructure and estate projects conducted by the division aim to maximize the potential of Defense-managed areas, ensuring ongoing capability, training, and support facilities.
Major capital works projects delivered by the Commonwealth require Parliamentary referral and/or approval via the Parliamentary Standing Committee on Public Works, in accordance with the Public Works Committee Act 1969 (AGb n.d.).

In essence, the Infrastructure Division is a multifaceted entity crucial to the strategic planning, development, and management of the extensive Defense estate in Australia, ensuring the provision of necessary facilities for the armed forces.

1.5. Latvian Defense Infrastructure: An Organizational Overview

Latvia's defense infrastructure stands as a testament to the nation's commitment to national security and preparedness. The organizational structure governing its development and maintenance ensures strategic planning, efficient resource allocation, and collaborative partnerships both domestically and internationally.

At the helm of infrastructure development is the Logistics and Defense Investments Policy Department of the Defense Ministry. This department serves as the nexus for gathering the needs of the National Armed Forces (NBS) and formulating comprehensive plans for the construction of new facilities and the upkeep of existing real estate. Working in tandem with the State Defense and Military Procurement Centre (VAMOIC), which handles the construction, management, and execution of environmental protection initiatives within the defense sector, the department oversees the implementation of vital infrastructure projects aimed at bolstering the nation's security (MOD of Latvia n.d.).

One of the primary focuses of infrastructure development is the enhancement of key military bases, notably Ādaži and Lielvārde. These bases play a pivotal role in hosting critical operations, including the NATO Battlegroup, underscoring their strategic importance. Major construction projects, supported by substantial funding allocations, have been launched to fortify these bases, including the construction of multi-functional barracks, sports complexes, and administrative buildings.

Despite owning a considerable portfolio of real estate, many structures within the Ministry of Defense exhibit signs of aging, prompting a gradual transition toward modernization. The demolition of outdated facilities and the construction of new ones are central to this endeavor, aimed at improving operational efficiency and overall security standards.

External funding sources play a significant role in financing infrastructure projects. Contributions from the NATO Security Investment Program (NSIP), the United States-European Deterrence Initiative (EDI), and partnerships with countries like Luxembourg provide essential financial support, enabling Latvia to strengthen its defense capabilities and fulfill its obligations as a host state.

Cooperation with local municipalities further enhances infrastructure development efforts, facilitating projects such as road reconstruction and environmental cleanup. Additionally, the integration of national financing ensures the continuity of construction projects and the provision of necessary infrastructure to support the National Armed Forces and allied forces.

Looking ahead, the organizational structure governing Latvian defense infrastructure remains focused on key priorities. These include the provision of infrastructure for hosting the NATO Battle Group, the implementation of NSIP projects, and the development of National Guard bases. Investments in training infrastructure, including shooting ranges and support facilities, underscore Latvia's commitment to enhancing its defense readiness and capabilities (MOD of Latvia n.d.).

In conclusion, Latvia's defense infrastructure thrives under a robust organizational framework characterized by strategic planning, collaborative partnerships, and a commitment to modernization. Through sustained efforts and partnerships both domestically and internationally, Latvia stands poised to further strengthen its defense capabilities and contribute to regional security and stability.

1.6. Comparative Analysis of Defense Infrastructure Organizational Models: Similarities and Differences

Organizational Approach

- *United Kingdom:* DIO operates as a unified organization within the MOD, with a centralized structure.
- *France:* SID employs a decentralized structure with various centers, establishments, and overseas directorates.
- *Germany:* IUD operates as the largest civilian element within the Bundeswehr, with regional centers of expertise and decentralized support units.
- *Australia:* The Infrastructure Division operates as part of a larger group, focusing on comprehensive planning and construction, reflecting a centralized approach.
- *Latvia:* The Logistics and Defense Investments Policy Department collaborates with the National Armed Forces and the State Defense and Military Procurement Centre to develop defense infrastructure, emphasizing strategic planning and efficient resource allocation.

International Operations

- *United Kingdom:* DIO primarily focuses on domestic infrastructure management.
- *France:* SID actively engages in external operations, supporting French forces abroad.
- *Germany:* IUD supports operations abroad, contributing to local economic development.
- *Australia:* The Infrastructure Division actively participates in international initiatives, including military training programs.
- *Latvia:* Latvian defense infrastructure development includes collaboration with international partners, particularly through funding from sources like NSIP and EDI, to strengthen defense capabilities and fulfill host state obligations.

Responsibilities and Focus

- *United Kingdom:* DIO's responsibilities cover a wide range, from major capital projects to soft facilities management.
- *France:* SID's focus includes construction, maintenance, and energy management with a strong emphasis on sustainability.

● *Germany:* IUD provides comprehensive services, including protective tasks, catering, and travel management.
● *Australia:* The Infrastructure Division emphasizes estate planning, environmental policies, and international military training initiatives.
● *Latvia:* Latvia's defense infrastructure focuses on enhancing key bases, modernizing aging structures, and supporting future NATO initiatives, reflecting a commitment to defense readiness and regional security.

Modernization and Strategy

● *United Kingdom:* DIO's strategy includes modernization efforts, digital systems, and resilience against evolving threats.
● *France:* SID focuses on technical expertise, sustainability, and economic dynamism.
● *Germany:* IUD emphasizes ongoing capability enhancement, training support, and strategic planning.
● *Australia:* The Infrastructure Division is involved in ongoing modernization and strategic planning, projecting developments up to thirty years into the future.
● *Latvia:* Latvia's defense infrastructure strategy prioritizes modernization and collaboration with international partners to strengthen defense capabilities and contribute to regional stability.

In summary, while each defense infrastructure model prioritizes the effective management of resources and infrastructure, differences in organizational structures, international operations, specific responsibilities, and strategic focuses highlight the unique approaches of the United Kingdom, France, Germany, Australia, and Latvia.

2. Current Landscape of Defense Infrastructure Organization in Georgia

2.1. Department of Defense Sustainability: Enhancing Security and Operational Efficiency

The Department of Defense Sustainability within the Ministry of Defense of Georgia plays a crucial role in fortifying the defense capabilities of the country, with a particular emphasis on infrastructure-related processes. The charter of the Department outlines the multifaceted responsibilities assigned to the department, aligning its efforts with the broader goal of ensuring the resilience of the Defense Forces and fostering interoperability with NATO.

One of the paramount tasks assigned to the department is the formulation of the infrastructure system development policy for the entire ministry. This includes defining a strategic-conceptual framework for effective infrastructure management, determining key directions for infrastructure development, and identifying

priorities for long-term infrastructure projects. The department is charged with the responsibility of developing recommendations based on the analysis of experiences gained in the field, aiming to continually improve the infrastructure system.

The competencies of the infrastructure management division within the department are pivotal in achieving these objectives. This division is tasked with not only developing the infrastructure system development policy but also actively monitoring its implementation. By coordinating the process of developing the infrastructure program budget, the division ensures that the allocated resources align with the strategic goals of infrastructure enhancement.

Furthermore, the standardization management division focuses on establishing a NATO-compatible standardization management system, specifically in the context of infrastructure. This involves developing policies for the system's development, ensuring its proper functioning, and coordinating consultation and training activities. The division collaborates with national and international organizations to implement the standardization management system for infrastructure, identifying and overcoming challenges related to standardization and compatibility.

In parallel, the logistics policy section operates with a keen eye on infrastructure. It is tasked with developing national principles and policies for logistics, emphasizing interagency cooperation in the development of logistics systems. By monitoring the interaction and interoperability of structural units involved in the logistics system, the section ensures the seamless integration of infrastructure elements. Recommendations for logistics system development are drawn based on international experience, contributing to sustainability and readiness.

The codification section, the fourth structural unit, contributes significantly to infrastructure-related processes. Responsible for developing the codification management system, introducing a unified codification catalog, and organizing relevant training courses, this section ensures that infrastructure elements are efficiently cataloged and managed (MOD 2022).

In conclusion, the Department of Defense Sustainability in Georgia's Ministry of Defense is at the forefront of fortifying the country's defense capabilities through strategic infrastructure development. The integration of various divisions and sections with explicit responsibilities for infrastructure-related processes underscores the department's commitment to fostering a robust and resilient defense infrastructure.

2.2. Navigating the Future: The Strategic Role of the J-4 Logistics Planning Department

Nestled within the intricate framework of the J-4 Logistics Planning Department of the General Staff of the Defense Forces of Georgia, the Infrastructure Planning

Division emerges as a specialized entity dedicated to the orchestration of pivotal infrastructure-related processes. This division shoulders a spectrum of competencies crucial for steering the Defense Forces toward enhanced operational efficacy and resilience.

At the heart of the division's mandate lies the astute ability to identify and delineate the primary directions for the development of infrastructure. This discernment is carefully calibrated to align seamlessly with the overarching Strategic Development Plan of the Defense Forces. By setting strategic priorities, the division becomes an architectural visionary, shaping the infrastructure landscape in concordance with broader defense objectives.

Delving into the realm of foresight, the division is tasked with crafting comprehensive long-term plans for infrastructure facilities. This spans the spectrum from construction to design and repair, ensuring a holistic approach to infrastructure development. Through meticulous planning, the division seeks to fortify the foundations of functionality, fostering facilities that stand the test of time and evolving operational needs.

Acknowledging the intrinsic interplay between infrastructure and vital resources, the division extends its influence into offering recommendations for the provision of heating and energy resources to infrastructure facilities. This foresighted approach ensures that the facilities not only stand robust but are equipped to navigate the complexities of energy demands, thereby enhancing sustainability (MOD 2021a).

In summary, the Infrastructure Planning Division stands as a beacon of strategic prowess within the broader landscape of defense logistics. Its commitment to strategic and long-term planning, coupled with the nuanced provision of recommendations for crucial resources, underscores its indispensable role in fortifying the infrastructure backbone of the Defense Forces. By navigating the intricate intersection of vision and pragmatism, the division propels the Defense Forces toward a future marked by resilient and strategically aligned infrastructure capabilities.

2.3. Logistics Empowerment: A Pillar of Defense Forces Infrastructure

The Command for Logistics Support of the Troops within the Defense Forces stands as a linchpin in the realm of infrastructure-related processes, with a steadfast focus on the effective provisioning, management, and maintenance of essential resources. This pivotal command shoulders a range of tasks and functions intricately tied to infrastructure, ensuring the seamless operation and sustenance of critical assets.

The command is entrusted with the responsibility of ensuring the timely and comprehensive provision of essential property to ministry subdivisions. This mandate extends across diverse situations, necessitating meticulous planning and adherence to relevant requirements. A critical facet involves accounting for

immovable property and implementing measures for its effective management and maintenance, which is given meticulous oversight by the command.
Collaborating with entrepreneurs, the command orchestrates the gradual repair of material and technical facilities within ministry units. This strategic approach ensures that infrastructure remains operational, supporting the sustained functionality of Defense Forces assets. The command assumes control over the intricate web of electrical, thermal, water supply, sewage, natural gas, and other engineering networks within ministry facilities. This encompasses not only monitoring but also meticulous accounting for utility expenses, ensuring efficient resource utilization.

In line with its comprehensive infrastructure-related role, the command spearheads construction, repair, and emergency work on relevant objects falling within the ambit of the ministry's competence. This proactive approach contributes to the ongoing enhancement of infrastructure capabilities. The command extends its influence into design and construction activities within the Ministry system. This holistic involvement reinforces its commitment to shaping and evolving the infrastructure landscape to meet evolving needs.
As the custodian of Defense Forces infrastructure, the command takes charge of ensuring smooth relations pertaining to the registration of real estate. This involves navigating legal and administrative intricacies to uphold the integrity of property records (MOD 2014).

These tasks collectively underscore the command's pivotal and multifaceted role in steering infrastructure-related aspects. By emphasizing the efficient logistics and management of property, the Command for Logistics Support of the Troops fortifies the operational readiness and capabilities of the Defense Forces. It stands as a testament to the critical nexus between effective infrastructure management and the overarching success of defense operations.

3. Identification of Key Areas for Improvement in Georgia's Defense Infrastructure Organizational Model

Georgia's defense infrastructure plays a critical role in fortifying the country's security and operational efficiency. To enhance its capabilities, it is crucial to analyze successful defense infrastructure models globally and identify key areas for improvement. Drawing insights from the comparative analysis of the United Kingdom, France, Germany, Australia, and Latvia, Georgia can develop a nuanced strategy tailored to its specific needs.

Here are recommendations and key areas for improvement:
Recommendation 1 – Establish a Dedicated Defense Infrastructure Organization as a Centralized Unit with Regional Adaptations:
Georgia can consider centralizing its defense infrastructure management, following

the UK's centralized model. This promotes streamlined coordination and efficient resource allocation. It is advisable to detach the infrastructure function from the Command for Logistics Support of the Troops and establish a separate Defense Infrastructure Organization (DIO), considering creating a legal entity of public law for this purpose.

The DIO would specifically focus on undertaking infrastructure-related functions currently provided by the Command for Logistics Support of the Troops, including design and construction activities, registration of real estate, forming infrastructure requirements, managing and maintaining real estate, providing communal and household conditions, offering bath-laundry services, and overseeing engineering networks and utility costs. Addressing the identified shortcoming of lacking a dedicated structural unit for infrastructure development, the establishment of the DIO aligns with international best practices, as highlighted by the comparative analysis. The DIO would have a comprehensive mandate, planning and conducting day-to-day infrastructure-related activities and supporting the Defense Forces throughout the lifecycle of infrastructure projects, from acquisition to disposal.

While the Department of Defense Sustainability focuses on policy development and monitoring, the DIO would complement these efforts by executing operational tasks, and conducting day-to-day infrastructure-related activities to support the Defense Forces "by enabling military capability through planning, building, maintaining and servicing infrastructure over the lifecycle of acquire, operate, maintain and dispose of," (MOD UK 2020, 36) thereby ensuring a more efficient and streamlined approach to defense infrastructure. The DIO will be entrusted with *managing the infrastructure program budget, with its Head serving as the program manager.*

It is worth mentioning that the lack of a specific department tasked with overseeing infrastructure development and conducting day-to-day infrastructure-related activities within the Ministry of Defense was identified as a deficiency in the findings of the State Audit Office's assessment of real estate management effectiveness in 2019 (SAO 2019). While the Department of Infrastructure Management, Standardization, and Codification was founded in 2021 (later renamed as the Department of Defense Sustainability), its responsibilities, as mentioned earlier, focus on formulating policy for Ministry infrastructure system development and overseeing its execution, rather than directly managing day-to-day infrastructure-related tasks (MOD 2021b).

The Department of Defense Sustainability, particularly its infrastructure management division, will assess the requirements of the Georgian Defense Forces (GDF) and develop or review policies for infrastructure system development in alignment with the overall Ministry of Defense policy. Moreover, it will actively supervise the implementation of these policies. Through coordinating the development of the infrastructure program budget, the division will ensure that the allocated resources align with the strategic objectives of infrastructure improvement.

As for the Command for Logistics Support of the Troops, it will concentrate on delivering logistical support to Defense Forces units during peacetime and wartime. It will serve as the primary operational unit for the logistical function, aiming to centralize the administration of limited resources and guarantee their distribution to tasks of utmost importance.

By establishing a dedicated Defense Infrastructure Organization, Georgia can enhance its infrastructure management capabilities, align with international models, and address the identified shortcomings in the current organizational structure. This separation of functions allows for a more specialized and effective approach to infrastructure planning, development, and maintenance within the Ministry of Defense (Okromtchedlishvili 2022).

It is recommended to establish the Defense Infrastructure Organization (DIO) as a centralized unit operating under the legal framework of a public law entity within the Ministry of Defense. Drawing inspiration from the United Kingdom's successful DIO, this centralized structure will streamline operations and ensure cohesive management of defense infrastructure projects.

Furthermore, it is advisable to incorporate regional adaptations inspired by France's decentralized model. By decentralizing certain functions or establishing regional branches, Georgia can better address localized needs and ensure the efficient allocation of resources across diverse geographical areas. This hybrid approach, combining the centralized framework of the UK's DIO with the regional flexibility of France's model, will allow for greater responsiveness to both national and regional defense infrastructure requirements.

Responsibilities and functions of the DIO will include:

- *Planning and Delivery:* Planning and executing major capital projects and lifecycle refurbishment initiatives to ensure the ongoing effectiveness and resilience of defense infrastructure.
- *Utilities Services:* Providing utilities services to support various defense activities, ensuring the availability of essential resources for defense personnel.
- *Soft Facilities Management:* Managing soft facilities management aspects, such as cleaning and catering services, contributing to the overall well-being and efficiency of defense personnel.
- *Safe Training Environments:* Providing a safe place for defense personnel to train, emphasizing the importance of secure and effective training environments.
- *Service Families Accommodation:* Allocating Service Families Accommodation, recognizing the significance of providing suitable housing for military families.
- *Routine Maintenance and Reactive Repair:* Procuring and managing routine maintenance and reactive repair services to ensure the ongoing functionality and security of defense infrastructure.

● *Asset Information Management:* Maintaining a central register of asset information, contributing to effective infrastructure planning and decision-making.
● *Stewardship of the Defense Estate:* Acting as the steward of the defense estate, overseeing and safeguarding the various elements of defense infrastructure.
● *Unarmed Guarding Service and Security Systems:* Providing both physical and electronic security systems, emphasizing the importance of protecting defense assets.

By implementing this organizational structure and delineating clear responsibilities and competencies, Georgia can enhance its defense infrastructure management capabilities, ensuring a more streamlined and efficient approach to infrastructure planning, development, and maintenance within the Ministry of Defense. Additionally, incorporating regional adaptations will allow for a tailored approach to address diverse defense infrastructure needs across different regions of the country. Establishing regional centers or directorates of the DIO would address local nuances, ensuring a more tailored approach to diverse defense infrastructure needs.

Recommendation 2 – Adopt a Comprehensive Approach with Emphasis on Sustainability, Digital Systems and Technical Expertise:
Georgia can adopt a comprehensive approach similar to the United Kingdom, covering major projects, soft facilities management, and strategic planning. The state should prioritize modernization efforts akin to the United Kingdom, emphasizing digital systems, informed asset management, and resilience against evolving threats. This ensures a holistic defense infrastructure strategy.

Emphasizing sustainability in line with France's model can prepare Georgia for long-term effectiveness and resilience in the face of environmental and geopolitical challenges. Incorporating France's focus on technical expertise will build a skilled workforce capable of managing complex defense projects, enhancing overall effectiveness.

Recommendation 3 – Actively Participate in Internal and External Operations and International Initiatives:
Following Australia's example, Georgia can explore active participation in international initiatives, strengthening capabilities and fostering diplomatic ties.
Learning from France's active engagement in external operations, Georgia can assess the potential benefits of international collaborations. Establishing capabilities to support operations abroad could enhance Georgia's strategic influence and contribute to global security efforts.
Georgia may explore collaboration with businesses and local economic development initiatives, similar to Germany. This approach not only strengthens defense capabilities but also fosters economic growth, creating a symbiotic relationship between defense infrastructure needs and local businesses.
Georgia can learn valuable lessons from Latvia's expertise in obtaining international financial assistance for the development of defense infrastructure.

Recommendation 4 – Ensure Integration of Efforts for Synergistic Effect:
Ensure seamless coordination between the Department of Defense Sustainability, the J-4 Logistics Planning Department, and the Defense Infrastructure Organization (if established), creating a collaborative environment for strategic planning and implementation.
Within the Department of Defense Sustainability, enhance collaboration between the infrastructure management division, standardization management division, and codification section to ensure efficient cataloging and management of infrastructure elements.

Conclusion

In conclusion, this in-depth exploration of defense infrastructure organizational models, both on a global scale and within the specific context of Georgia, yields valuable insights for strengthening the country's operational efficiency and effectiveness in defense infrastructure management.
The comparative study of defense infrastructure organizations in the United Kingdom, France, Germany, Australia, and Latvia presents a diverse array of strategies and structures that can be tailored to meet Georgia's distinct requirements. The establishment of a dedicated Defense Infrastructure Organization, active engagement in external operations, adoption of a comprehensive approach, emphasis on sustainability, and strategic modernization efforts collectively lay a robust foundation for enhancing Georgia's defense infrastructure.

In synthesizing insights from the United Kingdom, France, Germany, Australia, and Latvia, Georgia can craft a nuanced strategy for enhancing its defense infrastructure capabilities. A centralized yet adaptable organizational structure, a focus on sustainability, active participation in international collaborations, and an emphasis on ongoing modernization and strategic planning are key takeaways. By leveraging these insights and aligning defense infrastructure organization with international best practices, Georgia can fortify its defense infrastructure to effectively address contemporary security challenges and contribute to regional and global stability.
As Georgia navigates the complexities of the future security landscape, the opportunity arises to craft a nuanced strategy, drawing inspiration from international best practices while considering its unique context. Through these concerted efforts, Georgia can propel its defense infrastructure toward resilience, adaptability, and effectiveness in safeguarding the nation's interests.

Disclaimer
The views represented in this paper are those of the author and do not reflect either the official policy or the position of the Ministry of Defense of Georgia.
Conflict of Interest Statement
The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Australian Government (AGa). n.d. "The Infrastructure Division of the Security and Estate Group of the Department of Defense." Accessed February 12, 2024. https://www.directory.gov.au/portfolios/defence/department-defence/associate-secretary/security-and-estate-group/infrastructure-division

Australian Government (AGb). n.d. "Infrastructure projects." Accessed February 12, 2024. https://www.defence.gov.au/about/locations-property/infrastructure-projects

Bundeswehr. n.d. "Infrastructure, Environmental Protection and Services." Accessed February 10, 2024. https://www.bundeswehr.de/en/organization/infrastructure-environmental-protection-and-services

Defense Infrastructure Organization (DIO). 2017. "A quick guide to DIO." https://assets.publishing.service.gov.uk/media/5a82e84d40f0b6230269d533/DIO_Quick_Guide_vFINAL6.pdf

GOV UK. n.d. "Defense Infrastructure Organization (DIO)." Accessed January 10, 2024. https://www.gov.uk/government/organisations/defence-infrastructure-organisation/about

GOV UK. 2020. "Defense Infrastructure Organization (DIO) Strategy 2020 to 2030." https://assets.publishing.service.gov.uk/media/5f1e9536e90e0745691135e5/1_2_150083_DIO_Strategy_TL-Report_2020-2030_Email.pdf

Inside DIO Blog. 2022. "The next step on our journey to transform accommodation services for Armed Forces families." https://insidedio.blog.gov.uk/2022/04/04/the-next-step-on-our-journey-to-transform-accommodation-services-for-armed-forces-families/

Ministry of the Armed Forces (MOAF). n.d. "Defense Infrastructure Service." Accessed February 5, 2024. https://www.defense.gouv.fr/sga/nous-connaitre/organisation-du-sga/directions/service-dinfrastructure-defense

Minister of Defense of Georgia (MOD). 2014. "On approval of the regulations of the Command for Logistics Support of the Troops of the Ministry of Defense of Georgia." *Order №44.* https://mod.gov.ge/uploads/public/normatiuli_aqtebi/44_1.pdf

__. 2021a. "On approval of the regulations of the General Staff of the Defense Forces of the Ministry of Defense of Georgia." *Order №17.* https://www.matsne.gov.ge/ka/document/view/5143035?publication=0

__. 2021b. "On Approval of the Statute of the Infrastructure Management, Standardization and Codification Department of the Ministry of Defense of Georgia." *Order No. 23.* https://matsne.gov.ge/document/view/5151538?publication=0

__. 2022. "On approval of the regulations of the Department of Defense Sustainability of the Ministry of Defense of Georgia." *Order №73.* https://www.matsne.gov.ge/ka/document/view/5598438?publication=0

Ministry of Defense of the UK (MOD UK). 2020. "How Defense Works." Version 6.0. https://assets.publishing.service.gov.uk/media/5f6a2232e90e073fd9f7f466/20200922-How_Defence_Works_V6.0_Sep_2020.pdf

Ministry of Defense of Latvia (MOD of Latvia). n.d. "Military infrastructure development." Accessed February 15, 2024. https://www.mod.gov.lv/en/node/278/military-infrastructure-development

Okromtchedlishvili, Ivan. 2022. "Performance-based budgeting in the defense sector: organizational structure issues." *Journal of Defense Resources Management* 13:2(25):5-24. http://www.jodrm.eu/issues/Volume13_issue2/01%20-%20Okromtchedlishvili.pdf

State Audit Office of Georgia (SAO). 2019. "On the results of the Audit of the effectiveness of real estate management of the Ministry of Defense of Georgia." *Report no. 36/36.* https://sao.ge/files/auditi/auditis-angarishebi/2019/konebis%20martva_NEW.PDF

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

The power of intuition in decision-making under operational stress

Lieutenant-colonel Cătălin-Constantin CĂLIN*

*The National Military Center for Psychology and Behavioral Health, Bucharest
e-mail: catalin.calin.ctin@gmail.com

Abstract

The decision-making process represents one of the most interesting subjects in the field of cognitive sciences, as it is a concept that requires a complex multi- and interdisciplinary approach. Modern warfare involves operations in environments characterized by a high degree of uncertainty, presenting multiple challenges, and radical and unexpected changes in the situation, which require a sound knowledge of how human thinking works and how we can develop the cognitive processes involved in formulating a decision. The article proposes a brief analysis of the decision-making process by military leaders in situations that involve significant stressors and demand quick and intuitive decisions. For this purpose, the main theoretical and practical aspects discussed in the specialized literature are presented, with an emphasis on applications in the military field. Additionally, the concept of expert intuition is introduced. Although there have been attempts to study this concept since antiquity, the systematic study of this revolutionary concept began in the middle of the 20th century and continues to arouse lively interest even today, remaining the subject of lively academic disputes.

Keywords:

decision-making process; expert intuition; stress; bias; heuristic; natural decision-making process.

Article info
Received: 27 April 2024; Revised: 23 May 2024; Accepted: 4 June 2024; Available online: 5 July 2024

Citation: Călin, C.C. 2024. "The power of intuition in decision-making under operational stress". *Bulletin of "Carol I" National Defence University*, 13(2): 79-97. https://doi.org/10.53477/2284-9378-24-21

1. Introduction

1.1 Intuition

Our entire existence can be described as a continuous decision-making process. At every point in our lives, we are forced to make decisions, from the simple ones, such as deciding at what time to go to work, to complex, high-stakes personal or professional decisions that can change the trajectory of our own lives or the lives of others. In these circumstances, several very legitimate philosophical questions arise. How rational/irrational are our decisions? Does genetics push us towards a certain kind of decision? Can experience and/or knowledge help us make better decisions when we are under pressure from strong stressors? Thinkers such as Aristotle, Plato, Leibniz, Kant, and Hegel are just some of the great minds of humanity who have provided answers to these questions through works of inestimable value (Waxman 2019). However, the exploration of the decision-making process, in the form in which it is currently studied, begins with the volumes A Treatise of Human Nature (1739-1740) and The Dissertation on the Passions (1757) by the Scottish philosopher David Hume.

According to the American Psychological Association Dictionary (APA 2024a), decision-making is defined as the cognitive process of choosing between two or more alternatives. We therefore note that this process involves three essential elements: (1) the existence of a goal, (2) the possibility of choosing between several alternatives for achieving the goal, and (3) the cognitive process by which the options for achieving the proposed goal are analyzed.
Cognitive science research has shown that this process can be carried out both consciously, intentionally, voluntarily, and automatically. Daniel Kahneman (2011), in his famous book Thinking, Fast and Slow, describes two different ways of thinking: intuitive and analytical. Thus, according to the author, System 1 is intuitive and emotional, representing fast and automatic thinking, while System 2 is analytical and logical, representing slow thinking and conscious and voluntary mental effort in deliberating between several options.

System 1 is described as automatic, occurring with little effort and in the absence of conscious control. It is a way of thinking that allows the manifestation of acquired skills and the performance of several tasks at the same time. It is largely based on previous experience gained as a result of learning, practice, or familiarity. The main advantages of this type of thinking are that it unfolds quickly because it involves a reduction in the complexity of the situation or a generalization of circumstances, and it is not too energy-intensive.

In contrast, System 2, the analytical system, is often associated with the subjective experience of concentration and free will. This system requires considerable energy consumption to allocate and maintain attentional resources to ongoing mental activities and to access working memory. It is also the mode that is activated in

new situations, in which System 1 cannot recognize patterns or generalize, and in situations that do not comply with rules.
System 2 - slow thinking plays an important role in self-control situations by providing the necessary arguments for emotional and behavioral self-regulation to resist temptation (e.g., I do not want to start smoking again because it is bad for my health, and I need to save money). The benefits of System 2 are numerous, among the most important being that by analyzing as much information as possible, the risk of error is reduced, and the chances of making the most appropriate decision automatically increase.
It is important to emphasize that between the two systems of thought, there is a continuous dynamic; they interact, thus making the decision more effective (Peters *et al.* 2006). Both types of thinking are sensitive to internal and external factors, with the possibility of errors.

Thus, if System 1 can generate rapid responses, particularly based on similar experiences, these reasonings are highly context-dependent. At the same time, System 2, which is analytical, can be hijacked by errors inserted from the interaction with System 1, but also by other causes (for example, errors of perception, emotional states, etc.).
Intuition is a non-sequential way of processing information, which includes both cognitive and affective elements and results in direct knowledge without any use of conscious reasoning (Sinclair *et al.* 2002), and is, therefore, one of the core elements of the decision-making process, broadly identifying with System 1.

1.2. The Impact of Stress on the Decision-Making Process
Probably one of the most widely used concepts is stress. Borrowed from physics, the concept was introduced into the academic circuit by the Canadian physician Hans Selye in 1937. Stress has been defined as the physiological or psychological response to an internal or external stressor that interferes with the normal functioning of the individual. Over time, the concept has been refined, and new meanings and elements have been added. Currently, the most widely used theoretical model is that of cognitive appraisal of stress, proposed by Lazarus and Folkman (1984), in which stress is the result of a process of cognitive appraisal of the stimuli to which the individual is exposed.

Cognitive appraisal can be conscious and deliberate or automatic. This triggers the emergence of responses that may be cognitive, emotional, behavioral, or physiological. This process has two phases: the primary appraisal, which consists of assigning meaning and significance to the stimulus—in the case of stress, being negative (threatening)—and the secondary appraisal, which refers to the existence and identification of the resources necessary to cope with the pressure of the problematic stimulus. Secondary appraisal plays an important role in the emotional response of the individual and, implicitly, in the physiological response, with implications for the anticipation of the ability to cope (Lazarus 1993).

Many authors have noted that the cognitive appraisal theory of stress includes several elements presented in the model by Kahneman (2011), stress being the result of information processing by one of the two systems, particularly System 1, when it comes to stressors with adaptive value (situations characterized by uncertainty, time pressure, or in which life or physical and psychological integrity is endangered, etc.) (Yu 2016).

For example, when the stressor is a venomous snake, System 1 automatically kicks in, resulting in avoidance behavior and fear. In the case of a herpetologist, they know through learning and practice that a reptile is only aggressive under certain conditions, resulting in behavior appropriate to the situation and the absence of dysfunctional emotion. From an evolutionary point of view, System 1 is older on the phylogenetic and ontogenetic evolutionary scale, while System 2 is more recent, being the result of the development of the prefrontal lobe (Evans 2003).

System 1 is much more vulnerable to stressors than System 2, which has self-regulating mechanisms. Thus, from an evolutionary perspective, automatic and intuitive thinking is superior to analytical thinking in situations where we are faced with stressors of adaptive value (Da Silva 2023). An important evolutionary advantage is given by the situation where System 1 has acquired new tools through learning and practice, in some situations becoming highly specialized, expert.

1.3. Expert Intuition

Intuition is the ability to act or decide correctly without deliberately and consciously choosing between alternatives, following a particular rule or routine, and possibly automatically (Hogarth 2001; Kahneman & Klein 2009; Harteis & Billett 2013). Numerous situations have been documented where spur-of-the-moment decisions have averted air disasters, fire casualties, or saved lives in emergency rooms. Klein et al. (2010) note that it takes 23 years of experience for a firefighter to make such decisions; in the case of medical personnel or military aviation, this complies with the rule of over 10,000 hours, depending on the particularities of the situations (Nalliah 2016).

Regarding the study of intuition, particularly expert intuition, there are two major strands of research in the academic world. One that is based on the theoretical model of the decision-making process as a natural process - *Naturalistic Decision Making (NDM)* - whose exponent is the American psychologist, Gary Klein. The other is the heuristic and bias model (HB), promoted by the Israeli Nobel Prize laureate Daniel Kahneman (1934-2024). One of the finest examples of collaboration between the two authors, despite their different theoretical positions, is the joint article published in 2009 in American Psychologist, "*Conditions for Intuitive Expertise: A Failure to Disagree*".

1.3.1. Naturalistic Decision Making (NDM)

Since the first scientific approaches in the middle of the 20th century, initiated by the Dutch scientist Adrianus Dingeman (Adriaan) De Groot, the subject of

expert intuition has generated special interest in the scientific world. In the article Thought and Choice in Chess, De Groot (1965) shows that chess grandmasters can identify the best move accurately, quickly, and without any special voluntary effort, while mediocre players only occasionally succeed. Over the next decade, research was continued by other scientists. Chase and Simon (1973) discovered that high-performing chess players can easily recognize patterns on the chessboard in a short time. The authors note that their performance is the result of approximately 50,000 to 100,000 hours of practice.

This research represents a milestone in the study of expert intuition from the perspective of this paradigm. As a working definition, intuition is a process of recognizing patterns that are stored in long-term memory (Gobet and Herbert 1996). In specialized literature, several theoretical models are identified in the NDM paradigm (Lipshitz 1993). The most significant ones will be briefly described below.

1.3.1.1. Recognition Primed Decision (RPD)

Klein et al. conducted a study in 1986 on how firefighters make decisions. Following this approach, they concluded that firefighters make decisions automatically, without comparing several possibilities, calling this cognitive strategy recognition-primed decision. It soon became one of the core elements of Klein's subsequent research. Similar research has been carried out in other areas of activity such as the military, medicine, management, etc. A tragic event took place in 1988 (see Ch. 2), as a result of which the US Army financed research in the field, in which a significant number of specialists participated, and new information was brought about decision-making and the validity of this construct.

This model is based on two central cognitive processes: the assessment of the situation and its mental simulation. The two processes run quickly and complement/correct each other. The assessment of the situation consists of four stages: setting achievable goals that are consistent with the situation, selecting highly relevant information in the given context, formulating realistic expectations with a regulatory role, and identifying the optimal course of action. Mental simulation is an analysis of courses and chances of success (Klein 2015).

The RPD model differs from classic models of decision-making. Thus, the core elements in this model focus on leveraging previous experience in new similar situations, emphasizing the evaluation of circumstances, the need for action prevailing, the person focusing on a serial evaluation to save time, and aiming to maximize the chosen course of action rather than analyzing the strengths and weaknesses of different options. Klein also mentions that there are issues needing further research, such as situations involving mixed decisions (both analytical and intuitive), time constraints, high stress, or task type (perceptual or abstract).

1.3.1.2. Cognitive Continuum Model

The cognitive continuum model is inspired by medical practice and presents the decision-making process according to both the type of thinking (intuitive to analytical)

and the type of task (low structured to highly structured). Although not all 6 modes are very clearly defined, for mode 1 (intuition), mode 4 (quasi-experiencer), and mode 6 (analytical), we find detailed descriptions. Mode 1 (intuitive and low structured task) is fast and automatic, while in mode 4 both intuitive and analytical elements are equally present. Mode 6 (analytical thinking, structured task) is slow, conscious, and consistent (Hamm 1988). Hammond (1988) details the analytic mode as characterized by high cognitive and conscious control, low information processing speed, and a well-defined method, while the intuitive mode is the opposite: low cognitive control, unconscious, high processing speed, and the absence of a method. Research carried out in the medical field has demonstrated its validity, having the advantage that it can also provide data in cases of interdisciplinary decisions or involving the participation of several people (Cader, Campbell and Watson 2005).

1.3.1.3. The Search for Dominance Structure Model

The dominance structure theoretical model by Montgomery (1983) describes the stages of the cognitive decision-making process, from this point of view being quite similar to the model proposed by Klein. In this theoretical model, the cognitive process essentially consists of defining a dominance structure, with some sets of defining attributes dominant over the others. The process involves going through four distinct stages: pre-editing, finding a promising alternative, dominance testing, and dominance structuring (Montgomery 2012).

Pre-editing is the first phase of the process and involves simplifying the problem by choosing those attributes and alternatives that can have an impact on the decision. The second stage of the process is identifying a promising alternative. In this stage, the choice of one of the alternatives takes place, based on a specific attribute, forming a preference for it. In the penultimate stage, the test of dominance takes place, the test of choice. If the choice turns out to be valid, the process ends; if it does not turn out to be the best option, the dominance structuring stage follows. In this phase, the identified neutralization or counterbalancing is attempted. In case of success, the decision is made; otherwise, the continuation of the process is analyzed by resuming the stages starting with step 2, or it is abandoned.

Another important element of this theory is represented by the decision rules. According to Montgomery (1983), all rules assume that a decision situation consists of several choice alternatives that can be described in terms of subjectively defined dimensions or attributes. The model is not without criticism for the fact that it reduces the decision-making process to a choice between several options, the choice being equivalent to the resolution of a conflict, and that the whole process is reduced to mental structures and processes (Klein 1993).

1.4. Cognitive Biases and Heuristics

Another scientific perspective present in the study of the decision-making process involves theoretical models that focus on important elements of any cognitive

approach: bias and heuristics. As this is an extremely broad field and known both to the academic environment and to the general public, I will only give a brief introduction to the two concepts below.

In the APA online dictionary (APA 2024b), heuristics are defined as cognition, an experience-based strategy for solving a problem or making a decision that often provides an effective means of finding an answer but cannot guarantee a correct outcome. In contrast, an algorithm guarantees a solution but can be much less efficient. By algorithm, we mean a well-defined procedure or set of rules used to solve a problem, make a decision, or perform a task. The two concepts have a common point (making a decision/solving a problem), but they differ in that, in the case of the algorithm, the stages are very well defined, and the result is guaranteed.

With the cognitive revolution of the 1950s, the first systematic approaches to the study of thinking and the mental processes involved in problem-solving emerged (Miller 2003). In the early 1970s, however, Kahneman and Tversky published a series of scientific papers describing and analyzing heuristic processes and the factors that influence them when errors occur. In their famous article "Judgment under Uncertainty: Heuristics and Biases," published in 1974, the authors identify three major heuristic strategies: (1) representativeness; (2) availability; and (3) adjustment and anchoring.

Representativeness refers to the extent to which a cognitive processing outcome reflects the features of the event that generated it and is similar to the category to which it belongs. The two researchers highlight several factors related to representativeness: insensitivity to prior probabilities; insensitivity to sample size; misperception of probability; insensitivity to predictability; illusion of validity; and misunderstanding of regression.

Availability is a type of heuristic in which a person evaluates the frequency of classes, or the probability of events based on their accessibility, i.e., the ease with which instances or occurrences can be brought to mind (Kahneman 2011). Although useful in assessing frequency or probability, it can be influenced by factors such as the person's recall/familiarity with the class of objects/phenomena they are interacting with, search efficiency, imaginative ability, and illusory correlation.

Adjustment and anchoring are the processes by which, starting from an initial value (anchor), a final result is reached through successive changes. The initial value or starting point may be given by the problem formulation or maybe the result of a partial calculation. The two authors note that there are situations in which errors may occur, including inadequate adaptation, errors in the evaluation of conjunctive and disjunctive events, and errors in the evaluation of subjective distributions.
Based on these three heuristics, others have subsequently been identified, which represent particular situations of those described: simulation (Kahneman and

Tversky 1981), familiarity (Park and Parker 1981), peak-end rule (Kahneman and Tversky 1981), etc.

Heuristics can be influenced by several factors, thus producing dysfunctions. Kahneman and Tversky (1981) refer to these errors as cognitive biases, which they define as systematic and unconscious errors in thinking that occur when people process and interpret information in the environment, influencing decisions and judgments. They distort individual perceptions and produce rationally limited (Kahneman 2011) or irrational decisions (Garety *et al.* 2007). Other authors define biases as situations where the cognitive system produces systematically distorted representations in relation to a criterion (accuracy, logic, quality, speed of processing, etc.) (Haselton, Nettle and Murray 2016).

In addition, we find in the literature several lines of research on biases: heuristic biases, as artifacts (errors resulting from the architecture of our cognitive system) (Gigerenzer and Sedlmeier 1997), and biases of management errors (referring to the fact that some biases have evolved into cognitive strategies in situations where the cost of error is not constant) (Haselton and Buss 2000). Currently, a set of 24 basic cognitive biases has been quantified, each with subcategories, totaling approximately 180.

1.4. NDM Model versus HB Model

Both theoretical models have undeniable value in the cognitive sciences. However, they have both strengths and directions that require further study. The NDM model aims to investigate the decision-making process under natural conditions characterized by complexity and pressure, where experience is important. At the same time, it is sensitive to the multitude of variables that may be present in the environment. While for fields such as firefighting, medicine, the military, aviation, or chess, which are considered high-validity environments, the model is functional, in others such as intelligence analysis or politics, the data is inconclusive (Kahneman and Klein 2009).

The HB Model, whose data were obtained particularly from controlled environments where the variables studied were isolated, provides clear information on how heuristic processes work and their biases. The authors agree that expert intuition is predominantly the result of the operation of System 1 and less of System 2. Proponents of the NDM have focused their efforts on how intuitive judgments arise and what conditions must be met, while those of the heuristic approach focus on the outcomes that arise from simplifying heuristics, rather than from accumulating expertise, and which are less accurate and prone to bias.

Research in cognitive sciences and other fields with a central interest in how we make decisions or solve problems has focused on the applied side over the last three decades. The revolution in algorithms in the early 1990s (Gonzales 2024) has continued with the use of breakthroughs in artificial intelligence (machine

learning, natural language processing, decomposition of problems, or optimization of algorithms) (Hjeij and Vilks 2023).

2. Expert Intuition and Military Decision-Making

Advances in the field of cognitive science have also influenced the approach to the military environment when it comes to decision-making, especially when it involves decisions under the pressure of hard-to-quantify consequences. The military organization's interest in decision-making research is growing as a result of events in the late 1980s and early 1990s.

One example where an officer's intuition made a difference is that of the British destroyer HMS Gloucester during the Gulf War (1991). During a routine mission to support US warships, the ship's radar intercepted a signal that appeared to be from an American aircraft. In the few dozen seconds available, the British officer decided to fire the target, which turned out to be an Iraqi Silkworm missile (Pokrant 1999). In his book Source of Power, Klein (2017) recounts the dialogue with Lieutenant Commander Michael Riley about this event. The officer recounted that in the 90 seconds he had, he watched the radar carefully for 40 seconds, and what he observed confirmed his intuition from the very first moment he saw the target on the radar. Although several factors were taken into account, altitude was the decisive key. The officer knew that missiles fly at a low altitude of 1,000 feet, whereas an airplane flies at 2,000-3,000 feet.

A less fortunate event occurred in 1988 when the US battleship USS Vincennes in the Persian Gulf shot down an Iranian Airbus airliner by a serious mistake. More than 290 people lost their lives as a result of this incident (Friedman 1989). The battleship had been involved in another incident shortly before, this time with a happy ending. In this case, two Iranian F-4 fighter jets had taken action against the US Navy. The commander putting himself in the role of the Iranian pilots, sensed that the way in which the two planes had acted was not that of an attack and used electronic warfare means to remove them.

But things did not go so well on July 3, when the USS Vincennes shot down Iran Air flight 655. The ship was engaged in executing naval missions in the area when a signal resembling an Iranian Air Force F-14 aircraft appeared on its radar. Unfortunately, it was a civilian flight with passengers on board. After repeated attempts to contact the aircraft, 3 minutes and 9 seconds after the radar signal appeared, the Iranian flight was shot down. In this case, as well, the commander used the same cognitive strategy (role-playing), by engaging in mental simulation (Klein 2017). This time there were also several factors out of the commander's control (received information, confusion over the use of the identification system, and the AEGIS system), all compounded by the stress and pressure of making a decision, which ultimately led to this tragedy. Following this event, a committee of inquiry headed by Admiral William M.

Fogarty (1988) was set up. As a recommendation, the US Army started a research program for the study of the decision called *The Tactical Decision Making Under Stress (TADMUS),* which has been running for a long period (since 1999). The main objective was to identify methods and techniques for tactical decisions in conflict situations. These were operationalized in several research directions: define and measure; stress effects; development of the support tools; development of the principles for training and simulation; improving human-machine interface as well as integrated training (Riffenburgh 1991). The TADMUS program represented an important progress in military decision-making process studies. For example, *The Decision-Making Evaluation Facility for Tactical Teams* - a portable testing system for team tactical decision-making assessment (Hutchins and Duffy 1993) and The Heuristics 5 Steps Method (Cohen *et al.* 1998) were implemented.

Interest in decision-making existed even before the USS Vincennes incident. Kahneman and Tversky studied the implications of biases and heuristics in the military field, with some of their conclusions being published in *Science* in 1974 (Mustață and Bogzeanu 2017). However, improving decision-making in a military organizational context is an ongoing concern, and new studies appear periodically. One such work is Cognitive Biases in Military Decision Making by American officer Michael Janssen (2007). It formulates five recommendations for avoiding cognitive biases that can influence the stages of the military decision-making process (receiving the mission, analyzing the mission, developing, analyzing, comparing, and approving courses of action, as well as issuing action orders): (1) research on biases that may influence the decision, (2) continuous training, (3) updating procedures and introducing new methods to avoid errors (for example, having a sparring partner for the commander), (4) realistic training and rapid feedback, and (5) organizational policies. Similar studies emphasizing the importance of intuitive decisions have also been conducted by other authors in other militaries (Knighton 2004; Jing Kai 2016).

At the beginning of the 2000s, the concept of fast and frugal heuristics was introduced. This designates a type of heuristic characterized by low informational processing, lack of information, and time pressure (Gigerenzer and Goldstein 1996). This concept is quite similar to expert intuition, the difference being the degree of expertise. Banks *et al.* (2022) conducted research involving platoon commanders and military cadets in the British Army. The main goal was to optimize the decision-making process. The authors conclude that the development of this type of heuristic can help the emergence of expert intuition and can support less experienced personnel.

3. The Relationship Between Operational Stress and Expert Intuition

Operational stress is a newly introduced concept in military psychology. It is defined as *changes in physical functioning, cognitive performance, or the appearance of*

maladaptive behaviors resulting from direct or indirect participation in land, naval, or air military operations, during peacetime, or wartime (US Marine Corps, 2010, 1-3). Numerous operational stressors have been analyzed in the specialized literature. Van den Berge et al. (2014) describe three major categories of operational stressors: performance (time pressure, quality, innovation, etc.), organizational climate, and characteristics of the operational environment (meteorological factors, lack of sleep, privacy, hygiene conditions, etc.).

In a research paper involving military radar operators, Jue Qu et al. (2022) analyzed the relationship between operational stress and decision-making. They conclude that the expert group performed superiorly when the number of targets increased. The military was able to quickly combine the information and extract the relevant ones, which confirms the validity of the model proposed by Klein (2017). It should be noted that the authors emphasize the importance of an intuitive design of the radar interface, which is a mediating factor.

Organizational climate plays an important role in how we think, act, or behave, influencing decision-making. Klein (2007) proposes a method of risk analysis that he calls *Premortem*, in which we can use the expert intuition of team members, to mitigate the effects of operational stress. Briefly, this consists of going through five steps: preparation, failure image, failure cause generation, list consolidation, and risk prioritization to analyze courses of action. The method has been successfully used by the NATO armed forces (NATO 2017).
Lack of sleep, temperature, or physical exhaustion negatively influences information processing by reducing executive functions, making it difficult to access memory, or causing emotional hyperactivation (Petrofsky, et al. 2021). It should be noted that the use of psychoactive substances to replace lack of sleep did not reduce risk behaviors, impulsive actions, or erroneous decisions (Mantua, et al. 2021).

Expert intuition is an important component of resilience in terms of maladaptive emotional or behavioral responses to operational stress. Expertise influences reappraisal and suppression, cognitive mechanisms involved in emotional and behavioral regulation (Radtke, et al. 2020). In other words, the fact that experts make fast, automatic, and correct decisions when faced with an extreme situation in the operational environment does not lead to the emergence of counterproductive responses (Lyneham, Parkinson and Denholm 2008). Bonanno (2005) notes that experts possess a high level of resilience, reasoning that a prerequisite of expertise is the formation and development of adaptive coping mechanisms.

4. Can Expert Intuition Be Educated?

Although it seems like a simple question, the answer is not easy. Based on practice and learning, intuition can be developed, the key being when and how. Regardless

of the psychological approach, learning theories have three common pillars: the prerequisite cognitive structures (attention, memory, etc.), environment, and motivation.

The first condition for intuition is the existence of information from a specific field. In the instinct-intuition dispute, Spelke (1994) argues for the existence of an initial intuition (exemplifying the situation of children of 3-4 months who recognize a stimulus as an object or a being, which involves the rapid analysis of some criteria without voluntary effort), later developing other forms of intuition. Innate (instinctive) reactions are limited in number, important for survival, and do not change significantly throughout life.

Hogarth (2001) notes that the development of intuition is influenced by learning and experiences. He describes two stages: (1) forming mental connections between things that happen together, and (2) strengthening them. Thus, when a soldier studies the weaponry in stock, he learns the parts, features, and how to use them through memorization and interaction. The information is reinforced and new connections are added when the soldier participates in field exercises. Their depth and quality are moderated both by psychological factors (motivation, mood, emotional stability, etc.) and by the frequency of situations that facilitate implicit learning. This type of learning refers to the ability to understand the functioning of phenomena automatically, without being able to verbalize it (Curran and Schacter 2001).

The following factors are important for the development and education of intuition (Hogarth 2001):

- **Creating awareness**, through which the person intentionally exposes themselves to as many learning situations as possible and processes the experience at a conscious level, trying to optimize behaviors. For example, a military person can choose to train for borderline or less likely situations by accessing different forms of training (e.g., a climbing course, even if he/she is a radio operator). Awareness helps avoid bias.
- **The acquisition of new competencies and the development of skills**. In this case, the environment also plays an important role through the implicit learning mechanisms described previously (e.g., an officer from a combat unit carrying out a short internship in a similar function in a support unit).
- **Practice**, which, when it exceeds a certain number of repetitions or a period of time, can lead to expert intuition (e.g., a pilot who repeats the execution of a difficult maneuver through simulation and flight).

Another element that contributes to educating intuition is **continuous feedback** (Kahneman and Klein 2009). In this respect, Klein (2017) recommends the *Premortem Method*, which can also be used to learn new skills and competencies, create a group identity, and foster metacognition.

All organizations are interested in capitalizing on those people who can contribute to making the best decisions. Using the method of cognitive task analysis, Klein (2017) proposes the following steps for harnessing expertise: identification of the source of expertise; evaluation of the quality of expertise; knowledge extraction (methods, techniques, algorithms, or heuristics used by the expert); knowledge systematization (logical schemes, diagrams, simulations); application of knowledge (policies, procedures, regulations).
In conclusion, expert intuition is strongly conditioned by learning and context, which can speed up or slow down its development. There is a rich scientific literature in the field of optimizing learning or facilitating the good functioning of the cognitive processes involved.

Conclusions

Cognitive sciences represent one of the most dynamic fields of human knowledge, being in continuous progress. This article is a brief introduction to what it means to decide in situations characterized by stress, uncertainty, and time pressure, especially from the perspective of intuitive decisions. As we have shown in the case of the USS Vincennes, in such conditions, there is a fine and difficult-to-define line between the right decision and an error.

Does experience matter? The answer is YES, but...
It is obvious that expertise is important, to a greater or lesser extent, depending on the characteristics of the environment (predictable or unpredictable). However, this should not be considered absolute, as it is dependent on perceptual factors and personality. Avoiding perceptual errors requires that the environment, as far as possible, be designed to minimize these limitations or that individuals learn skills for effectively scanning the environment (Graham, Evitts and Thomas-MacLean 2008). Although knowledge transfer can be a good shortcut in terms of time, it cannot replace learning and practice. One line of action is the optimization of learning. One suggestion could be to use simple psychometric tools to determine the optimal number of repetitions or to understand learning styles simultaneously with modeling the environment.

Can we develop or enhance expert intuition? The answer is YES.
First used in cybernetics, ***the nudge*** concept was introduced to the practice of behavioral and cognitive sciences by Thaler and Sunstein (2008), in their book *Nudge: Improving Decisions About Health, Wealth, and Happiness*. With multiple practical applications, a nudge is any element of the architecture of a choice that can predictably change behavior, without forbidding any other option and without a reward. For example, a periodic reminder for a medical visit has contributed to the health of Canadian Army personnel (Sylvester *et al.* 2022). For a nudge intervention to work, it needs to be easy to apply, attractive, timely, and have social support (Mustață and Ionașcu 2018).

We can facilitate the development and enhancement of expert intuition with the help of nudge principles. For example, one such solution is to run training sequences continuously on standby desktops or monitors located in halls or common spaces in units to increase the level of training and ensure rapid assimilation of information. According to studies, the optimal duration of an educational clip is 3-6 minutes (Guo 2013). Another example is the presence of informative materials in relaxation areas (classic relaxation-information conditioning). Additionally, the presence of cognitive anchors, such as photos of different types of IEDs at checkpoints in operation areas, helps quick decisions. Through repeated exposure, they become automatic responses, thus creating a shortcut for the rapid accumulation of information or for updating it, facilitating expert intuition.

The paradigm shift triggered by artificial intelligence will certainly bring new challenges to the study of cognitive decision-making processes. In my opinion, the new challenges for the military organization will come both from the field of moral decisions from the perspective of cyber-ethics and from what it means to use intelligent interfaces and merge the processes of interaction between mental and computer processes.

References

APA (American Psychological Association). 2024a. *APA Dictionary of Psychology - decision making.* https://dictionary.apa.org/decision-making.

—. 2024b. *APA Dictionary of Psychology - heuristic.* https://dictionary.apa.org/heuristic.

Banks, Adrian P., David M. Gamblin and Heather Hutchinson. 2020. "Training Fast and Frugal Heuristics in Military Decision Making." *Applied Cognitive Psychology* 34 (3): 699-709. doi:10.1002/acp.3658.

Bonanno, George. 2005. "Resilience in the Face of Potential Trauma." *Current Directions in Psychological Science* 14 (3): 135-138. https://doi.org/10.1111/j.0963-7214.2005.00347.x.

Cader, Raffik, Steve Campbell and Don Watson. 2005. "Cognitive Continuum Theory in nursing decision-making." *Journal of Advanced Nursing* 49 (4): 397–405. doi:10.1111/j.1365-2648.2004.03303.x.

Calderwood, Roberta, Gary A. Klein and Beth W. Crandall. 1988. "Time Pressure, Skill, and Move Quality in Chess." *The American Journal of Psychology* 101 (4): 481-493. https://doi.org/10.2307/1423226.

Cambridge Dictionary. 2024. *Expertise.* https://dictionary.cambridge.org/dictionary/english/expertise.

Chase, William and Herbert Simon. 1973. "The mind's eye in chess." In *Visual information processing*, by W. G. Chase (Ed.), pp. 215–281. New York: Academic Press.

Cohen, Marvin, Jared Freeman and Bryan Thompson. 1998. *Critical Thinking Skills in Tactical Decision Making: A Model and A Training Strategy.* doi:10.1037/10278-006.

Curran, Tim and Daniel Schacter. 2001. "Implicit Learning and Memory: Psychological and Neural Aspects." *International Encyclopedia of the Social & Behavioral Sciences* 7237-7241. https://doi.org/10.1016/B0-08-043076-7/03513-0.

Da Silva, Sergio. 2023. "System 1 vs. System 2 Thinking." *Psych 2023* 5 (4): 1057-1076. https://doi.org/10.3390/psych5040071.

De Groot, Adrianus Dingeman. 1965. *Thought and Choice in Chess (2nd ed.).* The Hague: Mouton Publishers.

Evans, Jonathan. 2003. "In two minds: dual-process accounts of reasoning." *Trends in Cognitive Sciences* 7 (10): 454–459. doi:10.1016/j.tics.2003.08.012.

Fogarty, William M. 1988. "Formal Investigation into the Circumstances Surrounding the Downing of Iran Air Flight 655 on 3 July 1988." U.S. Navy, unclassified letter. https://en.wikisource.org/wiki/Formal_Investigation_into_the_Circumstances_Surrounding_the_Downing_of_Iran_Air_Flight_655_on_3_July_1988/Internal_Report.

Friedman, Norman. 1989. *The Vincennes Incident.* https://www.usni.org/magazines/proceedings/1989/may/vincennes-incident.

Garety, Philippa A., Paul Bebbington, David Fowler, Daniel Freeman, and Elizabeth Kuipers. 2007. "Implications for neurobiological research of cognitive models of psychosis: a theoretical paper." *Psychol Med* 37 (10): 1377-1391. doi:10.1017/S003329170700013X.

Gigerenzer, Gerd, and Daniel G. Goldstein. 1996. "Reasoning the fast and frugal way: Models of bounded rationality." *Psychological Review* 103 (4): 650–669. doi:10.1037/0033-295x.103.4.650.

Gigerenzer, Gerd, and Peter Sedlmeier. 1997. "Intuitions about sample size: The empirical law of large numbers." *Journal of Behavioral Decision Making* 10 (1): 33–51.

Gigerenzer, Gerd, P. M. Todd, and the ABC Group Research. 1999. *Simple heuristics that make us smart.* New York: Oxford University Press.

Gobet, Fernand, and Simon Herbert. 1996. "Templates in Chess Memory: A Mechanism for Recalling Several Boards." *Cognitive Psychology* 31 (1): 1-40. doi:10.1006/cogp.1996.0011.

Graham, Paul, Trina Evitts, and Roanne Thomas-MacLean. 2008. "Environmental Scans: How useful are they for primary care research?" *Can Fam Physician* 54 (7): 1022–1023. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2464800/.

Guo, P. 2013. Optimal video length for student engagement. https://blog.edx.org/optimal-video-length-student-engagement/.

Hamm, Robert. 1988. "Clinical intuition and clinical analysis expertise and the cognitive continuum." In *Professional Judgement: A Reader in Clinical Decision Making*, by Dowie J. and A. Elstein eds, pp. 78–109. Cambridge: Cambridge University Press.

Hammond, Keneth. 1988. "Judgement and decision making in dynamic tasks." *Information and Decision Technologies* 14: 3–14.

Harteis, Christian, and Stephen Billett. 2013. "Intuitive expertise: Theories and empirical evidence." *Educational Research Review* Vol. 9: pp. 145–157. doi:10.1016/j.edurev.2013.02.001.

Haselton, Martie G. and Daniel M. Buss. 2000. "Error management theory: A new perspective on biases in cross-sex mind reading." *Journal of Personality and Social Psychology* 78 (1): 81–91.

Haselton, Martie G., Daniel Nettle and Damian R. Murray. 2016. "The evolution of cognitive bias." In *The handbook of evolutionary psychology: Integrations (2nd ed.)*, edited by D. M. Buss, pp. 968–987. John Wiley & Sons, Inc.

Hjeij, M., and A. Vilks. 2023. "A brief history of heuristics: how did research on heuristics evolve?" *Humanit Soc Sci Commun* 10, 64. https://doi.org/10.1057/s41599-023-01542-z.

Hogarth, Robin M. 2001. *Educating intuition.* Chicago: University of Chicago Press.

Hume, David. 2000. *(1739-1740) A Treatise of Human Nature.* Editor D.F. Norton și M.J. Norton. Oxford: Oxford University Press.

Hutchins, Susan, and Lorraine Duffy. 1993. *Decision-Making Evaluation Facility for Tactical Teams.* https://apps.dtic.mil/sti/tr/pdf/ADA265058.pdf.

Janser, Michael. 2017. *Cognitive Biases in Military Decision Making.* https://apps.dtic.mil/sti/tr/pdf/ADA493560.pdf.

Jing Kai, Chen. 2016. "Cognitive Biases: The Root of Irrationality in Military Decision-Making." *Pointer, Journal of The Singapore Armed Forces* Vol.42 (No.2). https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/Vol42No2_6%20Cognitive%20Biases.pdf.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow.* London: Macmillan.

Kahneman, Daniel and Amos Tversky. 1974. "Judgment under Uncertainty: Heuristics and Biases." *Science* 185 (4157): 1124–1131. doi:10.1126/science.185.4157.1124.

—. 1981. "Variants of Uncertainty." *Cognition* 11 (2): 143–157. https://doi.org/10.1016/0010-0277(82)90023-3.

Kahneman, Daniel and Gary Klein. 2009. "Conditions for intuitive expertise: A failure to disagree." *American Psychologist* 64 (6): 515–526. doi:10.1037/a0016755.

Kahneman, Daniel, Barbara L. Fredrickson, Charles A. Schreiber and Donald A. Redelmeier. 1993. "When more pain is preferred to less: Adding a better end." *Psychological Science* 4 (6): 401-405.

Klein, Gary. 1993. "A recognition-primed decision (RPD) model of rapid decision making." În *Decision making in action: Models and methods*, de G. A. Klein, J. Orasanu, R. Calderwood și C. E. Zsambok (Eds.), pp. 138–147. Ablex Publishing.

—. 2004. *The Power of Intuition: How to Use Your Gut Feelings to Make Better Decisions at Work.* Crown Currency.

—. 2015. "A naturalistic decision making perspective on studying intuitive decision making." *Journal of Applied Research in Memory and Cognition* 4 (3): 164–168. doi:10.1016/j.jarmac.2015.07.001.

—. 2017. *Source of Power.How People make Decision.* The MIT Press.

—. 2021. "The RPD Model: Criticisms and Confusions." *Psychology Today*. https:/ /www.psychologytoday.com/intl/blog/seeing-what-others-dont/202102/the-rpd-model-criticisms.

Klein, Gary, Roberta Calderwood and Anne Clinton-Cirocco. 1986. "Rapid Decision Making on the Fire Ground." *Proceedings of the Human Factors Society Annual Meeting* 30 (6): 576–580. doi:10.1177/154193128603000616.

—. 2010. "Rapid Decision Making on the Fire Ground: The Original Study Plus a Postscript." *Journal of Cognitive Engineering and Decision Making* 43 (3): 186–209. doi:10.1518/155534310x12844000801203.

Knighton, Wing R.J. 2004. "The Psychology of Risk and its Role in Military Decision-Making, Defence Studies." 4 (3): 309-334. doi:10.1080/1470243042000344786.

Latham, Gary and Lise Saari. 1982. "The importance of union acceptance for productivity improvement through goal setting." *Personnel Psychology* 35 (4): 781–787. https://doi.org/10.1111/j.1744-6570.1982.tb02221.x.

Lazarus, Richard. 1993. "Coping theory and research: Past, present, and future." *Psychosomatic Medicine* (No. 55): pp. 234-247.

Lazarus, Richard and S. Folkman. 1984. *Stress, appraisal and coping.* New York: Springer.

Lipshitz, Raanan. 1993. "Converging themes in the study of decision making in realistic settings." In *Decision making in action: Models and methods*, de G. A. Klein, J. Orasanu, R. Calderwood și C. E. Zsambok (Eds.), pp. 103–137. Ablex Publishing.

Lyneham, Joy, Camillus Parkinson and Carey Denholm. 2008. "Explicating Benner's concept of expert practice: intuition in emergency nursing." *Journal of Advanced Nursing* 64 (4): 380–387. doi:10.1111/j.1365-2648.2008.04799.x.

Mantua, Janna, Alexxa F. Bessey, Carolyn A. Mickelson, Jake J. Choynowski and Jeremy J. Noble. 2021. "Sleep and high-risk behavior in military service members: a mega-analysis of four diverse U.S. Army units." *Sleep* 44 (4): zsaa221. doi:10.1093/sleep/zsaa221.

Miller, George. 2003. "The cognitive revolution: a historical perspective." *Trends in Cognitive Sciences* 7 (3): 141-144. https://doi.org/10.1016/S1364-6613(03)00029-9.

Montgomery, Henry. 1983. "Decision Rules and the Search for a Dominance Structure: Towards a Process Model of Decision Making." in *Analysing and Aiding Decision Processes*, pp. 343–369. doi:10.1016/s0166-4115(08)62243.

Montgomery, Henry. 2012. "Decision Making and Action: The Search for a Dominance Structure." In *The Construction of Preference*, pp. 342–355. Cambridge University Press.

Mustață, Marinel-Adi and Alina Ionașcu. 2018. "The Story of Behavioral Economics. In a Nutshell." *Strategic Changes in Security and International Relationship.* vol. 3. pp. 204-213.

Mustață, Marinel-Adi and Cristina Bogzeanu. 2017. *Programul euristicilor și biasurilor. Aplicații și implicații în domeniul militar.* București: Editura Universității Naționale de Apărare Carol I. pp. 123-259.

Nalliah, Romesh. 2016. "Clinical decision making – choosing between intuition, experience and scientific evidence." *British Dental Journal* (221): 752–754. https://doi.org/10.1038/sj.bdj.2016.942.

NATO. 2017. *The NATO Alternative Analysis Handbook.* Second Edition. https://www.act.nato.int/wp-content/uploads/2023/05/alta-handbook.pdf.

Park, Whan and Lessig Parker. 1981. "Familiarity and Its Impact on Consumer Decision Biases and Heuristics." *Journal of Consumer Research* 8 (2): 223-230. doi:10.1086/208859.

Peters, Ellen, Daniel Västfjäll, Paul Slovic, C.K. Mertz, Ketti Mazzocco and Stephan Dickert. 2006. "Numeracy and Decision Making." *Psychological Science* 17 (5): 407-413. https://journals.sagepub.com/doi/10.1111/j.1467-9280.2006.01720.x.

Petrofsky, Lyddia A., Corinne M. Heffernan, Brian T. Gregg and Enrique V. Smith. 2021. "Effects of Sleep Deprivation in Military Service Members on Cognitive Performance: A Systematic Review." *Military Behavioral Health* 10 (3): 202-220. doi:10.1080/21635781.2021.1982088.

Pokrant, Marvin. 1999. *Desert Storm at Sea: What the Navy Really Did.* London: Praeger. pp. 176-179.

Qu, Jue, Hao Guo, Wei Wang, Sina Dang and Haiping Liu. 2022. "A Study on the Intuitive Design of Target Search Tasks under Time and Information Pressure." *Brain Sci* 12 (11): 1464. https://doi.org/10.3390/brainsci12111464.

Radtke, Elise L., Rainer Düsing, Julius Kuhl, Mattie Tops and Markus Quirin. 2020. "Personality, Stress, and Intuition: Emotion Regulation Abilities Moderate the Effect of Stress-Dependent Cortisol Increase on Coherence Judgments." *Front. Psychol.* Vol. 11. https://doi.org/10.3389/fpsyg.2020.00339.

Riffenburgh, Robeert. 1991. *Tactical Decision Making Under Stress (TADMUS) Program Study Initial Design.* https://apps.dtic.mil/sti/tr/pdf/ADA242766.pdf.

Seijts, Gerard, Gary P. Latham, Kevin Tasa and Brandon W. Latham. 2004. "Goal Setting and Goal Orientation: An Integration of Two Different Yet Related Literatures." *Academy of Management Journal* 47 (2): 227-239. doi:10.5465/20159574.

Selye, Hans. 1973. "The Evolution of the Stress Concept." *American scientist* 61 (6): 692-699.

Shanteau, James. 1992. "Competence in experts: The role of task characteristics." *Organizational Behavior and Human Decision Processes, Elsevier* 53 (2): 252-266.

Sinclair, Marta, Neal M. Ashkanasy, Prithviraj Chattopadhyay and Maree V. Boyle. 2002. "Determinants of Intuitive Decision Making in Management: The Moderating Role of Affect." In *Managing Emotions in the Workplace*. New York: Routledge. https://www.researchgate.net/publication/45377370.

Spelke, Elizabeth. 1994. "Initial knowledge: six suggestions." *Cognition* 50 (1-3): 431–445. doi:10.1016/0010-0277(94)90039-6.

Sylvester, Benjamin, Damian O'Keefe, Steve Gooch and Eugenia Kalantzis. 2022. "Behavioral Economics in Military Personnel Research and Policy." In *Handbook of Military Sciences*, by A.M. Sookermany (eds). Springer, Cham. https://doi.org/10.1007/978-3-030-02866-4_83-1.

Thaler, Richard H. and Cass R. Sustein. 2008. *Nudge: Improving Decisions about Health, Wealth, and Happiness.* London: Yale University Press.

US Marines Corps. 2010. "Combat and operational stress control." MCTP 3-30E (Formerly MCRP 6-11C), p. 1-3. https://www.marines.mil/portals/1/Publications/MCTP%203-30E%20Formerly%20MCRP%206-11C.pdf.

Van den Berge, Carlo, Amy B. Adler, Roos Delahaij, Suzanne M. Bailey, Merle Parmak, Barend van Tussenbroek, José M. Puente, et al. 2013. "NATO Survey of Mental Health Training in Army Recruits." *Military Medicine* 178 (7): 760–766. https://doi.org/10.7205/MILMED-D-12-00549.

Waxman, Robert. 2019. *Five Philosophers on Free Will: Plato, Hobbes, Hume, Leibniz, and Hegel.* https://philarchive.org/rec/PHDFPO.

Yu, Rongjun. 2016. "Stress potentiates decision biases: A stress induced deliberation-to-intuition (SIDI) model." *Neurobiology of Stress* Vol. 3: pp. 83-95. doi:10.1016/j.ynstr.2015.12.006.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Mountain Combat Operations in the Context of Contemporary Battlefield Requirements

LTC Claudiu Valer NISTORESCU, Ph.D. Candidate*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: Nistorescu.Claudiu@unap.ro

Abstract

The integration of new technologies into military operations has a significant impact on the entire process, resulting in specific features and shaping the character of warfare. The modern battlefield is characterized by the accuracy and long range of new weapon systems, the extensive use of multi-spectral sensors, the continuous improvement of the sensor-to-shooter relationship, and the development of unmanned capabilities. In this context, there is a question as to whether military operations executed in mountainous environments are still relevant in contemporary battlefield equations. These operations are typically spatially limited, static, and attritional, and are subject to transformation from a doctrinal and operational perspective in a paradigm shift in the maneuver-support-fire-protection relationship. This study aims to identify and describe key factors associated with the adaptation of mountain warfare forces and the operations they conduct through an interpretive analysis of land operations.

Keywords:
mountainous environment; tactical operations; doctrinal adaptation; tactical asymmetries.

Article info
Received: 10 April 2024; Revised: 24 May 2024; Accepted: 3 June 2024; Available online: 5 July 2024

Citation: Nistorescu, C.V. 2024. "Mountain Combat Operations in the Context of Contemporary Battlefield Requirements". *Bulletin of "Carol I" National Defence University*, 13(2): 98-109. https://doi.org/10.53477/2284-9378-24-22

Mountainous areas occupy more than 25% of the world's land area, and approximately 20% of the world's population lives in these areas (Allied Tactical Publication, ATP-3.2.1.3 2022, 2-4). Despite the current trend of population migration to urban areas, the mountain environment remains a place where people engage in various activities. Throughout history, there have been numerous instances where armed forces have been required to conduct military operations in mountainous areas. The mountain environment presents a number of challenges in terms of planning, preparation and the execution of tactical operations. Consequently, the mountainous terrain has often provided a position of advantage to one side, leading to actions by the opponent to nullify that advantage. Consequently, regardless of their strategic, operational or tactical value, mountain areas have become the scene of armed confrontations where the belligerents have had to make doctrinal and operational adaptations to meet the specific requirements imposed by the nature of this environment.

The mountainous terrain retains a high potential for the conduct of tactical operations in conventional or unconventional conflicts. This is evidenced by the relevance of operations in this type of environment as outlined in the NATO doctrine for land operations, which requires particular attention from military planners (Allied Join Publication, AJP-3.2 2022, A-24). In a subsidiary manner, the tactical manual for mountain operations emphasizes the necessity for Allied states to maintain a sufficient number of forces capable of operating in this environment (Allied Tactical Publication, ATP-3.2.1.3 2022, 1-1). The current situation indicates that there are sources with the potential to generate armed confrontation in mountain environments. India and Pakistan continue to look at each other through the guns' prism for decades after the first war between the two countries broke out in 1947. Since then, several armed clashes have taken place between the two rivals in the Karakorum Mountains area for control of Kashmir, and *"from time to time along the border, guns are still being heard"* (Marshall 2022, 183). The effective resistance of the mujahedeen guerrillas in the mountainous areas of Afghanistan is well known and despite the continuous adaptation of the Soviet 40th Army, it was eventually defeated (Braithwaite 2015, 268). Ten years later, the scenario is being repeated to some extent and the Taliban insurgency is employing similar tactics to those in the Russian-Afghan conflict. In this case, too, the mountain environment played a role as a force multiplier, providing insurgents with both dispersal opportunities and safe locations for shelter and rebuilding fighting power. The 2020 Nagorno-Karabakh's war was conducted in its final phase, especially in the mountainous area of the region. Both attacker and defender sought to exploit the terrain's characteristics to their advantage, with a number of adjustments to force composition, tactics and combat procedures. Therefore, the field adaptation of the weapons and technologies was required in this case, too (Jones, et al. 2022).

In light of the insights gained from military conflicts and also based on Romania's geographical considerations[1], the Romanian Armed Forces maintain their mountain capabilities while continuing efforts to develop them. In this context, the objective is to identify the needs for doctrinal and operational adaptation of the mountain forces according with the requirements of modern warfare. To this end, a number of objectives have been set to canalize the research effort. Consequently, an interpretative analysis of the phenomenology of ground operations will be conducted in order to identify the necessary adjustments to be made to the composition and organization of those forces. An investigation into the integration of mountain operations with land operations serves to elucidate the respective roles and necessity thereof. Furthermore, the requirements for equipping tactical formations will be determined.

[1] Approximately 30% of Romania's territory is comprised of mountainous areas, with the Carpathians representing one of the country's most prominent geographical features.

The comparative analysis of Western Armies' tactical formations has enabled the acquisition of qualitative and quantitative assets related with the organizing and equipping Romanian similar forces. Finally, the theoretical milestones underlying the doctrinal adaptation of how to deploy forces for mountain hunters will be investigated. The identification and description of the impact of environmental characteristics and new technologies on the operational process, in a context marked by the multidimensionality of the battlefield, has enabled the drawing of relevant conclusions regarding the doctrinal adjustment of tactical operations executed in the mountain environment.

Integrating mountain operations into land operations

The complexity of land operations is the result of the interaction of several factors, which can be categorised as political, military, economic, social, informational and infrastructural. These factors are related to the temporal and spatial dimensions of the operational environment (PMESII-PTT). Under the impact of these variables, land operations fall under the general theme of operations, as defined by NATO doctrine for land operations. These operations can be distinguished by their purpose into defensive operations, offensive operations and stability operations. These tactical-level operations are the result of a tailored combination of several tactical actions, including offensive, defensive, intermediate and/or stability. The weight of the latter is determined by the nature of the tactical operation (Allied Tactical Publication, ATP-3.2.1 2022, 1). The relationship between the themes of operations, the type of tactical operations and the contribution of tactical actions to their materialisation is schematically represented in Fig. No. 1.

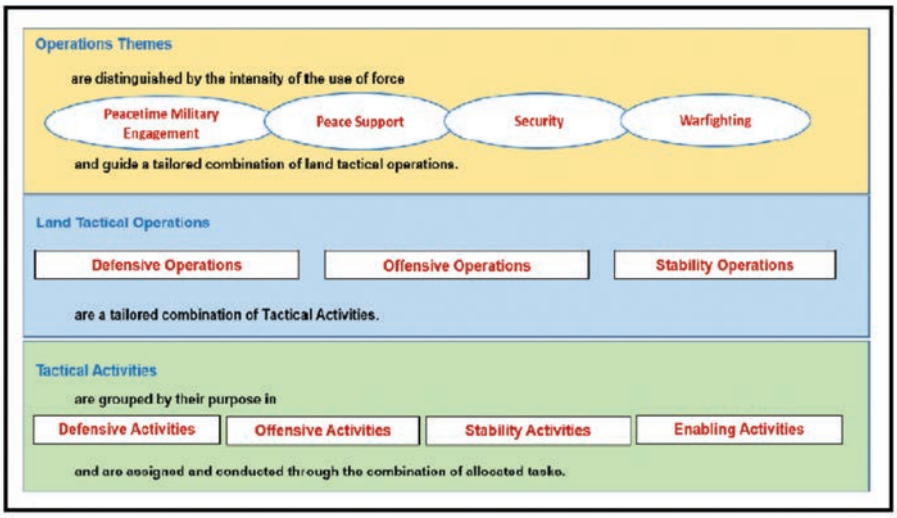

Figure No. 1 Operations themes and types of tactical activities
(Source: ***North Atlantic Treaty Organization, Allied Joint Publication, NATO Standard, *AJP-3.2, Allied Joint Doctrine for Land Operations*, Edition B Version 1, NATO Standardization Office (NSO), 2022, p. 56)

It is evident that the land component of the armed forces plays an indispensable role in a conflict situation, whether the context is combat operations or major crisis operations. The attributes of land forces –complexity, human presence, versatility, and persistence (Jordan, et al. 2016, 86) generated them with a unique status that transcends the specific theme of the operation. Tactical operations conducted in mountainous terrain align with the fundamental tenets of land operations, facilitating the attainment of desired outcomes. These operations may be standalone or be integrated into a larger tactical land operation conducted by the higher echelon. The composition of forces for a tactical operation in mountainous terrain may also be part of a larger ground force or, contingent on the circumstances, operate independently. A schematic representation of the integration of these operations is depicted in Fig. No. 2.

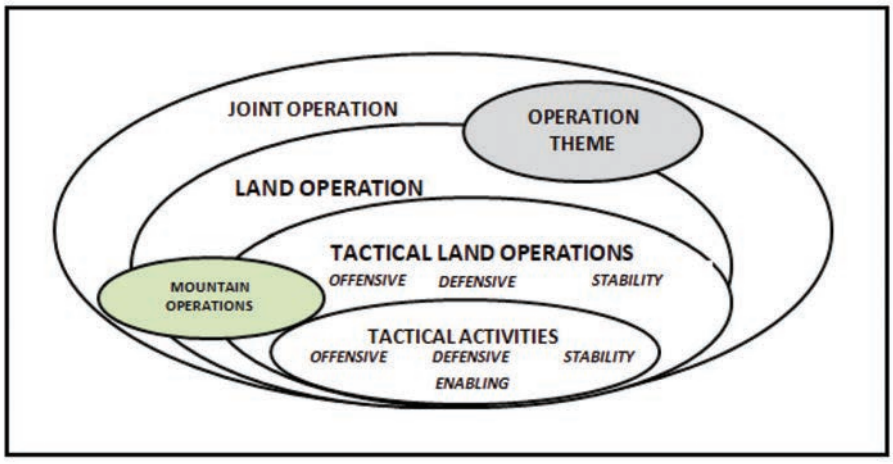

Figure No. 2 The integration of mountain operations into land operations

The specificity of the mountain environment and its influence on the conduct of operations

The mountain environment is a geographical area characterised by a highly fragmented terrain, large differences in altitude, specific weather conditions and poor or non-existent infrastructure. These areas are characterised by steep slopes, wide temperature variations and increased weather effects. Under the influence of these factors, tactical operations are designed in such a way so as to exploit the environment's advantages while reducing its disadvantages and inherent risks.

This type of environment necessitates the creation of military capabilities adapted to the requirements of the confrontation environment as well as the adjustment of tactics, techniques, and operating procedures. The rugged terrain and the electromagnetic wave shielding obstruct the command and control system, thereby hindering force coordination. In this respect, operations in mountain environments should be decentralised, both offensive or defensive operations usually taking the form of a series of clashes and fragmented battles. Intelligence plays an important role taking in consideration the vulnerabilities created by the environment's features. However, the use of ISR means of any kind is limited by the conditions of the environment. The lack of communication, the rugged and predominantly covered with vegetation terrain meant that the mounted forces' operations should to be combined with those of the dismounted ones. Tactical formations need to be equipped with all-terrain vehicles in order to increase their mobility in this type of terrain, as well as appropriate weapons systems to allow firing on ground and air targets. The equipment and armament of forces operating on foot must be designed to achieve an acceptable result in relation to their mass and performance. The maneuver of mounted forces is limited to existing communication paths, therefore maneuver operations are based on the actions of dismounted troops or airborne and forward detachments. From this perspective, the forces will be equipped with light infantry weapon systems to enable their rapid deployment. The availability of fire support is severely constrained by the highly fragmented nature of the terrain. Consequently, the most appropriate means of providing fire support are mortars. The mobility of self-propelled artillery is constrained by the necessity to utilize existing communications. Additionally, the substantial dimensions of the aforementioned platforms impose constraints on their utilisation of the road network. Furthermore, the existing coverings can reduce the effectiveness of ground effect munitions used to engage static targets as well as to neutralize enemy personnel. In this context, the use of fuse or airburst munitions is recommended. Conversely, the compartmentalization of terrain can impede the efficacy of smart munitions by constraining the ability to direct the projectile to the target. Anti-tank missile systems are effective in the engagement of armored vehicles operating in valleys. However, the fragmentation of the terrain and its extensive coverage limit the range of these systems. The existence of large blind areas impeding the targets' acquisition and fire control generate a necessity for the integration of ISR capabilities into combat support formations. The mountainous terrain, by reducing

the efficiency of electromagnetic wave propagation, increases the risk of losing contact with unmanned aerial vehicles (UAVs). Although terrain can facilitate UAS infiltration, adverse weather conditions, particularly high-intensity winds, fog, freezing rain and lightning strikes, severely restrict the time windows in which they can be used (Allied Tactical Publication, ATP-3.2.1.3 2022, 2-12). Finally, it should be noted that UAS class II require special runways for take-off and landing, as mountainous terrain significantly limits the possibility of their construction. Terrain-related difficulties in spotting and engaging targets necessitate the control of the high ground to prevent the helicopters' operations including reconnaissance, attack or insertions as well as UAS actions. MANPAD systems are effective in mountainous environments, provided that they are deployed on dominant terrain. However, the terrain itself limits their use because the presence of dense forest reduces the possibility of observation, while the mountainous terrain itself creates extensive "blind zones" that favour the infiltration of enemy helicopter formations (Department of the Army, ATP 3-90.97 2016, 6-12).

In light of the aforementioned modern battlefield's realities, analyzed from the perspective of the characteristics of the mountain environment, it becomes evident that *a balance of tactical operations* is required and it should take into account, especially the mobility and forces' protection, firepower and the additional environmental risks. In consideration of the operational process's requirements, limitations, and advantages offered by the mountain environment, a number of principles must be taken when planning and executing this kind of operations. These include *height control, decentralization of operations and exercise of mission command, achievement of surprise, the use of reserve, and leadership.* It is similarly important to note that the environment specificity imposes a particular character on operations, and therefore expertise in the field is necessary to integrate all combat functions.

Organisation, composition and forces' equipping

The modern multidimensional battlefield and new technologies embedded into new weapons systems, combat platforms and military equipment impose an adaptation of tactics and combat procedures in mountain environments. Consequently, the force's organisation and composition must also be adapted. In terms of the environment implications on the conduct of tactical operations it is evident that a force must be built in order to have sufficient mobility without drastically affecting its striking power and survivability. It is of the utmost importance to achieve a balance between maneuver and fire in mountain operations. This is assessed separately according to the level of terrain in which the operation is taking place[2]. In this context, in terms of the composition of military forces, the following benchmarks are of particular importance:

[2] The mountainous terrain is categorised into three distinct levels. Level I encompasses the valley bottoms situated along communication lines. Level II encompasses the slopes and secondary ridges on either side of the valleys. Level III encompasses the dominant peaks and ridges.

- ISR capabilities and cavalry to provide both the information needed to plan and execute operations and to create the conditions for taking the initiative;
- combat engineer elements to increase the mobility of maneuver forces while performing counter-mobility missions;
- maneuver formations capable of operating in an integrated manner at all levels of the terrain, combining mounted and dismounted operations with airborne and airmobile operations;
- fire support capabilities capable of decentralised operation and sufficiently mobile to accompany maneuver elements;
- mobile logistic detachments that facilitate the execution of decentralised logistic support.

In terms of force organisation and composition, given the size of the operational area and the requirements for intelligence, force mobility and manoeuvre execution, I believe that the following units should be integrated into a mountain brigade formation:

- 1 reconnaissance battalion ((or regiment);
- 3 to 4 maneuver formations (battalion or regiment level);
- 1 mountain airborne company (up to 1 battalion);
- 1 artillery battalion (up to 1 regiment);
- 1 combat engineer battalion;
- 1 MANPAD company;
- combat support and combat service support elements;
- 1 combat service support battalion;
- 1 subject matter expert/SME cell.

This basic organisational formula is also motivated by an analysis and comparison of the existing mountain brigade formation in some member countries of the North Atlantic Alliance. In the following lines, therefore, the organisation of the Alpine Brigades of the armed forces of Germany, Italy and France will be outlined. It should be noted that the data has been collected from open sources and that there may be differences in the organisation of two similar structures within the armed forces of the same state.

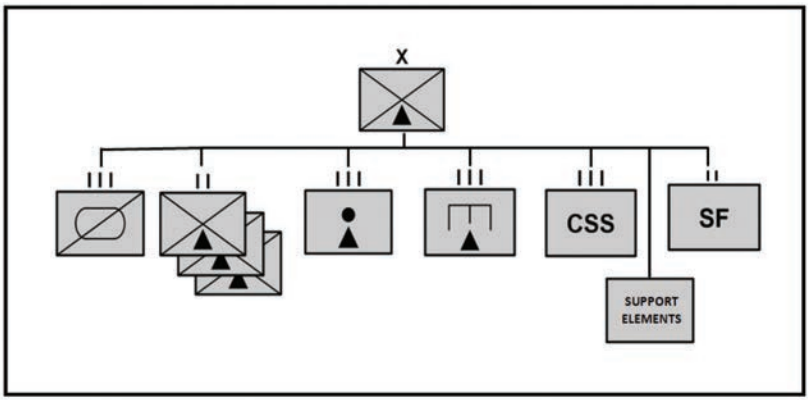

Figure No. 3 Deutsch 23rd Mountain Brigade
(Source: https://www.bundeswehr.de/de/organisation/heer/organisation/division-schnelle-kraefte/gebirgsjaegerbrigade-23)

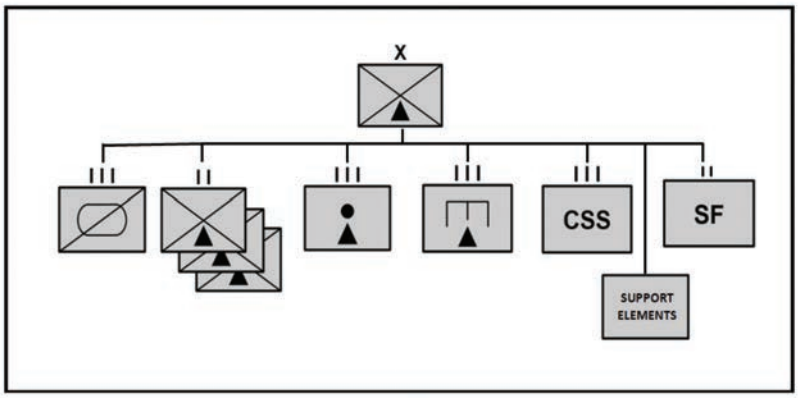

Figure No. 4 French 27 Mountain Brigade
(Source: https://www.defense.gouv.fr/terre/nos-unites/nos-brigades/27e-brigade-infanterie-montagne)

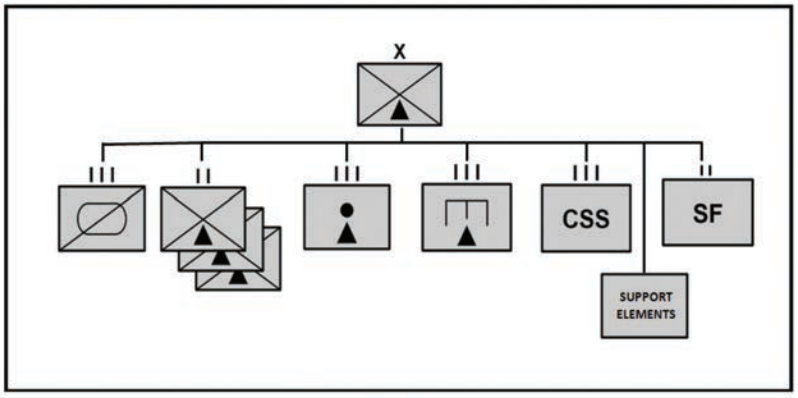

Figure No. 5 Italian „Taurinense" Mountain Brigade
(Source: https://www.esercito.difesa.it/en/organization/the-chief-of-general-staff-of-the-army/comfoter/alpine-troops-command/taurinense-alpine-brigade)

The analysis of the mountain brigade formations described above has identified key milestones in the delivery of weapon systems, combat platforms and equipment to mountain forces:

- the maneuver forces' endowment with combat platforms must provide an optimal mix of armoured, light armoured and unarmoured platforms; as far as armoured platforms are concerned, the use of tracked variants brings additional mobility, as they have a greater cross-country capacity in terrain covered with ice and snow, but modern medium-armoured wheeled variants are also effective in this type of terrain; lightly armoured and unarmoured ATVs are useful for specialised and reconnaissance detachments, enabling them to carry out screening and infiltration missions into enemy's rear;
- high trajectory artillery systems are most effective in mountainous environments, so it is necessary to equip mountain infantry with them down to the lowest tactical level; if at the level of the mountain battalion the main element of fire support is howitzers, at the level of the brigade, within the artillery battalion (or regiment), 155 mm self-propelled or towed howitzer can also be chosen; the integration of anti-tank weapon systems within the artillery battalion is not a priority, as the fight against armour is

decentralised and carried out by the brigade's battalions;

- given the limited mobility and versatility of recoilless gun anti-tank systems, we recommend replacing them with anti-tank guided missile/ATGM systems with *fire-and-forget, top-attack* and *flying top-attack* capabilities; given the difficulty of the terrain and the predominant use of dismounted forces, man-portable variants are the most appropriate; these capabilities to engage enemy armour will be formed into integrated sub-units at company and battalion level;
- the most appropriate means for aerial force protection are MANPADs; their high mobility, simplicity and effectiveness on target make them ideal for use in this environment;
- attack and surveillance drones can be useful during the conduct of military operations in mountainous environments, but due to weather conditions and communication system malfunctions, the effects of these capabilities are limited;
- the organisation and equipping of logistic modules must be carried out in such a way as to ensure the support of forces in all types of terrain (level I, II and III); thus, at brigade level, storage and transport sub-units must have vehicles (trucks) capable of operating in level I and II terrain, and at battalion level, these logistic structures must have transport capabilities capable of operating in level III high mountain areas (transport trackers, UTVs).

Doctrinal adaptation of tactical combat operations

In light of the specific characteristics of operations in mountainous environments and the requisite configuration, organisation and equipping of military forces, we will further examine the doctrinal implications of the shaping factors of the modern battlefield. These include the integration of advanced technologies into new weapon systems, the extension of the range and improvement of the accuracy of these systems, multispectral sensors, the fragmentation of operations and the extension of the phenomenon of "fragmented battles" specific to non-contiguous and non-linear areas of operations, as well as the use of unmanned and autonomous systems.

With regard to the defence operation, two possible approaches to its effective organisation can be identified:

a. A solid, linear and continuous defence, concentrating all combat power on the enemy's main directions of penetration.

b. An elastic defence, allowing the gradual absorption of the enemy's offensive effort.

In order for this strategy to be viable, it must be ensured that there are sufficient forces and resources available to guarantee a strong initial alignment on the battlefield, as well as reserves to execute counterattacks to close any gaps that may be created. The efficacy of this defensive strategy is evidenced by the lessons learned

from military conflicts, particularly those involving the integration of deep and contact strike systems. One of the most notable instances of the utilisation of this defensive form is the Battle of Monte Cassini during the Second World War. Here, German forces established the so-called Winter Line, with the central axis situated near Cassini, with the objective of impeding the Allied advance towards Rome. It is important to note, however, that due to the reduced number of forces available, this type of defence was challenging to implement in order to cover a large front. In addition to the aforementioned considerations, the enhanced capabilities of intelligence gathering will disadvantage those who find themselves in a position of disadvantage. Such individuals will be subject to accurate enemy fire.

The second scenario entails the organisation of mobile detachments with the objective of continuously harassing enemy forces through the implementation of swift hit-and-run attacks and ambushes on maneuver elements, as well as combat and logistical support elements. It is imperative that these detachments are equipped with the most up-to-date mobile combat platforms and portable weapon systems (RAD, MANPAD) if they are to be successful. It is of the utmost importance to control the dominant heights, and if they are lost, efforts must be made to prevent their occupation by the enemy by striking them with long-range weapons. It may also be necessary to maintain control of important objectives or key terrain. An extensive multispectral sensor system, providing coverage of the operation's area will provide timely information on enemy actions. Reconnaissance elements, should be deployed to complement the screening system, in order to coordinate the strike systems and the mobile detachments' operations. In this context, the most appropriate tactics and techniques of operation are ambushes, raids, Motti tactics, blocking communication lines, and actions designed to counter infiltrating elements.

The implementation of offensive operations in mountainous terrain is significantly constrained by environmental limitations. It is of the utmost importance to seize and control heights when undertaking offensive actions in the mountain environment. It is imperative that the valleys and the main axes of advance are secured before any movement is made along the slopes. The main forces advancing on communications will be preceded by forward detachments comprising anti-tank teams whose mission is to repel possible armoured counter-attacks. In order to maintain control over the dominant ground and other key terrain, the deployment of air defense capabilities becomes a priority. Given the difficulty of the terrain, MANPAD systems are the most appropriate solution. A key role in offensive operations in mountainous and forested terrain is played by turning movement detachments. The turning movement is conducted in order to shape the battle space, also aims to unbalance the enemy by creating a threat in his rear area. Regardless of the value of this detachment, its mission and mode of infiltration, the configuration and armament systems are crucial in order to generate effects designed to unbalance the enemy's defences. Concurrently, the deployment of extended-range strike systems, including unmanned aerial systems (UAS), can facilitate the extension of the mission of these detachments in terms of both

space and time. In the context of an offensive operation, the most appropriate tactics and techniques are as follows: turning movement, raids, air assault, and limited attacks. In light of the aforementioned considerations, it can be posited that the following implications are generated at the level of operations carried out in the mountain environment:

- the allocation of an area of operations, as in the urban environment, does not depend directly on the range of the weapons systems;
- the planning of tactical operations, whether offensive or defensive, must take into account the fact that mutual support and higher echelon's support is limited. Consequently, execution should be decentralised, which generates the need to organise the force in agreement with the combined-arms principle down to the lowest level;
- the employed TTPs must generate tactical asymmetries that undermine the enemy's operations cohesion. Consequently, the operation design must take into account the integration of all doctrinal frameworks – operational, geographical and tactical framework;
- the force's organisation must take into account the need to identify capabilities that can operate, at least separately, at all levels of mountain terrain;
- the allocation of weapons systems in support of small tactical units must be based on their mission type and on their degree of the independence;
- it is imperative that operations be conducted in a manner that will unbalance the enemy, thereby affecting his cohesion and comprehension. This is necessary for success, both in offensive and defensive operations. The creation of multiple operational dilemmas for the enemy will prevent him from implementing his plan and deplete his resources;
- the utilisation of extended-range and high-accuracy striking systems must consider the exploitation of limited windows of opportunity and the achievement of significant effects for the decisive operation.
- furthermore, the exercise of mission command, a crucial aspect of mountain operations, is enhanced by high-performance equipment and weapon systems.

Conclusions

The extended range and improved accuracy of new weapon systems, coupled with the rapid and continuous development of ISR assets, are significantly shaping the modern battlefield. This framework for future conflicts will drastically limit the possibility of large-scale combat operations in mountainous areas. It is unlikely that impetuous penetrations with armoured formations, such as those executed by the German Army in the Ardennes Mountains, will occur, nor will the organisation of cohesive defensive lines similar to those organised by the Germans in the Monte Cassini area in World War II. However, the analysis indicates that tactical operations conducted in the mountain environment retain their relevance today, particularly due to the ability of the terrain to channel the actions of maneuver forces. The opening

or closing of mountain passes can have significant consequences for the operations' design, whether offensive or defensive. While these approaches present operational difficulties, they facilitate the supply of forces, help to achieve or prevent surprise, and cause the enemy to redeploy forces to counter potential threats. Consequently, these operations have a shaping role in the execution of the joint operation.

The research's findings indicate that the success of executing tactical operations in mountainous terrain depends on the ability to outpace the enemy in the decision-making cycle. This is achieved by outperforming them in terms of intelligence acquisition, speed of maneuver, accuracy of fires, and an improved *sensor-to-shooter* relationship. It is of the utmost importance to satisfy operational requirements in terms of achieving a balance between force mobility, fire execution capabilities and the protection of force components. Increased survivability of the force is a key factor in achieving success on the battlefield. In this regard, reduction of the multispectral footprint is of paramount importance. Finally, commanders must be aware of the high risk of action due to terrain and weather effects. It is also important to consider the impact of sudden changes in weather conditions when using maneuver elements and fire support. It is of paramount importance that commanders and staffs maintain a constant focus on the need to enhance the expertise of specialized mountain combat cells. In this regard, the experience of "alpine" troops, lessons learned, staff studies and field reconnaissance offer a significant advantage.

References

Allied Join Publication, AJP-3.2. 2022. *ALLIED JOINT DOCTRINE FOR LAND OPERATIONS.* Edition B version 1. Bruxel: NATO Standardization Office (NSO).

Allied Tactical Publication, ATP-3.2.1. 2022. *Allied Land Tactics.* Edition C, Version 1. Brussels: NATO Standardization Office (NSO).

Allied Tactical Publication, ATP-3.2.1.3. 2022. *Conduct of Land Tactical Operations in Mountainous Environment.* Edition A Version 1. Bruxel: NATO STANDARDIZATION OFFICE (NSO).

Braithwaite, Rodric. 2015. *URSS în Afganistan (1979-1989).* București: Editura Corint.

Department of the Army, ATP 3-90.97. 2016. *Mountain Warfare and Cold Weather Operations.* SUA: Headquarters, US Army.

Jones, Seth G., Jake Harrington, Christopher K. Reid, and Matthew Stohmeyer. 2022. *Combined Arms Warfare and Unmanned Aircraft Systems.* International Security Project, Center for Strategic & International Studies, Washington: Rowman&LittleField, 10.

Jordan, David, James D. Kiras, David J. Lonsdale, Ian Speller, Christopher Tuck, and C. Dale Walton. 2016. *Understanding Modern Warfare.* Second Edition. Cambridge University Press.

Marshall, Tim. 2022. *Prizonierii geografiei.* București: Litera.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Naval forces operational environment. Flexibility and strategic adaptability

Lt. Cdr. (N) Lavinia Elena TĂNASE (MĂXINEANU), Ph.D. Student*
Commander (r.) Prof. Ion CHIORCEA, Ph.D.**

*Romanian Naval Forces, 56th Frigate Flotilla / "Carol I" National Defence University
e-mail: laviniamaxineanu@gmail.ro
**"Mircea cel Bătrân" Naval Academy, Constanța

Abstract

In the dynamic scene of naval operations, constant adaptation and innovation are imperative to meeting the challenges and opportunities of technological advances, geopolitical changes and environmental considerations. This article aims to explore the multidimensional landscape of the naval operational environment, offering original insights and solutions to enhance naval capabilities and cooperation on a regional and global scale. From the forefront of technological innovation, onboard unmanned systems integration and artificial intelligence-based decision-making, to strategic adaptability in response to geopolitical dynamics, the study explores the complex interplay between naval strategy and emerging trends, with environmental considerations taking centre stage. The article argues for a collaborative global naval framework, highlighting the importance of international cooperation in addressing common maritime challenges. This framework envisages the creation of alliances, initiatives and partnerships to foster collective security, promote environmental protection and ensure the peaceful use of the world's oceans. The main objective is to highlight the intersections between technological advances, strategic flexibility, environmental factors and international cooperation in shaping the future of naval operations. Overall, the study aims to engage a diverse audience comprising policymakers, maritime military leaders, researchers, academics and stakeholders involved in maritime security, defence and environmental protection.

Keywords:
naval operations; maritime security; unmanned autonomous systems; artificial intelligence; environmental factors; strategic adaptability.

Article info
Received: 9 May 2024; Revised: 3 June 2024; Accepted: 14 June 2024; Available online: 5 July 2024

Citation: Tănase (Măxineanu), L.E. and I. Chiorcea. 2024. "Naval forces operational environment. Flexibility and strategic adaptability." *Bulletin of "Carol I" National Defence University*, 13(2): 110-120. https://doi.org/10.53477/2284-9378-24-23

The operating environment of naval forces, characterized by the adjacency of the sea, rivers, and inland waters, constantly changes due to the fluctuating geopolitical situation, the impact of technological progress, the development of artificial intelligence, and the importance of environmental management. Naval forces around the world are being forced to adapt, innovate, and reconsider conventional frameworks for maritime strategies and naval operations.
In this article, we aim to examine and explore new and timely perspectives on the specifics of the naval force operating environment in general, with a particular focus on emerging technology, strategic flexibility, the consequences of climate change and the possibility of collaborative regional/global management of the world's seas and oceans.

The actions and operations of naval forces have been and continue to be the subject of extensive analysis, reflection and debate. From ancient Greece to the present day, operations, naval capabilities, battles and strategies have been instrumental in mapping the world and shaping global history. Thus, we will refer to present events as a perspective on the future of naval forces and the types of conflicts or engagements we will face.

We will explore the relationship between the environment, understood as civil society, and defence, focusing on conflict and cooperation. We will address the dual role of military structures in peacetime, highlighting both their conflicting aspect, which contributes to pollution and environmental degradation and their cooperative aspect, which engages in community activities such as emergency response, combating environmental degradation and managing climate change.
To this end, three research objectives have been set: following the status and trends of technological developments impacting naval operations, conducting an analysis of strategic adaptability and geopolitical factors, and identifying environmental factors and their impact on climate change.

In the first section of the article, we look at current tendencies and emerging technologies in naval operations, focusing on modular unmanned systems, artificial intelligence-based decision making and quantum cryptography to enhance flexibility and operational security. The second objective of this research is to highlight the importance of assessing alliances and military positions in the face of intense power rivalries, especially in regions such as the Black Sea. The paper proposes innovative strategies, such as dynamic force deployment plans to deter potential adversaries and create a secure environment for allies.

In addition to the first two proposed objectives, we considered it necessary to set an objective from the field of maritime security operations, in the area of non-combat operations, during which we will highlight the non-combat role of naval forces in contributing to the maintenance of maritime security, in the field of environmental protection. Thus, the study of the impact of naval activities on the environment and

the implications of climate change on maritime security is the focus of the final part, in which we have addressed the challenges and opportunities that climate change presents for naval forces, such as the opening of new shipping routes and the need for a strategic presence to secure maritime communications.
In conclusion, we will advocate for a holistic approach that balances operational efficiency, environmental responsibility and international cooperation in naval operations.

Advancements in technology for naval operations

We share the opinion that advances in technology have altered the way naval tactics are addressed (Scipanov and Totir 2023, 46), so we build on this premise to highlight the role of unmanned systems on board, predictive engagement based on artificial intelligence, and quantum cryptography in addressing future naval force strategies.
The vanguard of innovation in naval operations is marked by impressive developments in unmanned systems, artificial intelligence (AI) and cyber security. Unmanned systems, such as aerial vehicles (UAVs), underwater vehicles (UUVs) and surface vehicles (USVs), offer enhanced surveillance capabilities, mine countermeasures, anti-submarine warfare, targeting, and the list could continue, depending on the ingenuity and technical knowledge of the users (Boulanin and Verbruggen 2017). By incorporating artificial intelligence into these systems, we can improve autonomous decision-making processes, increase operational efficiency, and increase the pace at which risks are addressed. In addition, the cyber domain has emerged as a crucial conflict arena for naval forces. The need for cyber security measures has become paramount, given the increasing reliance on digital systems and networks. Advances in quantum computing and encryption technologies have the potential to provide naval forces with unprecedented protection against cyber threats, ensuring the reliability of command-and-control systems (Venegas-Andraca, Lanzagorta şi Uhlmann 2015, 1-8).

According to Mekdeci et al. (2012), maritime unmanned systems have become essential assets in contemporary naval operations, offering exceptional capabilities for enhancing Maritime Domain Awareness and force multiplication. In order to optimize the use of these technical advancements, it is possible to create modular unmanned systems (Barbier, Bensana and Pucel 2018) that may be readily tailored to different tasks. These platforms could have interchangeable modules for surveillance, electronic warfare, or striking vector delivery, allowing rapid reconfiguration to align with specific mission demands. According to Boulanin and Verbruggen (2017), the use of modularity would enhance operational flexibility and minimize the logistical strain by enabling a single platform to carry out various functions.

Artificial intelligence (AI) and machine learning (ML), which are rapidly expanding fields within contemporary technology, have the potential to significantly transform

naval operations via enhancements in decision-making processes, predictive equipment maintenance, and threat detection. Integration of artificial intelligence in analytics enables efficient and precise identification of threats and abnormalities by processing extensive quantities of data derived from satellite images, sensor networks, and ISR systems. The implementation of AI-driven predictive engagement systems, which leverage current operational models and historical data (feedback) to forecast potential threats and suggest preventive measures, has the capacity to streamline decision-making processes and effectively mitigate the impact of diverse risks. Simultaneously, machine learning algorithms could be implemented in these systems to enhance their precision progressively, enabling naval forces to maintain a strategic advantage over adversaries through predictive manoeuvring and preemptive countermeasures (Mukherjee 2018, 9).
Securing the digital infrastructure of naval operations is imperative as naval forces increasingly rely on networked systems, therefore cybersecurity becomes essential to protect these assets from espionage, sabotage and cyber threats. Concurrently, the complexity and sophistication of cyber threats require constant innovation and ingenuity in cybersecurity measures to protect communications, navigation and operational command systems.

Quantum cryptography for naval communications has been proposed as a potential way to address the challenges posed by cyber-attacks (Papathanasaki, et al. 2021). Quantum cryptography leverages the fundamental laws of quantum physics to provide encryption that is nearly impervious to decryption, therefore guaranteeing the preservation of communication integrity and confidentiality, even when confronted with sophisticated cyber threats. The use of quantum encryption technology in naval communications networks will greatly augment the security of confidential data and operational guidelines. Simultaneously, the establishment of alliances, the facilitation of information exchange, and the cultivation of situational awareness are critical components of a holistic strategy towards maritime cybersecurity, aiming to attain worldwide maritime cyber supremacy (Greiman 2019).

In summary, the use of technical advancements in naval operations offers a range of prospects and obstacles, alongside the introduction of new vulnerabilities. To solve these problems and enhance their operational capabilities, naval forces might use novel technologies such as modular maritime unmanned systems, predictive engagement based on artificial intelligence, and quantum cryptography. These technological advancements will empower naval forces to sustain strategic advantage in a progressively intricate and disputed maritime domain, guaranteeing their position as leaders in contemporary military technology and strategy. Simultaneously, we will witness a revolution in the way naval forces operate and a redefinition of maritime warfare and security. The future trajectory of naval warfare will be primarily influenced by the interplay between humans and machines, including both tangible realms such as water, space, air, and land, as well as intangible realms like cyberspace, electromagnetic networks, brain waves, and human consciousness.

Strategic adaptability and geopolitical factors

The purpose of this section is to evaluate the geopolitical processes that impact maritime security, especially in regions of strategic significance, such as the Black Sea. Additionally, this section aims to provide solutions for enhancing strategic adaptability in order to effectively respond to emerging threats and alliances.
Simultaneously, within the framework of evolving geopolitical circumstances, naval forces must exhibit strategic adaptability to maintain maritime security and exert significant influence within their designated area of responsibility and interest. The resurgence of intense competition among the dominant nations, particularly in the Black Sea, Baltic Sea, or Indo-Pacific region, necessitates a comprehensive evaluation of alliances and military stances. A novel and distinctive approach would include the development of a dynamic force deployment strategy, enabling adaptable and unpredictable naval operations. The regional military program BLACKSEAFOR, which operated from 2001 to 2008, has effectively deterred illicit activities in the Black Sea area. Exercises executed jointly by the littoral states, through the activation of a multinational naval group at least once a year (being also an 'on-call' force), in which naval forces of all littoral states participated, increased the stability of the Black Sea area (Sanchez 2012).

The advent and development of maritime hybrid warfare, which combines traditional naval capabilities with asymmetric tactics and cyber operations, has the potential to reinvent the fundamental concepts of naval warfare. By prioritizing non-kinetic warfare and information superiority, we can gain a significant advantage in contested maritime areas.

An effective approach to address these rapid transformations is the establishment of adaptable regional alliance frameworks. These include dynamic alliances between nations with similar interests, with a specific emphasis on swift deployment capabilities, combined maritime patrols, and also the establishment of a common database. In contrast to conventional alliances, which may get entangled in bureaucratic processes, the use of agile frameworks would provide prompt and synchronized reactions to new threats and occurrences, therefore enhancing collective security and deterrence.

Apart from rivalry between major powers or military threats, global maritime security is threatened by non-state actors, including piracy, maritime terrorism, illegal weapons and human trafficking, and environmental degradation. These challenges require multinational cooperation and innovative approaches to ensure the security of the seas for all nations. By implementing an integrated maritime surveillance and response initiative we could leverage satellite technology, unmanned autonomous systems, and artificial intelligence-based data analytics to monitor maritime traffic and threats regionally and globally. As hybrid threats originate from both state and non-state actors, targeting either a state's citizens, critical infrastructure or

even armed forces we can include naval forces, border police and even the civilian population in the surveillance system by developing national maritime awareness and vigilance to threats originating from the sea, so that every yacht or recreational vessel present at sea can be a sensor/warning system.
Participating nations could contribute with resources, and capabilities and also facilitate the exchange of information, enabling rapid response units to address piracy, trafficking, environmental crises, etc. The initiative would also promote adherence or facilitate compliance with international maritime laws and regulations, strengthening global maritime governance.

To enhance strategic adaptability, a term that signifies the ability to rapidly adapt strategy and course of action in response to circumstances, opportunities and trends based on past experience and available resources (McKee, Varadarajan and Pride 1989) the concept of hybrid naval force development can be introduced. This approach involves training and equipping naval forces with a combination of conventional, unconventional and cyber warfare capabilities. By integrating cyber units with traditional naval forces, they can conduct a diverse array of operations, from naval operations to asymmetric warfare and cyber defence. This multi-dimensional force structure would significantly complicate the calculations of potential adversaries, enhancing deterrence and operational flexibility.

In conclusion, the complexity of today's geopolitical landscape and the broad nature of maritime security challenges require a prospective approach to naval strategy. Hybrid warfare and its cyber dimension also force us to reassess traditional naval strategies. Naval forces must adapt to these changes to protect their interests and maintain their strategic advantage, and by adopting flexible alliance frameworks, launching a Maritime Surveillance and Response Initiative and developing hybrid naval forces, we could achieve a high degree of strategic adaptability. These solutions support building resilience, promoting international cooperation and securing maritime interests in an uncertain and unpredictable regional/global environment.

Environmental factors and the impact of climate change

This section aims to examine the impact of naval activities on the environment and the implications of climate change on maritime security. The goal is to identify sustainable practices and measures that enhance the resilience of naval forces. This will be achieved by demonstrating the non-coercive benefits of projecting naval power at sea.
The interplay between the environment, sometimes referred to as a civil society, and defence is marked by both divergent components and collaborative efforts. During times of war, it is undeniable that the armed forces have a purpose of causing violence and destruction. However, in times of peace, military formations have a dual responsibility in relation to the environment. The initial role is characterized

by conflict, as the armed forces, tasked with preparing for missions mandated by the Constitution and the government, inadvertently contribute to extensive pollution (including acoustic, atmospheric, and chemical pollution) and the degradation of the territory. This occurs through the execution of training exercises and operations, as well as the frequent establishment of industrial enterprises, military airports, barracks, and arms and munitions depots. The second function is collaboration, whereby the armed forces position themselves as entities capable of executing actions that are often dual in character, including both preventive and intervention in emergency scenarios, for the benefit of the community.

As mentioned above, the naval operational environment is inextricably linked to the natural environment, and the phenomenon of climate change presents both challenges and opportunities for naval forces. The ongoing phenomenon of polar ice cap melting is creating new shipping routes that require a strategic presence to ensure safe maritime navigation. Furthermore, naval forces have the potential to assume a pioneering role in environmental preservation via the use of sustainable technology, including alternative fuels and energy-efficient propulsion systems, in order to mitigate their ecological footprint.

The need for naval forces to reduce their environmental footprint has led to the exploration of sustainable technologies and practices, and we can include the adoption of alternative fuels, energy efficiency measures and advanced propulsion systems. One solution is the widespread adoption of advanced biofuels and hybrid-electric propulsion systems in fleets. Sustainably sourced biofuels can significantly reduce greenhouse gas emissions compared to conventional fuels. Hybrid-electric systems, which combine electric propulsion with traditional engines, offer improved fuel efficiency and lower emissions (Council of the European Union 2023). In addition, the development of solar-powered charging stations at sea or in port for these hybrid vessels could reduce pollution.

Regarding the climate change issue, to enhance resilience we can adapt infrastructure and naval operations. Climate change poses significant challenges to naval operations, including rising sea levels affecting naval bases and increasing frequency of severe weather events impacting force deployment and even training. One potential strategy is the establishment of naval bases that are resilient to climate change. This necessitates the construction of bases that can endure the impacts of rising sea levels and severe weather events which be achieved by integrating floating docks, flood defence systems, and stormwater management systems. Furthermore, equipping bases with weather radars, marine beacons, waste collection infrastructure, and the integration of renewable energy sources like solar and wind power into base infrastructures has the potential to enhance sustainability and diminish reliance on external energy sources (Ministerul Transporturilor și Infrastructurii 2023).
Due to their distinctive capabilities and extensive worldwide presence, naval forces are in a favourable position to make significant contributions to environmental

conservation initiatives and advancements in meteorology and oceanographic research. The involvement of naval forces in environmental monitoring and catastrophe response may significantly contribute to the advancement of innovation in these domains. The use of sophisticated satellite imagery and data analysis techniques has the potential to enhance comprehension of climatic patterns, hence making valuable contributions to humanitarian aid operations and disaster relief endeavours.

One potential unique project could be the implementation of regional or global naval environmental patrols, which would consist of dedicated naval forces responsible for monitoring environmental well-being, enforcing rules pertaining to illegal fishing and pollution, as well as performing climate research. These entities have the potential to engage in partnerships with global scientific institutions, facilitating the exchange of data and resources in order to enhance comprehension of oceanic climatic phenomena, marine biodiversity, and the ramifications of climate change on marine ecological systems. Utilizing technology for environmental monitoring and disaster response has exceptional prospects to enhance the involvement of naval forces in environmental monitoring and emergency response to climate change-induced natural catastrophes.

The utilization of artificial intelligence (AI) in the advancement of environmental monitoring and catastrophe prediction systems is a novel strategy for leveraging naval technology capabilities. These systems could use satellite imagery, drone surveillance and sensor data to monitor environmental conditions, predict natural disasters and coordinate rapid response efforts. By integrating artificial intelligence algorithms, these systems could analyze vast data sets to identify patterns and predict events such as tsunamis, hurricanes and oil spills, enabling proactive response and mitigation efforts.

To summarize, the convergence of naval operations, environmental factors, and climate change poses a range of obstacles and prospects. Naval forces can effectively address global environmental and climate challenges by implementing sustainable naval operations, enhancing resilience to climate change, actively participating in environmental protection and climate research, and utilizing technology for environmental monitoring and disaster response. The proposed solutions have the dual objective of reducing the environmental consequences associated with naval operations and using naval assets to foster a sustainable and resilient marine environment.

The pressing need for naval forces to embrace a more sustainable and responsible strategy is underscored by the environmental consequences of naval operations and the broader ramifications of climate change on maritime security. Comprehensive strategies to incorporate environmental responsibility into navy activities include several initiatives, including the deployment of biofuel-powered and hybrid-electric

ships, the creation of climate-resilient naval facilities, and the organization of naval environmental patrols. These endeavours not only provide a significant contribution to the worldwide battle against climate change but also guarantee the long-term viability of naval operations for future generations.

An alliance to address environmental challenges could promote the adoption of green technologies in naval fleets, encourage joint research missions to study the impact of climate change on the seas and oceans and initiate global naval operations dedicated to reducing pollution and supporting the conservation of marine biodiversity. International seminars and conferences would provide a platform for naval forces to exchange best practices and innovative approaches in the field of environmental management.

The promotion of technical cooperation and innovation among naval forces worldwide should not be disregarded. This hub would function as a centralized platform for the exchange of information, resources, and optimal methods in the advancement of naval technology, with a specific emphasis on unmanned systems, cyber security, and artificial intelligence.

Establishing a global maritime governance and legal framework is essential to ensure consistent and equitable application of international maritime law, addressing emerging challenges such as cyber warfare at sea and the militarization of maritime zones. This framework would work towards harmonizing maritime law enforcement and conflict resolution processes, ensuring that all actions are grounded in international law. Additionally, it would assist with continuous communication and bargaining on the revision of global maritime legislation, guaranteeing its continued applicability in light of evolving maritime security dynamics and technology advancements.

Conclusion

By achieving the objectives listed in each section, the study aims to contribute to advancing knowledge and understanding of the naval operational environment from a different perspective, while providing applicable recommendations for policymakers, military leaders, and stakeholders to skillfully manoeuvre through the complexities of the contemporary maritime sphere.

The 21st-century naval operational environment presents a panorama of challenges and opportunities, so by embracing technological innovation, adapting to geopolitical changes, addressing environmental impacts and pursuing collaborative frameworks, naval forces can navigate the uncertain waters ahead with confidence and strategic foresight. The future of naval operations will be characterized by agility, innovation and an unwavering commitment to maintaining regional/global maritime security.

However, in an era marked by rapid technological advances, changing geopolitical landscapes and pressing environmental challenges, the role of naval forces extends far beyond traditional notions of maritime security and power projection.

Throughout this study, we have explored the multifaceted dimensions of the naval operational environment, offering original solutions aimed at improving technological innovation, strategic adaptability, environmental management and regional/global collaboration. Collaboration must operate on the principles of mutual respect, shared responsibility and collective action, encouraging the participation of regional and/or global naval forces, irrespective of their size or capabilities.

Through regular technology exchanges, workshops and joint development programs, cooperation between naval forces, defence industries and academic institutions is achieved, and by pooling resources and expertise, the development and deployment of state-of-the-art technologies in global naval operations would be accelerated, enhancing overall maritime security and operational effectiveness.

The proposed solutions provide a roadmap for the transformation of naval operations, highlighting the need for a holistic approach that balances operational efficiency with environmental responsibility and international cooperation. In the context of the 21st century, the establishment of a peaceful, safe, and sustainable maritime domain for present and future generations necessitates the collaborative efforts of international naval forces.

References

Barbier, Magali, Eric Bensana, and Xavier Pucel. 2018. "A generic and modular architecture for maritime autonomous vehicles." Porto, Portugal. 2018 IEEE OES Autonomous Underwater Vehicle Symposium (AUV).

Boulanin, Vincent, and Maaike Verbruggen. 2017. *Mapping the Development of Autonomy in Weapon Systems.* Stockholm International Peace Research Institute. https://www.sipri.org/publications/2017/policy-reports/mapping-development-autonomy-weapon-systems.

Council of the European Union. 2023. *FuelEU maritime initiative: Council adopts new law to decarbonise the maritime sector.* https://www.consilium.europa.eu/en/press/press-releases/2023/07/25/fueleu-maritime-initiative-council-adopts-new-law-to-decarbonise-the-maritime-sector/.

Greiman, Virginia. 2019. "Navigating the cyber sea: Dangerous atolls ahead." International Conference on Cyber Warfare and Security: 87-93,XI. https://www.proquest.com/conference-papers-proceedings/navigating-cyber-sea-dangerous-atolls-ahead/docview/2198531195/se-2.

McKee, Daryl O., P. Rajan Varadarajan, and William M. Pride. 1989. "Strategic Adaptability and Firm Performance: A Market-Contingent Perspective." *Journal of Marketing* 53 (3): 21-35. https://doi.org/10.2307/1251340.

Mekdeci, Brian, Adam M. Ross, Donna H. Rhodes, și Daniel E. Hastings. 2012. „Investigating Alternative Concepts of Operations for a Maritime Security System of Systems." *INCOSE International Symposium* 22 (1): 1986-1998. https://doi.org/10.1002/j.2334-5837.2012.tb01451.x.

Ministerul Transporturilor și Infrastructurii. 2023. "Ordinul nr. 1848/2023 privind aprobarea Schemei de ajutor de stat pentru realizarea de investiții în infrastructura de transport naval aferentă Programului Transport (PT 2021-2027)." Publicat în Monitorul Oficial nr. 954 din 23 octombrie 2023. https://legislatie.just.ro/Public/DetaliiDocument/275550.

Mukherjee, Tuneer. 2018. *Securing the Maritime Commons: The Role of Artificial Intelligence in Naval Operations.* ORF Occasional Paper. https://www.orfonline.org/research/securing-the-maritime-commons-the-role-of-artificial-intelligence-in-naval-operations.

Papathanasaki, Maria, Panagiotis Fountas, Leandros Maglaras, Christos Douligeris, and Mohamed Amine Ferrag. 2021. "Quantum Cryptography in Maritime Telecommunications." *2021 IEEE International Conference on Cyber Security and Resilience (CSR).* Rhodes, Greece. doi:10.1109/CSR51186.2021.9527973.

Sanchez, W. Alejandro. 2012. *Did BLACKSEAFOR Ever Have a Chance?* https://www.e-ir.info/2012/11/18/did-blackseafor-ever-have-a-chance/.

Scipanov, Lucian Valeriu, and Valentin Costinel Totir. 2023. "Nevoia de adaptare a tacticilor navale la evoluția tehnologică – drone și platforme port-drone", *Gândirea Militară Românească* (nr. 3). doi:10.55535/GMR.2023.3.

Venegas-Andraca, Salvador E., Marco Lanzagorta, and Jeffrey Uhlmann. 2015. "Maritime applications of quantum computation." *OCEANS 2015 - MTS/IEEE Washington.* doi:10.23919/OCEANS.2015.7404356.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

Preliminary considerations on China's international cooperation in cyber security: legislation, competent authorities, and challenges

Andreea-Maria PIERȘINARU, Ph.D. Student*
*National University for Political and Administrative Studies (SNSPA)
e-mail: andreea_piersinaru@yahoo.com

Abstract

This article addressed general issues regarding the Chinese legislative framework, competent authorities, China's strategic objectives and the challenges in terms of international cooperation in the field of cybersecurity. The main objective of the research is to identify the actors involved in ensuring China's cybersecurity, describe their responsibilities and correlate them with Chinese cyber-security legislation and China Cyber Security Cooperation Strategy. This study traces preliminary considerations for future in-depth analyses of the impact of China's actions in the field of international cybersecurity.

Among the main findings of the study the aspects briefly identified were related to the influences of the policies and narratives of the Chinese Communist Party presented in China's International Cyber Security Cooperation Strategy, as well as to the fact that, despite China's intention to become a cyber power, open to cooperation, international reactions are quite reluctant due to allegations of cyber espionage and domestic surveillance problems existing at the national level, among others.

Keywords:
China; cyber security; cyber sovereignty; cyber espionage; international cooperation; cyber superpower.

Article info
Received: 10 May 2024; Revised: 10 June 2024; Accepted: 13 June 2024; Available online: 5 July 2024

Citation: Pierșinaru, A.M. 2024. "Preliminary considerations on China's international cooperation in cyber security: legislation, competent authorities, and challenges". *Bulletin of "Carol I" National Defence University*, 13(2): 121-141. https://doi.org/10.53477/2284-9378-24-24

Cybersecurity has become an essential part of states' foreign and security policy, due to accelerated globalisation and digitalisation. As one of the world's largest economies and technological powers, China has created a comprehensive strategy for international cooperation in cybersecurity. In recent years, China has stepped up its efforts to participate in global discussions and partnerships, multilateral cooperation being the key to addressing international cyber challenges.
In the reviewed literature some studies approach the Chinese legislative framework regarding cyber security historically and others analytically from the perspective of international cooperation.
Thus, relevant studies on the evolution of cybersecurity legislation in China include Rogier Creemers's study which provides an in-depth analysis of Chinese cybersecurity legislation.

Since the late 1990s, China has adopted a policy of "informatization" – or 信息化 (xìn xī huà), which includes the use of digital technology in economic, social and governmental activities. This policy evolved with the establishment in 2014 of the Central Leading Group for Cybersecurity and Informatisation, chaired by President Xi Jinping. Following this step, during the Xi administration, the "Cyber Power Strategy" or "网络强国战略" (Wǎngluò qiángguó zhànlüè) was developed, with the primary aim to improve China's technological capabilities and modernize state governance, including projects such as judicial informatization and the social credit system (Creemers 2023).

Another landmark study in the reviewed literature is Meirong Guo's "China's Cybersecurity Laws, Their Relevance to Critical Infrastructures and the Challenges They Face". His study brings a new interpretation to the Cybersecurity Law adopted in 2016, which from his perspective was not effectively implemented because cybersecurity was integrated into several laws, or administrative regulations already in place at the departmental level and the law lost consistency. Guo also points out that the People's Republic of China did not have specific legal regulations for cybersecurity before the adoption of the Cybersecurity Law in 2016; nevertheless, he stresses the importance of China's participation in international cooperation in cybersecurity to formulate international technical standards and deal with global cyber threats (Guo 2018).

In this context, China is committed to building extensive cooperative partnerships with all participants of the international community, developing dialogue platforms, and promoting a fair cybersecurity framework for all (MFA CN 2017). China has adopted this approach in its cooperation with ASEAN and the Shanghai Cooperation Organization on network and information security emergency response.
In all normative papers and Chinese leaders' speeches, China declares itself open to cybersecurity cooperation, demonstrating this interest through active participation in World Summits on Information Society and other international or regional cybersecurity-related conferences. China hosted the first World Summit

on Cybersecurity, which was organised by the EastWest Institute in Dallas. This event is mentioned by Chinese leaders in all cybersecurity-related public presentations to position China as a leader in the field and one of the initiators of international cybersecurity dialogue (Chinese Embassy in the UK 2011). China also states that it supports a multilateral, democratic and transparent global internet governance system (MFA CN 2023) and includes supporting the United Nations in its leadership role in global digital governance and rulemaking, stressing the need for an open and fair approach to cyber governance.

Another pillar of China's strategy is cooperation in research and development to enhance cybersecurity through industrial and academic partnerships. This includes collaborating with international research institutions and universities (Zhang, et al. 2022). In this context, China announced, in 2017, a project to 4 to 6 world-renowned cyber security institutes by 2027. These institutes will have the main objectives of training professionals in network security, conducting relevant academic research and cooperation with companies and governmental departments. One of the major objectives of these institutes is international cooperation, which includes the training of key academic staff abroad and the development of academic research collaboration within international consortia (Chinese Ministry of Education 2017).

According to the study published in 2021 by the Center for Security and Emerging Technologies, China established the National Cyber Security Center (NCC) in Wuhan[1], which includes seven research, talent development and entrepreneurship centres. NCC is home to two laboratories focused on governmental cybersecurity research and an incubator to support innovation in the private sector. (Fig.1.) This centre is supported from the highest levels by the Chinese Communist Party (CCP) and aims to reduce dependence on foreign technologies and promote national innovation (Cary 2021).

[1] Video about NCC in Chinese language : https://www.bilibili.com/video/BV1Vz411z7gT/?t=0h0m54s

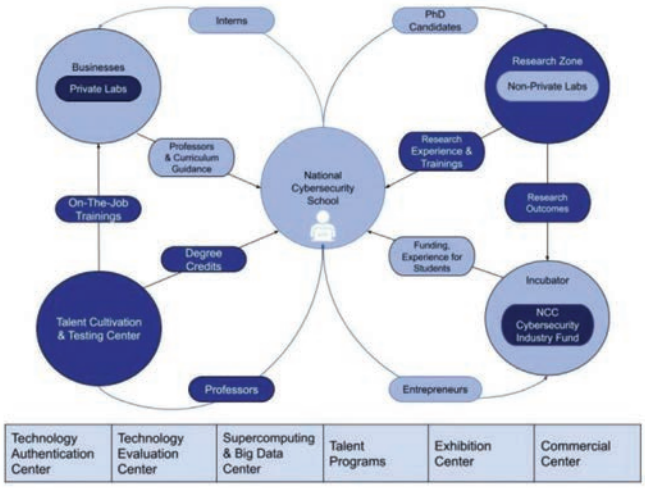

Figure No. 1 National Centre for Security and Emergent Technologies (Cary 2021)

Price Waterhouse Cooper (PWC) notes in a report published in 2023 that, despite public openness to cybersecurity cooperation, international cooperation norms are affecting China's domestic cybersecurity policy, forcing Beijing to implement strict regulations and laws to manage data flows and protect critical infrastructure (PwC Indonesia 2023).
Despite its efforts to become a cyber superpower, China faces significant challenges, such as accusations of cyber espionage and concerns about its domestic methods of surveillance and information control (Julian 2021).

Given China's legislative developments in cybersecurity but also its strategic goal of becoming a cyber superpower during the Xi administration, an introductory study on China's current legislative outlook on cybersecurity was deemed appropriate. The research will include a brief overview of the structures that ensure cybersecurity at the national level given that these were not identified in a unified way in the literature reviewed, but only in the text of the Chinese Cybersecurity Law. Finally, the perspective of the cyber security cooperation strategy and the challenges in implementing the objectives will be briefly analysed.

Methodology and Research Limitations

This study aims to identify the preliminary considerations regarding China's legislation and strategy in cybersecurity and their effects on international cooperation on cybersecurity. This research hypothesises that China's desire to protect its cyber sovereignty and strengthen its position as a cyber superpower has a significant impact on international cybersecurity cooperation. Thus, the following research question emerges: *How does China's cybersecurity legislation affect cooperation with other states?*
In the testing of the hypothesis, quantitative methods were used for data collection and analysis: secondary data analysis (for literature) and content analysis (for legislative texts). Secondary data analysis involves finding answers to new research questions using data that has already been collected from other studies (Fulton Library n.d.).

The article is a brief introduction to China's cybersecurity, which is limited to presenting the most important aspects, from the author's perspective, of the China Cyber Security Act, but also of the Chinese International Cooperation Strategy, as well as identifying some of the challenges that the Chinese Government has in achieving its objectives of international cooperation in the field of cyber security. These preliminary considerations will also refer to the main tasks of the competent authorities dealing with the implementation of the action plan of the cybersecurity strategy according to the law.

All these might open new research opportunities in the field, by in-depth studies using other research methods, which due to the constraint of time, could not be

developed in this article. The elements presented in the study can thus be used as a reference or starting point for future in-depth analyses conducted by researchers interested in the topic, as well as by experts in policy and strategy development in China's international cybersecurity cooperation.

The article is structured into two main sections preceded by a short introduction and this methodology is accompanied by the limits of research. At the end, there are underlined a series of conclusions. The first section is devoted to a brief presentation of the structure of the state apparatus dealing with cybersecurity in the People's Republic of China and the legislative framework on cyber security. As far as the legislative framework is concerned, only China's Cyber Security Act has been examined.

The second section of the article is an introduction to the Strategy of the People's Republic of China for International Cooperation in the field of cybersecurity and the challenges in achieving the objectives set out in the strategy. Regarding China's challenges in achieving the objectives set out in the strategy of international cooperation, three cases of Chinese cyber-spying-related groups were analysed: APT10, APT 31 and APT41.

The findings of the study highlight the importance of the topic and the need to conduct more studies in the field of cybersecurity, especially on the perspectives that come from China for a better understanding of the prospects of international cooperation in cyberspace security.

Brief Overview of the Structure of the State Apparatus in Charge of Cybersecurity in the People's Republic of China and the Legislative Framework for Cybersecurity in China (gov.cn)[2]

To understand the structure of the state apparatus in charge of cyber security in China, it is necessary to remember that in an autocratic state like China, no governmental structure is independent or functions on its own without the impact of the strategies and narratives of the Chinese Communist Party and its leaders.

So, given this pyramidal structure, the Central Commission for Cyberspace Affairs (CCCA) of the Central Committee of the Communist Party of China is the main body responsible for implementing cyber security policies, founded in 2018 following the 2014 efforts initiated by the Cyber Security and Information Security Working Group. The CCAC is responsible for coordinating the activities of the following subordinate agencies and entities, which communicate and collaborate: Cyberspace Administration

[2] The law will be analysed as a whole.

(CAC), Public Opinion Information Center, China DNS Registry managed by China Internet Network Information Center (CNNIC), CNCERT (National Cybersecurity Incident Response Center), TC260- China National Information Security Standardization Technical Committee, and China Cybersecurity Association. The effective coordination of these agencies and entities is essential for implementing cybersecurity policies and promoting integrated cyberspace governance in China. Reflecting the strategic importance that the Communist Party of China gives to cyber control and cybersecurity, Xi Jinping, together with Li Qiang and Cai Qi, chairs the CCAC.

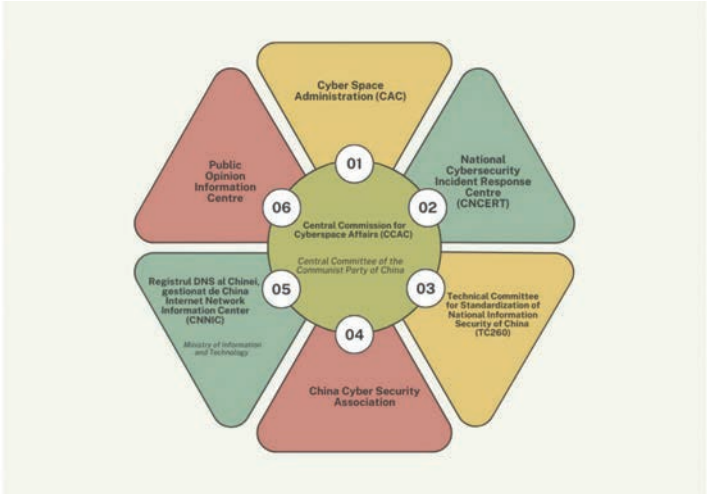

Figure No. 2 Structure of the state apparatus in terms of cyberspace and cybersecurity in China[3]

[3] Personal interpretation following China's Cyber Security Law.

The following diagram, designed by the author, presents the structure of the state apparatus in charge of cyberspace and thus cybersecurity in China for a more precise understanding of the above. After the presentation of the diagram, a brief overview of the tasks of each institution will follow.

The Cyberspace Administration (CAC) is China's national cyber regulation agency. In addition to national cyber regulation, the CAC also deals with cyber censorship and sets specific policies. This entity is vital to China's cyber governance system as it is responsible for overseeing and controlling the internet to ensure that all content published on the internet meets the requirements of the Communist Party of China (CCP). The CAC, through its cyberspace management responsibilities, also sets rules for technology companies and monitors online communication to prevent the spread of information deemed dangerous or destabilizing to the state (CAC n.d.).

In 2019, CAC launched a project to eliminate pornography, violence, gambling, fraud, superstition, parody, threats and the spread of "inappropriate lifestyles" and "bad popular culture" that imposed a high level of online content control, favouring the online positive image of the CCP (Xinhua 2019).
In the same year, CAC issued a regulation stipulating that any behaviour

deemed to be considered a cybercrime will be added to the social credit system – the cyber criminals' punishment being the impossibility of accessing bank credits or other citizen facilities (Dandong 2019).

Another important institution of the state apparatus in the field of cybersecurity is the *Public Opinion Information Centre,* which brings together government efforts of censorship and surveillance of information on the internet, and monitors, and analyses public opinions on the internet. There are references to this centre, only in the text of the law. The study has so far not yet identified any other sources to present or discuss the activities of the Centre.

The structure responsible for managing the DNS Registry of China is the *China Internet Network Information Centre (CNNIC)*. Regarding the management and operation of the top-level domain (TLD), CNNIC is responsible for the ".cn" domains. This includes overseeing domain entries and ensuring that the DNS infrastructure associated with these domains works well. On the other hand, CNNIC has an important responsibility in protecting personal data and cybersecurity: ensuring the security of the DNS infrastructure and protecting users' data. This includes establishing security rules to prevent abuse and cyber-attacks, as well as managing WHOIS data, which contains information about domain owners. To comply with international standards in domain name management, CNNIC works with ICANN and other international internet management organizations. This includes active involvement in global policy processes and implementation of international decisions in China's domain system. Finally, CNNIC encourages the creation and use of internationalized domain names (IDNs), which allow the use of Chinese characters in the domain name. This would facilitate internet access in the native language of Chinese speakers (CNNIC n.d.).

CNCERT (National Cybersecurity Incident Response Center) oversees cyber threat prevention efforts, anticipating and blocking potential attacks before they affect national networks or critical infrastructure, and ensures the fullest and fastest possible recovery after handling an incident, thus restoring affected services and systems. CNCERT works with similar teams in other countries and with international organisations to manage cybersecurity incidents that may affect various countries. CNCERT is a member of the Forum of Security Incident Response Teams (FIRST) and one of the founders of the Asia Pacific Computer Security Incident Response Group (APCERT). CNCERT informs the public and organizations about cybersecurity risks and best practices for protection and collects and distributes data about security vulnerabilities through the China National Vulnerability Database (CNCERT/CC n.d.).

The main objective of *China's Technical Committee for National Information Security Standardization (TC260)* is to create national standards for cybersecurity. This committee is responsible for the establishment and maintenance framework of

standards governing various aspects of cybersecurity in China, such as network products and service security, critical information infrastructure protection and cybersecurity incident management. TC260 works with other government entities and private sector organizations to ensure that cybersecurity standards are consistent and effective. This involves non-government legal entities such as national and international companies' contributions. According to public data published on the organization's official website, TC260 has published about 300 technical cybersecurity standards so far and continues to improve them to meet the ever-changing needs in cybersecurity (TC260 n.d.).

The Cybersecurity Association of China (CSAC) coordinates public-private policies between the private, public and academic sectors. CSAC influences Chinese cybersecurity legislation through its activities. This includes promoting industry best practices and security standards. CSAC argues that the Chinese origins of goods and services improve the country's security, so it recommends using goods and services offered by Chinese companies over foreign competitors. The association works to promote and defend China's cybersecurity interests internationally by participating in discussions and negotiations on international cybersecurity standards and legislation (Cyber Security Association of China (CSAC) n.d.).

China's Cyber Security Act (gov.cn 2016), approved in its first format on 7 November 2016 and entered into force on 1 June 2017, constitutes the legislative frame for cyber security in China. The general objective of the law is to ensure network security, cybersecurity, national security and public interests, protect the rights and legitimate interests of citizens, and promote healthy economic and social digitalisation. The state provides measures to monitor, defend and manage network security risks and threats coming from within and outside China's borders, protects critical infrastructures from potential attacks and menaces, provides penalties for cybercrimes, and is meant to assure order and security in cyberspace. Another important aspect mentioned in the law concerns data localization. In China, the law requires essential personal data and other personal data collected from cyberspace to be stored within the country. Critical infrastructure operators are required to ensure this by law. Article 2, Chapter 1 states:

This Law shall apply to data processing activities, security supervision and regulation of such activities within the territory of the People's Republic of China. If data processing outside the territory of the People's Republic of China harms national security, public interests or the legal rights and interests of persons or organizations in the People's Republic of China, legal liability shall be investigated in accordance with the law. (NPC.GOV.CN 2021)

In addition to the Cybersecurity Law, the Data Security Law was published (2021) that imposes new rules for enterprises interacting with Chinese citizens both at home and abroad, and the influence of domestic legislation migrating to foreign space with implications for China's international cybersecurity cooperation is observed.

China's cybersecurity law also provides perspectives on international cooperation, governance of cyberspace, research in network technology and setting standards for combating cybercrime. It also stresses China's commitment to building a secure and open cyberspace as secure that reflects the values of transparent, democratic and multilateral governance, as stipulated in the text of the law (gov.cn 2016). In addition, the Chinese Government is encouraging the adoption of various skills training policies in the field of cybersecurity, encourages international talent exchanges and supports companies and research institutions to participate actively in the national network security standards' design. Regarding this process, the China Cyber Space Administration (CAC) is responsible for authorizing and testing all network products before they are marketed, ensuring that they meet the strict security standards imposed nationally (Cyberspace Administration of China 2017).

On 12 September 2022, major amendments to the China Cyber Security Act were introduced. These amendments introduced new fines and penalties for breaches of general network security rules. In addition, the administrative penalties for cybercrimes committed by critical infrastructure operators have been reviewed and several administrative sanctions and prohibitions for other illegal acts not mentioned in the previous administrative legislation have been added. The amendments to the Cyber Security Act underline China's commitment to strengthening cybersecurity and responding dynamically to emerging challenges in the field (gov.cn 2016).

Thus, the cybersecurity legislative framework as well as the CACC's objectives, through all subordinate agencies and entities, are meant to strengthen China's ability to control and regulate the national cyberspace. These structures not only enforce policy but also influence the cyber landscape, targeting both domestic and international audiences. It is important to reflect on the role these structures play in promoting cyber security as well as censoring online content, with a significant impact on freedom of expression and human rights in the digital age, especially when references are made to China's international cooperation in the field of cyber security. The following section will discuss some relevant introductory issues and themes, from the author's perspective, on China's strategy for international cybersecurity cooperation.

People's Republic of China's Strategy for International Cybersecurity Cooperation – Short Presentation of the Key Points and Challenges in Achieving the Strategy's Goals

China's Strategy for International Cooperation in Cyberspace (launched in 2015 but updated on a regular basis - last update: 2022) (Xinhua News Agency 2017) is in line with President Xi Jinping's belief that countries are interconnected, have common interests and must cooperate to achieve common goals of maintaining peace and security. Therefore, promoting openness and cooperation in cyberspace are common

interests, but also responsibilities of the entire international community.
The Chinese model of international cooperation (as it appears, officially, in all normative acts and especially in the speeches of Chinese leaders) is the promotion of a new kind of cooperation in international relations: *win-win*. This model is also present in the Chinese strategy for international cooperation in cyberspace.

In the text of the strategy, the phrase 网络强国 (*wǎngluò qiángguó*) is frequently found, which can be interpreted as an expression of the main objective of the strategy: the Chinese pathway to become a "cyber superpower" or "a national power in cyberspace", and among the secondary objectives of the strategy there is identified the need for a state to control and govern its own cyberspace (Xinhua News Agency 2017).

There are six objectives of the Chinese Strategy for International Cybersecurity Cooperation:

1. Defending national sovereignty and security in cyberspace.
2. Developing a system of new international rules and norms for cyberspace.
3. Promoting fair Internet governance: it advocates for fair and equitable international Internet governance.
4. Protecting the legitimate rights and interests of citizens: it focuses on protecting the rights and interests of individuals in cyberspace.
5. Promoting cooperation in the digital economy: it aims to strengthen cooperation in the digital economy at the international level.
6. Building relevant platforms for cultural cyberspace exchange: it emphasizes the importance of cultural exchanges in cyberspace (Xinhua News Agency 2017).

The strategy states that the Chinese state promotes international cooperation based on the principles stipulated in the UN World Summit on Information Society (WSIS) format: building an inclusive, people-centred and development-oriented information society (Sustainable Development 2016).

China's concrete initiatives in international cooperation in cyberspace, according to the strategy's action plan, include (Xinhua News Agency 2017):

- Promoting fair Internet governance: China has advocated for fair and equitable international Internet governance.
- Deepening cyber cooperation with other countries: China has worked to deepen cyber cooperation with the UN, US, Russia and the EU (joint activities, expert-level meetings and development of cooperation projects through digital economy initiatives).
- Cyberspace trade rule formulation and policy coordination: China has expressed support for the formulation of cyberspace trade rules and effective policy coordination between states.

- Enforcement of international law in cyberspace: China aims to enforce international law in cyberspace to strengthen its position in the global digital order.
- China will continue to organise the annual Wuzhen Summit (World Internet Conference) and other international conferences and forums: the Conference on Interaction and Confidence Building Measures in Asia (CICA), the Forum on China-Africa Cooperation (FOCAC), the China-Arab States Cooperation Forum, the Forum of China and the Community of Latin American and Caribbean States and the Asian-African Legal Consultative Organization.
- Discussions and consultations in the China-Japan-Korea format, ASEAN Regional Forum and Boao Forum on cyber policies will continue.
- China is promoting cooperation on cybersecurity within the Shanghai Cooperation Organization (SCO) and BRICS.

Nevertheless, in terms of advanced technologies, China aims to become a world leader in the field. This goal has a significant impact on global cyberspace. The article will further highlight China's strategic goals in the development of processors and other high technologies, as well as their effects on global cyberspace. To become a world leader in advanced technologies, China is advancing in reducing dependence on foreign technology products, especially those coming from the United States and other Western countries. This refers to the creation of domestic software and processors to replace imported products. So, an important step in this endeavour was to ban the use of Intel and AMD processors on government computers and servers (Zulhusni n.d.).

The Chinese government is investing substantially in emerging technologies such as artificial intelligence (AI), and *quantum computing*, among others. For example, China began building open-source RISC-V processors and launched quantum communications satellites. These processors are used in various industries, such as autonomous vehicles and artificial intelligence (Goswami 2023; Cheung 2023).

By exporting technology, its own standards, and promoting cyber sovereignty, China is seeking to increase its global influence. This also includes promoting the standards that support China's Internet governance model and active involvement in international standardisation organizations (Cary 2023). Thus, integrating Chinese technology into the vital infrastructures of other states can cause vulnerabilities, which can later lead to cyber espionage activities (Pleil 2023).

China's international cybersecurity cooperation strategy promotes the establishment of a world order in cyberspace, based on rules agreed upon by all members of the international community, highlights the need for expanded partnerships in cyberspace, supports international cooperation in combating cyber terrorism and cybercrime, and promotes reform of the global governance system of the internet. (Xinhua News Agency 2017).

Within the text of the strategy, special attention is attributed to public opinion and its presence in the online space. It is considered that the online presence of public opinion has become the most important task of Chinese propaganda, and as such, the need to maintain a "positive energy" online and offline is emphasized to "keep things under control" as mentioned in the text strategy (Xinhua News Agency 2017). Positive online advertising must be stronger than ever so that the Party's ideas always become the strongest voice in cyberspace. An important feature of China's cyber security is the Chinese government's strict control and supervision of the internet, as reflected also in Art.12, Chapter 1 of the PRC Cyber Security Law:

Any person and organization using the internet must comply with the Constitution and laws of the country, respect public order and social morality; must not jeopardize cyber security and may not use the internet to engage in activities that endanger national security, national honour and national interests; must not undermine national sovereignty, overthrow the socialist system, incite separatism, break national unity, support terrorism or extremism, promote ethnic hatred and ethnic discrimination, disseminate violent, obscene or sexual information, create or circulate false information to disrupt economic or social order or information that violates the reputation, confidentiality, intellectual property or other legitimate rights and interests of others and other such acts.

To ensure the successful implementation of Art.12, Chapter 1 cited above, China has developed the control and monitoring system known as the "Great Firewall". It involves monitoring users' online activity and blocking access to numerous international websites. By preventing the spread of information considered subversive or harmful, this centralised and comprehensive method seeks to maintain political and social stability. China monitors and censors the content that appears on the internet: it blocks or censors sensitive information about the government or human rights, users are monitored in detail for all their online activities, including browsing history, messages and posts on social networks; personal information such as phone numbers or identity cards are collected by internet service providers; Chinese websites are obliged to censor content deemed inappropriate, as well as to collaborate with authorities to track and report suspicious activities (Stanford n.d.).

Regarding international cooperation with other regions, China uses the BRICS platform (Brazil, Russia, India, China and South Africa, Iran, Egypt, Ethiopia and the United Arab Emirates) to promote cooperation in the field of cybersecurity. China has sought within this group to collaborate on joint projects to combat cybercrime and improve information security. In a broader approach, these efforts are part of a goal linked to building a network of alliances with developing countries and counterbalancing Western influence on global internet governance (Li 2018).

China has also made significant steps in cybersecurity cooperation with Thailand to create a safer cyberspace and protect citizens from malicious activities. This

collaboration includes information sharing, best practices and technological innovations to combat cyber threats (Saffa 2024).

In East Asia, countries such as India, Vietnam, Japan and South Korea consider China an aggressive cyber power, despite China's efforts to position itself as a leader in cyber cooperation through BRICS. These nations are concerned about China's ability to exploit cyber power for surveillance and espionage purposes, a situation that has generated regional tensions and spurred initiatives to strengthen cybersecurity (Wagner 2019).

Following this context, Vietnam and Japan have signed a cybersecurity agreement to combat China's aggressive cyber-attacks. This agreement is a consequence of both countries' concerns about China's cyber activities in the Indo-Pacific area (Yamaguchi 2021). Nonetheless, in January 2024, Vietnam discovered that China-supported advanced persistent threat groups (APTs), such as APT31, APT41, Grayling, Mustang Panda and SharpPanda, were involved in cyber espionage activities on Vietnamese governmental agencies. Japan has also intensified cyber defence cooperation with the United States, Australia and others, participating in NATO cyber exercises and signing cyber security agreements, in addition to that with Vietnam Singapore and Indonesia. Japan has regularly protested the presence of the Chinese Coast Guard near the Japan-controlled, but China-claimed Senkaku Islands, indicating a constant concern about China's cyber and military activities in the region (Truong 2024).
Unlike East Asian states, which are reluctant to cooperate on cybersecurity with the PRC, the Russian Federation and the Solomon Islands, as well as Thailand, are open to cooperation with China and have already taken steps in this direction.

As for the relationship with the Russian Federation, since 2017, the Chinese Cyber Space Administration (CAC) has been working with Roskomnadzor, the Russian internet regulatory and censorship authority. This cooperation demonstrates that the two states share similar views on internet control and surveillance. It is also part of a broader effort to promote cyber sovereignty and counter Western influence in terms of governance of international cyberspace (Kremlin 2017).
In 2023, China and the Solomon Islands signed a cooperation agreement in the fields of cybersecurity and police. This agreement is part of China's efforts to expand its influence in the South Pacific by providing technical assistance and training in cybersecurity (Smith 2023).

Regarding cooperation in the field of cybersecurity between China and the EU, although there have been several discussions on cooperation on cyberspace between the EU and China, so far, there is still no real cooperation between the Union and China. In the negotiating process on cooperation, efforts have been for cooperation in the digital field, including the development of a common framework for the governance of electronic data (EIAS 2023). These efforts are the result of mutual

recognition of the potential benefits of collaborating in combating cybercrime, promoting digital commerce and protecting critical infrastructures (European Commission 2019).
The difficulty of China-EU cooperation is also caused by China's malicious cyber activities, carried out by state actors against the EU, which will be detailed further in this section. As a result of these incidents, the EU has asked China in 2021 to take adequate measures to stop these activities. (European Council 2021).

Although in 2015, during the Obama administration, the US and China reached an important agreement by which they pledged to refrain from cyber economic espionage in both states (The White House 2015), China is still involved in numerous cases of cyber espionage targeting government and private companies. The APT10, APT31 and APT41 groups are recognized for their complex attacks on critical infrastructure and theft of intellectual property in the US and Europe. The following are some cases of Chinese cyber espionage that have a major impact on China's international cooperation in the field of cyber security and represent another facet of the challenges China faces in international cybersecurity cooperation.

The Chinese state-sponsored cyber espionage group, APT10, also known as Cicada or Stone Panda, has been active for over a decade, with the main objective of spying on technology and defence companies in the US and Europe. The "Operation Cloud Hopper" (2014-2018) campaign is an example of this regard, targeting the Managed Service Providers (MSPs) in several countries, such as the United States, Japan, Canada and Australia. APT10 penetrated MSP customer networks and stole technology and business secrets (CYWARE 2022; Vijayan 2017).

Several cyber security reports and official sources have confirmed the link between China's State Security Ministry and the APT10 cyber-attack group. The first report was made in 2018 by an anonymous group of researchers named Intrusion Truth who published a report about Zhu Hua and Zhang Shilong as members of the APT10 group and linked to China's State Security Ministry. Nevertheless, cybersecurity company CrowdStrike has confirmed this fact, too (O'Donnell 2018). The U.S. government subsequently accused this group of infiltrating the networks of more than 45 US technology companies and government agencies and stealing private data, including information about U.S. Navy personnel (Office of Public Affairs 2018). In December 2018, the United Kingdom and its allies publicly revealed that the APT10 group acted on behalf of China's State Security Ministry (MSS) to launch large-scale cyber campaigns targeting intellectual property and commercial sensitive data in Europe, Asia and the United States (National Cyber Security Centre 2018).

Besides APT10, other hacking groups are believed to be linked to China's Ministry of State Security, such as APT31 and APT41.
APT31 (Zirconium, Judgment Panda, Bronze Vinewood, Red Keres) is a hacking group notorious for stealing sensitive data and intellectual property. This group

has been involved in cyber-attacks targeting journalists, politicians, academics and governmental institutions, as well as security companies and public institutions. The US and UK have claimed that APT31 is a weapon of China's Ministry of State Security - used by the Security Department of Hubei Province, Wuhan and was developed to detain critics of the Chinese regime and compromise government institutions (gov.uk 2024; US Department of the Treasury 2024).

In 2021, APT31 attacked the UK Electoral Commission's systems, obtaining the personal data of around 40 million voters (Yerushalmy 2024) and was involved in attacks on critical US infrastructure (defence and energy). APT31 was accused, also of hacking Microsoft Exchange email server software and the personal emails of campaign staff working for Joe Biden in 2020 (Office of Public Affairs 2024).
As a result of these attacks, the US and UK governments have sanctioned individuals and organizations related to the APT31 group, including Wuhan Xiaoruizhi Science and Technology Company Limited, which facilitated the MSS cyber operations (UK GOV 2024; US Department of the Treasury 2024).

Another Chinese cyber-espionage group, APT41, also known as Double Dragon, combines state-sponsored espionage with cybercrime for financial purposes. This group has worked in many industries such as telecommunications, high technology and health (Fraser, et al. 2019).
A high-profile case of APT41's actions is the attack that targeted the software company NetSarang in 2017. Back then, the group injected malicious code into a software update package that was signed with a legitimate NetSarang certificate. Hundreds of businesses around the world were affected by the attack (Mandiant 2022).

The United States Department of Justice filed charges against seven APT41 members in 2020 for cyber-attacks targeting technology, telecommunications and health companies, as well as for theft of intellectual property and sensitive data (Office of Public Affairs 2020). Nonetheless, in March 2021, in the case of the cyber-attack that targeted Microsoft's email software, attackers used a previously undetected vulnerability to gain remote access to email boxes. NATO, the European Union, Australia, New Zealand and Japan have officially attributed the attack to state-sponsored Chinese actors, the group known as Hafnium (GMF 2021).

Given the above, one can see the complexity of assuming the fulfilment of all the objectives set out in China's strategy for international cooperation in the field of cybersecurity. China claims that every nation has the right to have control over its national cyberspace and uses this discourse internationally intending to protect national interests and the state from external influence, due to geopolitical conflicts with the United States and other Western countries (Shen 2016). At the opposite pole, to ensure an open and free cyberspace, the European Union is advocating a multi-stakeholder cyber governance model, such as public-private cooperation with NGOs and international academic institutions.

Conclusions

The study responded to the research question launched following the hypothesis and shows that China's desire to protect its cyber sovereignty and to strengthen its super cyber power position, as well as domestic legislation based on both internal and external monitoring of databases belonging to Chinese citizens, have a major impact on the strategy of international cyber security cooperation. Nonetheless, challenges arise in meeting the objectives proposed in the strategy of international cooperation in the field of cybersecurity, such as cyber espionage carried out by Chinese state actors.

China's goal of protecting critical infrastructures and personal data of Chinese citizens is highlighted by the China Cyber Security Act, the Personal Data Protection Act and the recent amendments to the two laws. Although these acts were essential to creating an atmosphere of international collaboration, along with the International Cyber Security Cooperation Strategy, some countries in East Asia, the US and Europe have expressed concern about China's objectives, accusing China of cyber espionage and excessive surveillance.

China's desire to protect its cyber sovereignty is a key component of its international cyber security cooperation strategy. China is seeking to strengthen its position as a cyber superpower and to protect its interests by implementing a transparent and multilateral Internet governance system. Contrary to China's desire, many states and international organizations do not trust China's efforts to build a global Internet governance system. Accusations of using technology for internal surveillance, regularly conducting cyber-attacks as a state actor or concerns about domestic intelligence monitoring and control practices have affected China's objectives in international cybersecurity cooperation, as potential partners are reluctant to the Chinese government's intention of openness and sincere collaboration.

In this brief introductory study, in addition to references to the legislative framework on cybersecurity in China, a presentation was made of the governmental structures dealing with cyberspace security in China. The study concluded that all those structures are interdependent and coordinated hierarchically by the Central Commission for Cyber Space Affairs (CCAC) of the Communist Party of China. Therefore, the CCP committee governs the activities of cyber-related agencies and entities (CAC, CNNIC, CNCERT, TC260 and CSAC) and traces the priority lines for the implementation of strategies in the field.

This hierarchical structure influenced by the CCP has also caused the reluctance of foreign countries to identify increasing threats from Chinese state-controlled groups, such as APT10, APT31 or APT41, which mainly aim at cyber espionage of critical and national-interest infrastructures in areas such as military, telecommunications, health or energy, according to the cyber security reports mentioned throughout the article.

In conclusion, China is in an extensive process of demonstrating its cyber superpower capacity, to contribute to the creation of a safer cyberspace, but with the clear objective at the same time of maintaining a secure cyberspace at the national level that positively reflects all the actions of the CCP.

References

ABC News. 2015. *US and China Reach Agreement to Stop Commercial Cyber Espionage.* https://abcnews.go.com/US/us-china-reach-agreement-stop-commercial-cyberespionage/story?id=34041002.

Atlantic Council. 2023. *The 5×5—China's cyber operations.* https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/.

CAC (Cyberspace Administration of China). n.d. **中央网**络安全和信息化委员会办室. https://wap.cac.gov.cn/.

Carolan, Ciara. 2024. *Europe and Belgium are 'unresponsive' in the face of Chinese cyber-attacks, says hacked MP.* https://www.brusselstimes.com/983253/europe-and-belgium-are-passive-in-the-face-of-chinese-cyber-attacks-says-hacked-mp.

Cary, Dakota. 2021. *China's National Cybersecurity Center. A Base for Military-Civil Fusion in the Cyber Domain.* https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/.

—. 2023. *Community watch: China's vision for the future of the internet.* https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/.

CCTV News. 2023. *Strategy for International Cooperation in Cyberspace.* https://news.cctv.com/2023/11/07/ARTILliq1FlQi0B7msdoKsBn231107.shtml.

Cheung, Sunny. 2023. *Examining China's Grand Strategy For RISC-V.* https://jamestown.org/program/examining-chinas-grand-strategy-for-risc-v/.

Chinese Embassy in UK. 2011. *China's Perspective on Cybersecurity.* http://gb.china-embassy.gov.cn/eng/ambassador/dsjhjcf/2011lr/201106/t20110602_3386103.htm.

Chinese Ministry of Education. 2017. *Management Measures for the Demonstration Project of Building a First-Class Cibersecurity College.* http://www.moe.edu.cn/srcsite/A16/s3342/201708/t20170815_311176.html.

CNCERT/CC (National Computer network Emergency Response technical Team/Coordination Center of China). n.d. **国家互**联网应急中心. https://www.cert.org.cn/publish/main/34/index.html.

CNNIC (China Internet Network Information Center). n.d. **中国互**联网络信息中心. https://www.cnnic.com.cn/.

Consiliul de Stat al Chinei. 1994. *Regulations of the People's Republic of China on Computer Information System Security Protection.* https://www.gov.cn/gongbao/content/2011/content_1860849.htm.

Creemers, Rogier. 2023. *Cybersecurity Law and Regulation in China: Securing the Smart State.* https://brill.com/view/journals/clsr/6/2/article-p111_001.xml.

Cyber Security Association of China (CSAC). n.d. 中国网络空间安全协会. https://www.cybersac.cn/.

Cyberspace Administration of China. 2017. 关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告 *[Announcement on the release of the "Catalogue of Critical Network Equipment and Network Security Special Products (First Batch)"].* https://www.cac.gov.cn/2017-06/09/c_1121113591.htm.

CYWARE. 2022. *APT10: A Chinese Threat on a Global Espionage Mission.* https://cyware.com/resources/research-and-analysis/apt10-a-chinese-threat-on-a-global-espionage-mission-56fe.

Dandong, Han. 2019. *Legal Daily.* http://epaper.legaldaily.com.cn/fzrb/content/20190729/Articel04004GN.htm.

EIAS. 2023. *EU Digital Dialogue and Cooperation with China: The Way Forward?* https://eias.org/publications/op-ed/eu-digital-cooperation-with-china-the-way-forward/.

European Commission. 2019. "EU-CHINA - A Strategic Outlook." https://commission.europa.eu/system/files/2019-03/communication-eu-china-a-strategic-outlook.pdf.

European Council. 2021. *China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory.* https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/#:~:text=We%20continue%20to%20urge%2.

Fraser, Nalani, Fred Plan, Jacqueline O'Leary, Raymond Leong Vincent Cannon, Dan Perez, and Chi-en Shen. 2019. *APT41: A Dual Espionage and Cyber Crime Operation.* https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation.

Fulton Library. n.d. *Quantitative Research Methodologies.* https://uvu.libguides.com/methods/quantitative.

GMF. 2021. *NATO, EU, and allies attribute email intrusion to Chinese state-backed hackers.* https://securingdemocracy.gmfus.org/incident/allies-attribute-email-hack-to-china-backed-hackers/.

Goswami, Namrata. 2023. *China Prioritizes 3 Strategic Technologies in Its Great Power Competition.* https://thediplomat.com/2023/04/china-prioritizes-3-strategic-technologies-in-its-great-power-competition/.

gov.cn. 2016. 中华人民共和国网络安全法_滚动新闻_中国网 *[Cybersecurity Law of the People's Republic of China].* https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.

gov.uk. 2024. *UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity.* https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity.

Guo, Meirong. 2018. "China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces." *International Journal of Critical Infrastructure Protection* vol. 22: pp. 139-149. doi:10.1016/j.ijcip.2018.06.006.

Handler, Simon. 2023. *Atlantic Council.* https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/.

Hmaidi, Antoni. 2023. *"Here to stay" – Chinese state-affiliated hacking for strategic goals.* https://merics.org/en/report/here-stay-chinese-state-affiliated-hacking-strategic-goals.

Julian, Nicholas. 2021. *United States' and China's Cybersecurity Policies: Collaboration or Confrontation?* https://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation.

Kremlin. 2017. *Russia and China Enhance Cybersecurity Cooperation.* https://www.kremlin.ru/events/president/news/55842.

Li, H. 2018. "BRICS and the Internet: Building a New Global Consensus." *International Affairs* 94 (5): 1125-1145.

Mandiant. 2022. *APT41 (Double Dragon): A Dual Espionage and Cyber Crime Operation.* https://www.mandiant.com/resources/reports/apt41-double-dragon-dual-espionage-and-cyber-crime-operation.

MFA CN (Ministry of Foreign Affairs of the People's Republic of China). 2017. *Ministry of Foreign Affairs Holds Briefing for Chinese and Foreign Media on President Xi Jinping's State Visits to Russia and Germany and Attendance at 12th G20 Summit.* https://www.fmprc.gov.cn/mfa_eng/topics_665678/2017zt/XJPDEDFWBCXGEODSECFH/201707/t20170704_703649.html.

—. 2023. *Proposal of the People's Republic of China on the Reform and Development of Global Governance.* https://www.fmprc.gov.cn/eng/wjbxw/202309/t20230913_11142010.html.

National Cyber Security Centre. 2018. *APT10 continuing to target UK organisations.* https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations.

NPC.GOV.CN. 2021. "Data Security Law of the People's Republic of China." http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html.

O'Donnell, Lindsay. 2018. *APT10 Under Close Scrutiny as Potentially Linked to Chinese Ministry of State Security.* https://threatpost.com/apt10-under-close-scrutiny-as-potential-chinese-ministry-of-state-security-contractor/137139/.

Office of Public Affairs. 2024. *Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians.* https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived.

—. 2020. *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally.* https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

—. 2018. *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information.* https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

Pleil, Helen. 2023. *Being a Cyberpower – China's Ambitions in Cyberspace.* https://www.techpolicy.press/being-a-cyberpower-chinas-ambitions-in-cyberspace/.

PwC Indonesia. 2023. *A comparison of cybersecurity regulations: China.* https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html.

Saffa, Azizah. 2024. *Thailand and China Strengthen Cybersecurity Cooperation.* https://opengovasia.com/2024/05/29/thailand-and-china-unite-for-cyber-resilience/.

Shen, Yi. 2016. "Cyber Sovereignty and the Governance of Global Cyberspace." *Chinese Political Science Review* vol. 1: pp. 81-93. https://doi.org/10.1007/s41111-016-0002-6.

Smith, J. 2023. *China and Solomon Islands Sign Security Pact.* https://www.theguardian.com/world/2023/apr/12/china-and-solomon-islands-sign-security-pact.

Stanford. n.d. *Free speech vs Maintaining Social Cohesion.* https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.

Sustainable Development. 2016. *World Summit on the Information Society (WSIS).* https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170.

TC260 (National Cybersecurity Standardization Technical Committee). n.d. 全国网络安全标准化技术委员会. https://www.tc260.org.cn/.

The White House. 2015. *U.S.-China Cyber Agreement.* https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/us-china-cyber-agreement.

Thomas, Nicholas. 2009. "Cyber Security in East Asia: Governing Anarchy." *Asian Security* 5 (1): 3-23.

Truong, Sylvie. 2024. *Chinese espionage campaigns and cyberattacks on critical infrastructure in Southeast Asia.* https://thereadable.co/chinese-espionage-campaigns-and-cyberattacks-on-critical-infrastructure-in-southeast-asia/.

UK GOV. 2024. *UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity.* https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity.

US Department of the Treasury. 2024. *Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure.* https://home.treasury.gov/news/press-releases/jy2205.

Vijayan, Jay. 2017. *China-Based Threat Actor APT10 Ramps Up Cyber Espionage Activity.* https://www.darkreading.com/cyberattacks-data-breaches/china-based-threat-actor-apt10-ramps-up-cyber-espionage-activity.

Wagner, B. 2019. "Cybersecurity in East Asia: Government Policies and Sectoiral Responses." *Journal of Cyber Policy* 4 (1): 55-72.

Xinhua. 2019. http://www.xinhuanet.com/yuqing/2019-01/04/c_1210030391.htm.

Xinhua News Agency. 2017. 网络空间国际合作战略 *[Cyberspace International Cooperation Strategy]*. http://www.xinhuanet.com/politics/2017-03/01/c_1120552767.htm.

Yamaguchi, Mari. 2021. *Japan, Vietnam Look to Cyber Defense Against China.* https://thediplomat.com/2021/11/japan-vietnam-look-to-cyber-defense-against-china/.

Yerushalmy, Jonathan. 2024. *China cyber-attacks explained: who is behind the hacking operation against the US and UK?* https://www.theguardian.com/technology/2024/mar/26/china-cyber-attack-uk-us-explained-hack-apt-31.

Zhang, Duanhong, Wenjia Ding, Yang Wang, and Siwen Liu. 2022. *Exploring the Role of International Research Collaboration in Building China's World-Class Universities.* https://doi.org/10.3390/su14063487.

Zulhusni, Muhammad. n.d. *China's new tech policies challenge Intel and AMD in a shifting landscape.* https://techwireasia.com/03/2024/chinas-tech-shift-what-it-means-for-the-future-of-intel-and-amd/.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Digital technologies used in the field of military transport

Major Ana-Maria MERLUȘCĂ, Ph.D. Candidate*

* "Carol I" National Defence University
e-mail: merlusca.maria@unap.ro

Abstract

Military transport as a sub-field of operational logistics ensures both the movement of forces from one location to another as well as their supply and support during military exercises or operations. Ensuring the transportation of materials to the fighting forces at the right time and place, as well as in the necessary quantity, is essential for the successful completion of missions. In this regard, during the planning process for force support, determinants such as destination, duration, distance, and the logistic support demand for the operation are taken into account. Technological evolution allows for the adoption of digital solutions in the logistics field, with the following benefits: reducing the risk of human losses, access to difficult locations, visibility over transported goods, and increased speed of response to logistic support requests.

The purpose of this article is to highlight a series of digital technology solutions applied in the field of military transportation. To write this article, a qualitative research strategy was applied to gain an in-depth understanding of the phenomena and processes related to military transport. The data collection technique used was the analysis of manuals, regulations, doctrines, articles published in journals and magazines, media content, websites of digital technology developers, and specialized books.

The conclusion of the article lies in highlighting the advantages of using robotic technology to ensure military transport.

Keywords:

transport; military; sustainment; digital solutions.

Article info

Received: 13 May 2024; Revised: 4 June 2024; Accepted: 14 June 2024; Available online: 5 July 2024

Citation: Merluşcă, A.M. 2024. "Digital technologies used in the field of military transport". *Bulletin of "Carol I" National Defence University*, 13(2): 142-150. https://doi.org/10.53477/2284-9378-24-25

Transport activities are carried out in support of the armed forces, with the purpose of their movement and providing the necessary logistics support for mission fulfillment. According to the "Instructions on the movement and transportation operations of large units and military units" manual, operational requirements for efficient transportation aim at adaptability to existing situations, flexibility to respond to force support requests, and the ability to interrelate its components (Ministerul Apărării Naționale 2014, 3).

Fulfilling the mission of transporting materials to the fighting forces at the right time and place, as well as in the necessary quantity, is essential for the success of operations. In this regard, during the process of force support planning, logistics planners take into account determinants such as *destination, duration, distance*, and the logistic support *demand* for the operation.

The current challenges require identifying new solutions in the field of robotic technologies to provide forces with goods and services at any time and in any situation. In the current technological development context, the use of digital solutions plays an important role in the defense industry sector. Not only the military environment witnesses such developments but also the private business setting, especially in the logistics field, experiences surprising evolutions in technological domains, under the auspices of competitive factors and available resources.

The military logistics sector can benefit from technological advancements to decrease human losses due to activities in hazardous zones, reduce the execution time of logistical activities, mitigate losses due to logistical errors and delays that may occur in the supply chain, and increase the transparency level of logistics operations by ensuring visibility of goods.

Studying specific solutions of robotic technologies used in the private sector and in the logistic systems of other armies can lead to transformations in terms of predictability, transparency, and efficiency of the activity field. The advantages consist of enhancing operational efficiency by providing necessary materials to forces in the shortest time, reducing risks associated with transporting goods in hostile operational zones, and reducing the dependence on human labor.

To elaborate on this article, a qualitative research strategy (Șandor 2013, 51) was applied for a deep understanding of the phenomena and processes in the field of military transport. The methodology was also applied to gain detailed knowledge of technologies in the digital transportation sector.

For this purpose, the data collection technique used was the analysis of various manuals, regulations, doctrines, articles published in journals and magazines, media content, websites of digital technology developers, and specialized books.

Logistic planning through the 4D formula

In the context provided, the text discusses the operational logistics planning perspective through the 4D formula. Starting with the definition of logistics as a managerial science, according to the „Unified Logistics Doctrine of the Romanian Army" (S.M.Ap. 2023, 12), it is broken down into three elements (production logistics, support logistics, and operational logistics), organized along four lines of logistic support. From this perspective, the article's focus is on operational logistics, a component responsible for ensuring military forces with the necessary services and goods for the uninterrupted conduct of military actions.

Among the main objectives of operational logistics, timely and secure provision of goods and services, maintenance services for military equipment, support for changing the location of military forces and materials, movement and transportation of personnel and materials, operational medical support, host support assistance, and the utilization of contractor support are enumerated (S.M.Ap. 2023, 28).

Operational logistic support entails providing combat forces with materials and services (medical evacuation, equipment repair evacuation, campaign services) at the "right time and place, in the necessary quantity and quality" (S.M.Ap. 2023, 19). The execution of logistic support is based on a conception that is the result of the logistical planning process. As per the "Manual of logistic support in joint operations," the factors influencing the logistics planning process are determined by destination, duration, distance, and the logistic support demand for the operation (C.L.I. 2007, 10). This approach can also be found in the support concept of the British Army. For example, the "Joint Doctrine Publication 4-00" presents the formula of the "four Ds": demand, duration, distance, destination, as simplified in Figure Number 1 (M.o.D. 2015, 156).

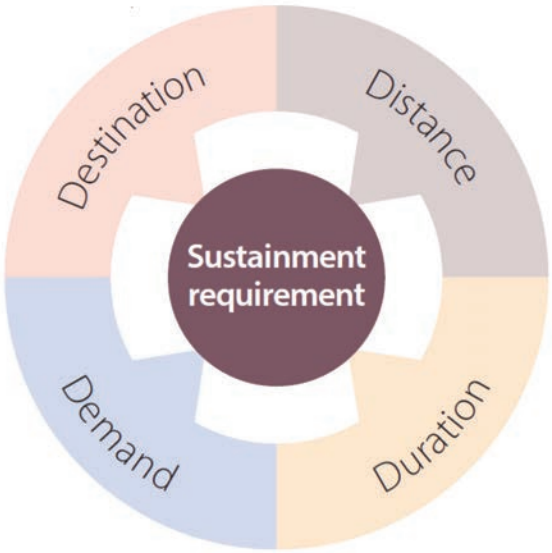

Figure 1 The four Ds – demand, duration, distance, destination (determining factors for logistic planning) (M.o.D. 2015, 156)

According to the figure, the *destination* refers to determining the requirements for providing logistic support. Thus, in the process of planning military transport, factors such as access to infrastructure in the operational area, the level of its development, or the presence of civilian contractors are considered. *Distance* is a factor from which considerations regarding the length of transport routes, the time required for transport, transport capacity, and topographical elements can be deduced. The *duration* of a mission generates varying efforts for logistic support. Therefore, planning logistic support for a short-duration mission considers different elements than those for supporting forces in a long-term mission. An example of this is the African Union Mission in Somalia in 2007 (Major and Strickmann 2011, 6), where the initial six-month mission mandate was extended, and the initial logistic support planning required adjustments to meet the new requirements. Meeting the *demand* is a challenge for logistic support planning, as it requires accurate forecasting of resource consumption for the operation's completion. Demand estimation takes into account both the intensity of combat and the mission duration, which place additional strain on logistic support.
These aspects need to be considered in military transport planning, given the challenges that can be encountered in providing logistic support during the mission.

Challenges for transportation in order to support troops in operations

Lessons learned from ongoing conflicts show that the current military operational environment is becoming more complex and dynamic than in the past, and logistic support is subject to much more difficult-to-forecast factors. Nevertheless, some logistical challenges of past centuries faced by military commanders remain relevant today (Clausewitz, et al. 1984, 340). In the cited work, Clausewitz describes the conditions under which troop logistic support is carried out with difficulty. The author presents these aspects from the perspective of the commander of the force conducting offensive actions, in other words, from the attacker's point of view. From experience, he recognized that at the moment of initiating an attack, the attacking force conducts combat actions with an increased rate of material consumption. However, resupply needs may be difficult to meet, given that the necessary goods cannot be transported at the same pace as the offensive operation. To prevent delayed resupply of troops, Clausewitz recommends rigorous pre-planning of resource deployment.

The author details another moment when logistic support can be provided with difficulty. At the end of a successful military campaign, the lines of communication between the frontline forces and logistic support forces can become very extended. As Clausewitz observes, providing logistic support over very long distances, in

hostile environment, can lead to a loss of initiative or even withdrawal of forces from captured positions. Similar observations were noted in the early weeks of the Russia-Ukraine conflict. Considering that the armed forces of the Russian Federation managed to successfully exploit the surprise effect of the attack, the increased tempo of the operation led to rapid advancement into Ukrainian territory, nearly reaching Kyiv. Thus, the high rate of ammunition and fuel consumption, along with the extended supply and transport lines, posed challenges to the continuous provision of logistic support for Russian troops. The logistical convoys loaded with necessary supplies for the Russian armed forces did not reach their objectives, leading to the withdrawal of Russian troops from captured positions. The causes of the convoy stoppages were numerous, including the extended length of supply lines (Martin, Barnett and McCarthy 2023, 7-8).
These aspects observed by Clausewitz during the Napoleonic wars are still relevant today in the principles of logistic support, representing current elements for operational planning as found in the "Joint Operations Logistics Regulation" (Ministerul Apărării 2008, 3).

Digital technologies applied in transportation

Today, military operations tend to develop multi-domain capabilities (NATO 2023), requiring appropriate logistic support. As mentioned earlier, it is not a novelty that military operations are conducted faster than the logistic forces can support the armed forces. The evolution of technology drives new trends in the conduct of armed conflict. The use of advanced technologies such as long-range unmanned aircraft systems (UAS) that can identify targets thousands of kilometers away presents a significant potential for revolutionizing military affairs (Gupta, Ghonge and Jawandhiya 2013). Additionally, satellite imagery (Planet.com n.d.) can be easily accessed, providing precise information on the positions of armed forces and their changes within minutes. It can be said that military actions in the tactical field are conducted under conditions that can be visible to interested parties.

To meet current operational requirements, a more flexible, efficient, and adaptable approach to managing logistic support is needed, according to the basic principles of the Romanian Army's logistics (S.M.Ap. 2023, 20).
We will further refer to several technologies applicable in logistics, such as robotic systems for logistics, autonomous vehicles, and radio-frequency identification technologies.

Robotic systems used in logistics aim to improve the efficiency of the logistic system by increasing the accuracy and speed of logistic operations (Bi, et al. 2024, 245). In the European Union (EU), industrial companies continuously invest in developing and implementing robotic solutions. According to the President of the International Federation of Robotics (IFR), Marina Bill, the top five EU countries leading the

way in robotic systems are Germany, Italy, France, Spain, and Poland. These five countries use approximately 70% of all industrial robots installed in the EU in 2022 (IFR Press Room 2023). In the military system, current trends focus on developing and evaluating robotic systems specifically designed for military logistics operations. For example, there is interest in autonomous transport vehicles (Milrem Robotics n.d.). THEMIS (Tracked Hybrid Modular Infantry System) is an unmanned ground vehicle (UGV) developed by Milrem Robotics with the support of the Estonian Ministry of Defense to perform multiple missions (Army Technology 2024). Other technological developments are noticeable in the drone sector, robotic manipulators, and automated storage and retrieval systems. The United States Marine Corps intends to equip logistic units with tactical resupply drones, such as TRUAS (Tactical Resupply Unmanned Aircraft System), by 2028 (Skove 2024). These systems have been used by the armed forces of the Russian Federation and Ukraine for material supply and casualty evacuation (Burgess 2024). The main benefits of such technologies include eliminating human losses due to exposure to enemy actions, accessing various locations even in complex operational environments, reducing resupply time, and improving logistic support efficiency (McKay, et al. 2020, 7).

McKay et al (2020, 49) addresses in the paper "Automating Army Convoys" the opportunities and risks from the perspective of using autonomous vehicles in military convoys. According to the authors, transport missions in military operations involve traveling long distances on unsecured routes. For this reason, transport means are vulnerable to enemy attacks and ambushes in non-linear and non-contiguous operational environments that generally do not have secured rear areas. Experience in the theaters of operations in Iraq and Afghanistan highlighted these vulnerabilities: army convoys suffered heavy losses while traveling hundreds of miles on unsecured distances. The main opportunity derived from these experiences is the possibility of protecting military personnel from such dangers. The risks to the implementation of autonomous vehicles refer to a "technical immaturity" of these projects (McKay, et al. 2020, 13).

Digital and robotic technologies are solutions adopted to improve the *supply chain* by managing inventories, forecasting material demand, designing distribution networks, and optimizing transport to enhance efficiency and response speed. Armies of countries such as the United States, Brazil, or Australia run programs that ensure the traceability of material goods (Roberti 2013). For example, the possibility of identifying products by allocating a unique code (Unique Identification/UID). Also known as IUID (Item Unique Identification), the system serves to differentiate items from other similar elements to facilitate the exchange of logistic information. This program requires a unique and specific number to be assigned to tangible equipment owned by the government, according to the publication "Army Regulation 700–145 Item Unique Identification" (Department of the Army 2020, 5).

Other ongoing programs aim to implement a set of *radio frequency identification* (RFID) technologies for material goods and equipment. To successfully carry out missions, armed forces must be continuously supported with materials and equipment, including food, weapons, ammunition, fuel, spare parts, medical products, etc. RFID technology can improve supply chain operations by confirming that the appropriate items have been picked up and shipped at the right time. Additionally, RFID systems allow for updates with information indicating the location of goods and the time when the item tags were scanned, ensuring visibility in the locations where they are stored (mojix.com 2019).

Conclusions

Transport activities are carried out to support the armed forces, facilitating their movement and providing the necessary logistic support to accomplish missions. Operational requirements for efficient transport include adaptability to existing situations, flexibility to respond to force support requests, and the ability to interrelate its components.

Technological advancements for improving transport include autonomous transport through the use of drones and unmanned vehicles. These can be applied by military logistics to ensure material transport and supply for forces in hard-to-reach or unsecured areas. New technologies ensure faster and safer transport, eliminating the risks associated with human presence in such zones.

Robotic technologies can be used to automate logistic operations, such as handling and moving goods, loading and unloading vehicles, and quickly identifying and locating materials. The benefits brought relate to reducing human losses due to exposure to enemy actions, decreasing dependency on human labor, increasing logistic efficiency, and speeding up response times to logistic support requests.

References

Army Technology. 2024. *THeMIS Hybrid Unmanned Ground Vehicle.* https://www.army-technology.com/projects/themis-hybrid-unmanned-ground-vehicle/?cf-view.

Bi, Yanchao, Jiale Cheng, Limei Wang, and Yizhun Peng. 2024. "Intelligent Logistics Handling Robot: Design, Control, and Recognition." *Proceedings of International Conference on Artificial Life and Robotics.* pp. 337–345. https://doi.org/10.5954/ICAROB.2024.OS13-1.

Burgess, Matt. 2024. *Robots Are Fighting Robots in Russia's War in Ukraine.* https://www.wired.com/story/robots-are-fighting-robots-in-russias-war-in-ukraine/.

C.L.I. (Comandamentul Logistic Întrunit). 2007. *Manualul Conducerii Sprijinului Logistic În Operaţii Întrunite.Doc.*

Clausewitz, Carl, Michael Howard, Peter Paret, Bernard Brodie, and Rosalie West. 1984. *On war.* New Jersey: Princeton University Press.

Department of the Army. 2020. "Army Regulation 700–145 Item Unique Identification." https://milreg.com/File.aspx?id=1411.

Gupta, Suraj G., Mangesh Ghonge, and Pradip M. Jawandhiya. 2013. „Review of Unmanned Aircraft System (UAS)." *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 2 (4): 1646-1658. http://dx.doi.org/10.2139/ssrn.3451039.

IFR Press Room. 2023. *European Union: Industries Invest Heavily in Robotics.* https://ifr.org/ifr-press-releases/news/eu-industries-invest-heavily-in-robotics.

M.o.D. (Ministry of Defence). 2015. *Joint Doctrine Publication 4-00.* Logistics for Joint Operations, Ministry of Defence. https://assets.publishing.service.gov.uk/media/5a7f9a4d40f0b62305b8824e/20150721-DCDC_JDP_4_00_Ed_4_Logistics_Secured.pdf.

Major, Claudia, and Eva Strickmann. 2011. „You can't always get what you want-Logistical Callenges in Military Operations." https://www.swp-berlin.org/publications/products/arbeitspapiere/AP_Major_2011_Logisics_in_EU_Operations_ks.pdf.

Martin, Bradley, D. Sean Barnett, and Devin McCarthy. 2023. *Russian Logistics and Sustainment Failures in the Ukraine Conflict: Status as of January 1, 2023.* RAND Corporation. https://doi.org/10.7249/RRA2033-1.

McKay, Shawn, Matthew E. Boyer, Nahom M. Beyene, Michael Lerario, Matthew W. Lewis, Karlyn D. Stanley, Randall Steeb, Bradley Wilson, and Kate Giglio. 2020. *Automating Army Convoys: Technical and Tactical Risks and Opportunities.* https://www.rand.org/pubs/research_reports/RR2406.html.

Milrem Robotics. fără an. *The THeMIS UGV.* https://milremrobotics.com/defence/.

Ministerul Apărării Naționale. 2014. "Instrucțiunile privind operațiunile de mișcare și transport ale marilor unități și unităților militare." Parte integrantă din Ordin 4/2014.

Ministerul Apărării. 2008. "Regulamentul logisticii operațiilor întrunite." Ordin nr. M 36, Publicat în MONITORUL OFICIAL nr. 353 din 7 mai 2008.

mojix.com. 2019. "RFID and IoT Technology: Improving Military and Defense Applications from End to End." https://www.mojix.com/rfid-iot-technology-military-defense/.

NATO. 2023. *Multi-Domain Operations in NATO – Explained.* https://www.act.nato.int/article/mdo-in-nato-explained/.

Planet.com. fără an. *Enhance Geospatial Intelligence with Planet's High Frequency Satellite Data.* Accessed March 01, 2024. https://www.planet.com/markets/defense-and-intelligence/.

Roberti, Mark. 2013. "How Can the U.S. Army Use RFID?" *RFID Journal.* https://www.rfidjournal.com/question/how-can-the-u-s-army-use-rfid.

S.M.Ap. (Statul Major al Apărării). 2023. *Doctrina logisticii Armatei României.* București: Ministerul Apărării Naționale.

Skove, Sam. 2024. *Marine Logistics Battalions to Get Resupply Drones by 2028.* https://www.defenseone.com/technology/2024/05/marine-corps-set-field-resupply-drones-all-logistics-battalions-2028/396353/#:~:text=The%20TRUAS%20drone%2C%20also%20known,risky%20to%20send%20in%20vehicles.

Șandor, Sorin Dan. 2013. *Metode și tehnici de cercetare în științele sociale.* București: Editura Tritonic.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Romanians and Bulgarians at the end of the 19th century and the beginning of the 20th century. Political assassinations, border incidents and the attempted anarchist/terrorist plot against King Carol I (1900-1901)

Daniel Silviu NICULAE, Ph.D.*

*"Dimitrie Cantemir" Historical Association - A.S.I.C. Bucharest
e-mail: danielniculaie@yahoo.com

Abstract

At the beginning of 1900, Romanian-Bulgarian relations were very tense, being fuelled by both the incidents at the Southern border and the attacks that took place on the Romanian territory, thus, on the agenda of the Romanian politicians, the problem of the Aromanians from the Balkan Peninsula and Macedonia, the province coveted by Bulgarians, Greeks and Serbs, where comitagii gangs, the antarti and the cetnic fought both for the liberation of the countrymen from Ottoman rule and with the Turkish troops. In this context, assassination came to be used as a weapon against opponents, being present in Romania, Bulgaria, Serbia and Greece.
At the end of the 19th century, Romanian society was suddenly awakened to reality, facing the consequences of the barbaric manner in which one of these revolutionary secret committees acted, whose anarchist subcommittee was established in Bucharest – nowadays we frequently use the phrase terrorist cell for something similar. Thus, it received the mission to commit several bombings on the Romanian territory, as well as the assassination of King Carol I and Romanian dignitaries, while, at the Southern border, the Romanian border guards reported daily incidents at the common border whose purpose was to destabilize and maintain a tense state on the conventional demarcation line between Romania and Bulgaria.

Keywords:
asymmetric threat; secret committee; nationalist terrorism; border incident; political assassination.

Article info
Received: 15 May 2024; Revised: 7 June 2024; Accepted: 14 June 2024; Available online: 5 July 2024

Citation: Niculae, D.S. 2024. "Romanians and Bulgarians at the end of the 19th century and the beginning of the 20th century. Political assassinations, border incidents and the attempted anarchist/terrorist plot against King Carol I (1900-1901)". *Bulletin of "Carol I" National Defence University*, 13(2): 151-165. https://doi.org/10.53477/2284-9378-24-26

Bucharest under the terror of the anarchist group/terrorist cell Supreme Macedonian Revolutionary Committee. The assassination of Cyril G. Fitowski

The proclamation of the Bulgarian Exarchate, on February 28, 1870, by an order of the Sublime Porte signed by Sultan Abdul-Aziz, spurred the latent aspiration to fulfil the national ideal of the Macedonians, liberation from the Ottoman Empire. In the second half of the nineteenth century, Macedonia, the Ottoman province, had a varied ethnic composition with different religious orientations. However, the Macedonian dioceses joined as a result of a referendum on the Bulgarian Exarchate, which influenced the formation of the first local, revolutionary, militia formations, who fought for freedom and identity against the Turkish occupant. In 1891, in Thessaloniki, a small group of young Macedonian insurgents began organizing paramilitary bands whose merger led to the creation in 1893 in the same city, of the Macedonian Revolutionary Organisation. Shortly after, inspired by the Macedonian insurgents, in 1895 in Sofia, at the congress organized by several cultural associations, it was decided to establish the Macedonian Supreme Committee, an anarchist terrorist organization, which gradually came under the coordination of Bulgarian military personalities. One of them was General Danail Nikolaev, who fought in the Serb-Turkish war (1876-1877) and then as commander of a company of Bulgarian volunteers in the Russian-Romanian-Turkish war of 1877-1878, distinguished in the battles of Sipka and Sejnovo.

In 1899, the Macedonian Revolutionary Organisation decided to work with the Supreme Macedonian Committee in Sofia for a limited period, being appointed to coordinate joint actions, Boris Sarafov. Moreover, it should be noted that starting in 1895, detachments of comitagi from the Macedonian Supreme Committee or national liberation fighters, as they were perceived by Bulgarian society, raided Macedonia alongside members of the Macedonian Revolutionary Organisation. About the cruelty of these attacks and their atrocities on the poor Greeks and Aromanians in Macedonia, the media of the era reported facts that were also reflected in the diplomatic correspondence in their home states. If initially, the struggle of the Macedonian Revolutionary Organization was regarded with sympathy by the peoples of the Balkan Peninsula and not only, at the moment when Bulgarian comitagi began to operate on the territory of the province under Ottoman occupation and the Macedonian Supreme Committee became the platform of Bulgarian government interests in Macedonia, which, under the pretext of liberating the Bulgarian brothers from Ottoman rule, sought and managed, in large part, to diminish the performances of the indigenous Macedonian revolutionary movement, the Bulgarian cause in Macedonia was perceived as a threat to the interests of the Great Powers on the Balkan Peninsula. Bulgaria gradually became a supplier state of instability in the region by supporting anarchist/anarchist attacks/ terrorist members of the Macedonian Supreme Committee on the national territory of neighbouring states whose reaction could trigger an armed conflict.

In this context, in the second half of November 1899, a subcommittee/subsidiary/ cell of the Macedonian Revolutionary Supreme Committee was established in Bucharest, an anarchist/terrorist group, whose headquarters was, as I mentioned, in Sofia. The Committee's management consisted of Boris Sarafov – President, D. Davidov - vice president, Vladimir Covacev – secretary and George Petrov – cashier. The main purpose of this organization was to obtain by revolutionary means the autonomy of Macedonia and its adherence to the Bulgarian Principality, which is why the members of this committee used propaganda not only in Bulgaria but also among the Bulgarians who emigrated to other countries and gathered the money contributions to maintain turmoil and prepare the revolution. In Bucharest, the Committee was led by Alexandru Trifanov and consisted of members such as Nicola Bogdanov called Hagiu, Anghel Pop Arsov and Marcu Bosniacov. Soon the group was completed with students George Theodorov, Cristu Carambulev, Coti Zafirov and Traciu Zvetcov. All of them swore an oath on a dagger and revolver. The founding of the cell in Bucharest in December 1899 was attended by the Committee chairman Boris Sarafov Sarafov (Dreptul Magazine 1900, 505-516).

Almost two months after its establishment, the members of the anarchist cell in Bucharest received a first mission: the assassination of the Bulgarian Cyril G. Fitowski (Adevărul 1900) accused of treason, as he was considered a Turkish spy. On the evening of February 1, 1900, Cyril G. Fitowski was killed on Ceaus Radu Street. According to the indictment drawn up by the first prosecutor of the Ilfov Tribunal, Emil Miclescu, „commissar of the 41st section was notified that, in the house at no. 2, located in Ceaus-Radu Street, the building belonging to Adolf Solomon, was found near the pavement, a man badly hit and in insensibility. The judicial authorities at the scene found that the unknown near which was also a thrown axe, had already ceased from life and that, no doubt, a murder had been committed" (Dreptul Magazine 1900, 505-516).

The main suspects of the crime were immediately identified, namely the members of the Macedonian Committee: Boiciu Iliev, Alexandru Trifanov, Nicola Mitev, Mitu Stoicev, Cristu Carambulev, George Theodorov, Marcu Ivan Bosniacov, and others, Anghel Pop Arsov, Traiciu Svetkov, Coti Zafirov or Zamfirov. Accomplices or, according to the indictment, provocative agents were identified the following: Boris Sarafov, Vladimir Kovachev, Gheorghe Petrov and D. Davidov (Dreptul Magazine 1900, 505-516).
The investigation established that there were several people sent from Sofia: the named Boiciu Iliev, with the duty to commit the crime, Nicola Mitev – the coordinator of the murder of Cyril G. Fitowski - and Mitu Stoicev. They were helped in order for the mission to be carried out in good conditions by Cristu Carambulev, Marcu Bosniacov and student George Theodorov (Dreptul Magazine 1900, 505-516).

From the hearings that took place during the investigation, the scenario of the assassination emerged. The crime was prepared in Sofia by the members of the

Macedonian Supreme Committee, for which, in mid-January 1900, Nicola Mitev was summoned to the chancellery of the Committee, where Boris Sarafov brought to his attention the suspicions of espionage that appealed to Fitowski, as well as the death sentence pronounced by him and his companions. Boiciu Iliev received the special mission to assassinate Fitowski with the axe, Nicola Mitev and Mitu Stoicev were only supposed to assist the former, and, if Iliev failed to kill him, one of the two men had to intervene to take the life of the spy who, as Sarafov claimed, had claimed, he betrayed the Turks in 1897, the location of a secret weapons depot in Vinita, Macedonia. In addition to the axe, the group assigned to carry out the assassination received another dagger, two revolvers and 150 lei (Dreptul Magazine 1900, 505-516).

On January 25, 1900, Mitu Stoicev, Boiciu Iliev and Nicola Mitev entered Romania through the port of Giurgiu (Dreptul Magazine 1900). The days of January 29 and 30, 1900, were exclusively dedicated to identifying and finding the most favourable place to commit the crime, following that, on January 31, 1900, a meeting took place in Trifanov's house to discuss and establish the last details of the execution plan. In short, for the evening of February 1, 1900, it was decided that Trifanov would leave the cafe Iosef (Calea Dudesti), arm in arm with Fitowski, and under the pretext of a walk on the streets of Bucharest, to lead him to a dark, back alley where every participant in the assassination knew very well what to do. Therefore, on the evening of February 1st, 1900, Chiril G Fitowski collapsed on the Ceaus-Radu street under repeated axe blows by Boiciu, applied from behind with so much skill and power that the victim could not even scream for help (Dreptul Magazine 1900, 505-516).

Who was Cyril G. Fitowski? A supporter and devotee of the Bulgarian cause in Macedonia. He defected from the 2nd Rusciuc Infantry Regiment in 1899. He was a member of the Macedonian Committee and spied on the Turks by putting his life in danger, which was why he was given the mission to buy weapons for the Committee from Romania if possible, however, he stole money to achieve this goal. Under the pretext of a patriotic act, in fact, it seems that the assassination had a trivial motive: a quarrel over the lack of a sum of money between a simple soldier acting outside the law and his bosses (Dreptul Magazine 1900, 505-516).

This action was coordinated with those that took place in Bulgaria. At the end of February and the beginning of March 1900, a few Aromanian merchants were also threatened with death, which is why our diplomatic agent in Sofia, Nicolae Misu, intervened. Bulgarian authorities arrested those Macedonian agents but soon released them. On April 6, 1900, on one of the main streets of Sofia, the president of the Romanian colony, the merchant Papa-Gheorghe was attacked with knife blows, but still managed to escape from the hands of the killers. On April 25, 1900, at Braila, the Bulgarian merchant Stelian Stefanovici was mortally wounded with the dagger by Gh. Nedelkov. On 24 June Theodor M. Kradja the great merchant in Sofia, the Romanian submissive was seriously injured in front of his shop by several revolver shots. The assassin was in the service of the Macedonian Committee (although he was

of Macedonian Romanian origin but was banished from his father's family for bad behaviour). At the protest made by Nicolae Misu, a protest also made known to the ministers of Italy, Germany and Austria-Hungary present in Sofia, from the provisions of our foreign ministry, Ion N. Lakhovari, chairman of the T. Ivanciov council, did not take action because, as some of the Bulgarian ministers said, as foreign diplomats did, on the one hand, the government was powerless before the Committee, on the other hand, provisions coming from the top of political power required it to be given a free hand (Archives of the Ministry of Foreign Affairs, 1966, 43).
On this issue, in the correspondence of the Romanian diplomatic corps in Sofia with the Ministry of Foreign Affairs in Bucharest there was mentioned the unconditional attachment and support of the Bulgarian society to the revolutionary secret committees fighting for the Bulgarian cause in Macedonia.

Assassination of Professor Stefan Mihaileanu. The plot against King Carol I. Aspects regarding the activity of the foreign minister Alexandru Marghiloman regarding the actions of the Supreme Macedonian Central Committee in Bucharest. Worsening the bilateral relations between Romania and Bulgaria.

Stefan Mihaileanu was born in 1859 in Ohrid, Macedonia. At the age of 10, he came to Bucharest where he attended the Sf. Sava where he obtained the Baccalaureate Diploma. He was licensed in letters at the University of Bucharest. For 17 years he was a professor of Greek and Latin at various high schools and private institutions in the capital (Adevărul 1900). In 1892 he founded the Balkan Peninsula newspaper in Bucharest, whose circulation was stopped in 1895. A good patriot, distinguished professor and pleasant writer, he had not given up, however, ever, the idea of restarting the printing of his newspaper, in which he had warmly defended the interests of the Aromanians and thus, the periodical reappeared on 23 January 1900 (Dreptul Magazine 1900, 505-516).

On January 25, 1900, a secret meeting of the Supreme Macedonian Central Committee in Bucharest was held, led by Alexandru Trifanov, discussing the consequences of the reprinting of the Balkan Peninsula newspaper and the effects on Bulgarian propaganda for Macedonia. The conclusions drawn were sent to Sofia for the necessary instructions, but on February 2, 1900, all members of the committee were arrested in the case of the murder of Kiril G. Fitowski (Dreptul Magazine 1900, 505-516).
In this context, in the second half of March 1900, the Bulgarian Dimitrie Iconomov, a highly trusted man of the Macedonian Central Committee, was sent to Bucharest, with the mission, on the one hand, to continue the started propaganda, on the other hand, to establish communication with those imprisoned in the Fitowski business, so that they could be informed that Sofia was making every effort to get them out of jail, even an escape being planned, if, by judgment, they failed to obtain their acquittal. At the same time, Dimitrie Iconomov received the mission to organize the assassination of Stefan Mihaileanu as well as the murder of Alexandru Trifanov,

the president of the anarchist group in Bucharest. Thus, Iconomov, with the help of photographer Fackirov, the socialist Alex Burlacov, the grocer Spiru Alexov and the student Achim Petcov, found the one who executed the criminal sentence of the Committee, the assassination of Stefan Mihaileanu, namely Stoian Dumitrov, a simple tailor-worker, young, intelligent and fanatical, Macedonian, from the town of Uskub (Today Skopje, capital of North Macedonia), who was 19 years old (Adevărul 1900). However, expulsions of Bulgarian citizens in early June 1900 by Romanian authorities postponed the implementation of the plan devised for the murder. On June 17, 1900, at the insistence of Iconomov, Stoyan Dimitrov went to Sofia to meet Boris Sarafov, from whom he received the execution order. With the promise of continuing his studies and taking a solemn oath (the text of the oath: according to the statement given during the investigation was: "In the name of God, I swear, that I will fight for the Bulgarians in Macedonia and defend their interests", (Gazeta Transilvaniei Newspaper 1900), followed by the solemnity of the kiss on the mouth of President Boris Sarafov and the other members of the leadership as well, Stoian Dimitrov left for Bucharest with the plan of the assassination in his pocket and the amount of 50 lei for possible expenses. The instructions received were clear: committing the axe murder and denying membership in the Committee if arrested by the Romanian authorities (Dreptul Magazine 1900, 505-516).

Returning to Bucharest on 2 July 1900, Stoyan Dimitrov began to implement the stages of the plan conceived in Sofia. Thus, not having the ability and physical strength of Boiciu to handle the axe, he bought a revolver for 10 lei from a millet beer seller named Nicola who lived on Lucaciu Street. For the proper development of the plan, he was helped by the student Achim Petev, the grocer Spiru Alexov and the socialist Alexandru Burlacov, a native of Tulcea. Alexandru Burlacov was the one who helped him to identify Stefan Mihaileanu who used to go to the Macedonian cafe at the Nifon Palace. From that moment on, Stoian Dimitrov began to follow him for several days, step by step, in order to know his movements and habits. On the evening of July 22, 1900, after receiving the address from Spiru Alexov, 34 Iancului Street (Adevărul, 1900), respectively, he remained in front of the building where Stefan Mihaileanu lived. Shortly after, accompanied by his wife and 10-year-old daughter, he left the house, heading towards the street Tepes-Voda where, at number 31, a friend lived, a school reviser of Putna, who he was going to spend a few hours with (Gazeta Transilvaniei Newspaper, 1900, 2).

Around 24.00, Stefan Mihaileanu, on his wife's arm and with his daughter, left the location in Tepes-Voda Street being followed by Stoian Dimitrov. In the proximity of Stefan Mihaileanu's house, on the street of Linistei, corner of Iancului Street, Stoian Dimitrov approached the editor of the Balkan Peninsula newspaper and 3-4 meters away he fired a gunshot from behind. To be sure that Stefan Mihaileanu could not escape alive, he wanted to fire a second fire but the revolver did not work, which is why, panicked, he hurried away from the scene, losing his black beaver hat (Adevărul 1900). Frightened, bare-headed, and easily recognizable, he arrived on Plantelor

Street where he noticed a building (house) (Adevărul 1900) under construction and decided to hide in it until things calmed down to go unnoticed. The incident caused two street sergeants who were nearby to hear the noise of the gun and so, they followed in the footsteps of the killer after they arrived at the scene of the murder and informed themselves about the author's features. The first thorough investigation was made by police inspector Sava Grigorescu (Adevărul1900). Shortly after, the two sergeants, Tudor Constantin and Zornescu Gheorghe, reached the building in the street of Plantelor, where they found him lying down, pretending to sleep, identified without a hat, in the light of a match, Stoyan Dimitrov, whom they led to the Prefecture of Police. Meanwhile, although he was transported to Coltei Hospital, Stefan Mihaileanu died in prison, just 30 minutes after the crime was committed as the bullet had hit his lungs (Dreptul Magazine 1900, 505-516).

According to media reports, the interrogation was led by a team of investigators consisting of Emil Miclescu, first prosecutor, (Jean) Ion Th. Florescu, the investigating judge, prefect D.Dobrescu, Sava Grigorescu and Puiu Alexandrescu, the head of the Security, who brought to the attention of the general public details on how the assassination was planned and executed (Adevărul Newspaper 1900).
The press of the time reported that Stefan Mihaileanu's father-in-law, Pompiliu Eliade, a week before the murder, while dining inside the Paris Garden, learned by chance about the possible assassination, but Stefan Mihaileanu ignored his warnings, despite the insistence of Paulina Stefan Mihaileanu, his wife, to be careful in this regard (Adevărul Newspaper 1900).

The press also mentioned the public protests that took place in August 1900. Amid these discontents of the capital's population, the investigators found out about the missions received by the Macedonian Central Committee from Bucharest. After the assassination of Stefan Mihaileanu, the Albanian Yashar Erebaro and the Bulgarian Nicola Gheorghiev were to be killed, suspected of such espionage on behalf of the Ottoman Empire and, at the same time, with these killings, the Sofia committee planned to operate several burglaries in Bucharest, but the plot against King Carol I outraged the entire Romanian society (Dreptul Magazine 1900, 505-516).

One of the missions received by Dimitrie Iconomov from Boris Sarafov in the second half of March 1900 was the assassination of Alexandru Trifanov, president of the Supreme Macedonian Central Committee in Bucharest. The reason he was sentenced to death was found out by investigators during the investigation into the murder of Cyril G. Fitowski. Facing the full protection of Romanian justice, Alexandru Trifanov, confessed in detail the plan of the plot ordered by Boris Sarafov against King Carol I, in order to provoke disorder in Romania. While the king of Romania was being killed, there had to be a bomb attack at the Chamber of Deputies and because Romania was allied with Serbia, the Serbian sovereign was also to be killed (Dreptul Magazine 1900, 505-516).

The proposal of this attack was enthusiastically received by the members of the Supreme Macedonian Central Committee in Bucharest. Mark Bosniacov and Anghel Pop Arsov were assigned to kill King Carol I. Immediately after the assassination, they had to declare that they were bakers and hide at the home of Nicola Bogdanov, until the favourable time to leave for Bulgaria. The plot was decided at the Unirea hotel in Bucharest, in the room that Sarafov occupied on 9, 10 and 11 December 1899 (Dreptul Magazine 1900, 505-516).

On the occasion of the reconnaissance, the daggers bought by them were found to carry out the assassination, as well as their passports, necessary for the smooth crossing of the border. From the press of the time, it turned out that they followed the king when he came out of the palace stables and when he was walking in the company of a single aide, on the Dambovitei quay, near the state printing house (Tribuna Newspaper 1907, 4). The attack did not take place simply because Mark Boineakov and Anghel Poparasov managed to flee to Bulgaria before the confinement of Alexandru Trifanov, being proposed for expulsion from Romania by police representatives without suspecting their role in the planned plot. Nicola Bogdanov also called Hagiu was arrested and imprisoned at Văcărești prison by the investigating judge Th. Florescu (Tribuna Newspaper 1907, 4).

The sentencing delivered by the Ifov Court of Justice to Bulgarian diplomatic representatives accredited in Bucharest was in line with the facts committed. For the murder of Cyril Fitowski, Boiciu Iliev was sentenced to life imprisonment. His accomplices, Nicola Mitev and Dumitru Stoicev, received 20 years of hard labour. This group also included Christu Carambulov who received 7 years of hard labor and Alexandru Trifanov who got 2 years of correctional imprisonment (Telegraful român Newspaper 1900, 1).

The author of the assassination committed against Stefan Mihaileanu, Stoyan Dimitrov, received a sentence of forced labour for life, and his accomplices, Spiru Alexov received 20 years hard labour and Achim Petev received 5 years imprisonment (Telegraful român Newspaper 1900, 1).
The group that planned the plot against King Carol I received punishments in money and years' imprisonment, respectively, Nicola Bogdanov a 10-year prison sentence and Alexov Petev and Stoian Dimitriv a fine of 10,000 francs (Telegraful român Newspaper 1900, 1). Boris Sarafov and his helpers in Sofia were sentenced to life imprisonment. Iavconomov received a sentence of 20 years of hard labour (Telegraful român Newspaper 1900, 1). From the statements of the Bulgarian anarchists, given during the investigation, Romanian prosecutors learned that the group in Bucharest intended to assassinate Take Ionescu (Telegraful român Newspaper 1900, 1).

All these facts, the involvement of senior Bulgarian dignitaries in the work of the Committee, the publicity of the process, the presence of Bulgarian representatives, S. Shivachev –a member of the Rousiuc Court of Appeal (now Ruse) and Theodorov,

are all, the delegate of the Bulgarian diplomatic agency in Bucharest, in the courtroom at the time of the sentence against which they had no say in front of the administered probationer, the threat that floated on the Romanian sovereign and the indignation of the Romanian society that did not hesitate to say its opinion on, at least, the crime committed against Stefan Mihaileanu, vehemently, in the street, they determined the Romanian foreign minister, Alexandru Marghiloman, both during the investigation of the assassinations and the plot and after reading the sentence, to formulate according to the diplomatic procedure, protest notes suggesting a possible break in the bilateral relations between Romania and Bulgaria.

Aspects regarding the activity of the foreign minister Alexandru Marghiloman regarding the actions of the Supreme Macedonian Central Committee in Bucharest. Incidents on the Southern border of Romania

The reaction of the foreign minister Alexandru Marghiloman was immediate and firm, delegating Nicolae Misu, Romania's plenipotentiary minister to Bulgaria, to make an energetic protest in Sofia, as a result of which, if the Bulgarian government responded by delaying matters concerning the activity of the Macedonian Central Committee on Romanian territory, the Romanian side reserved the right to act according to international provisions in the field. The provisions sent by the Romanian foreign minister to Nicolae Misu on August 1, 1900, indicated the intention of the Romanian government to use all the legal instruments at its disposal, gradually, even to the breakup of diplomatic relations between the two countries. The facts had been brought to the attention of the Sublime Porte and some of the governments of the great powers, especially since Nicolae Misu had also received an anonymous letter in which he was threatened. At the first meeting between the Romanian diplomat and the Bulgarian prime minister, the latter defended the Macedonian committee and claimed that the assassinations of the Macedonian Romanians in Bulgaria – the Krajda case (On 24 June Theodor M. Krajda, a significant merchant in Sofia, a Romanian subject, was seriously injured in front of his shop by several revolver fires. The assassin was in the service of the Macedonian Committee so it was a personal struggle between the Macedonian Romanians in Sofia who sought to make all the discussion a personal quarrel with the Romanian minister (Archives of the Ministry of Foreign Affairs 1966, 44).

In the second audience, requested immediately after the assassination of Stefan Mihaileanu, the chairman of the Bulgarian Council of Ministers, said that if the Romanian police were unable to take action, he could not be responsible for a crime committed in Romania (Archives of the Ministry of Foreign Affairs 1966, 44). From the discussions held by Nicolae Misu, the Romanian diplomatic agent in Sofia, with the other foreign ministers accredited in Bulgaria, it was obvious that the Bulgarian government and King Ferdinand, both, did not dare to start an internal investigation

into the work of the Macedonian Committee, for the simple fact that for the entire Bulgarian people, this anarchist organisation had actually become a national institution and was the main instrument for obtaining advantages for Bulgarians in Macedonia. Regarding the attitude of the Bulgarian king Ferdinand concerning Romania, in a report addressed to the foreign minister, Alexandru Marghiloman, Nicolae Misu said that he could not write on the map the conclusion he reached, which is why he had to travel to Bucharest to report personally (Archives of the Ministry of Foreign Affairs 1966, 43).

In this fragile bilateral context, which characterized the Romanian-Bulgarian relations, Alexandru Marghiloman asked Nicolae Misu for a report detailing the situation of Romanian traders in Sofia who had paid large amounts of money to the Macedonian Committee in the form of a loan. By August 1900, several merchants had been identified who had paid about 30,000 gold lei and refused to declare anything about the money. On these issues, on how Romanians in Bulgaria were practically robbed, Alexandru Marghiloman gave clear dispositions to the Romanian diplomatic representatives present in the Tsarist Empire and the Ottoman Empire to inform the respective governments about this situation (Archives of the Ministry of Foreign Affairs 1966, 47).

Moreover, Alexandru Marghiloman sent clear provisions in Sofia to Nicolae Misu to inform the Bulgarian prime minister, T. Ivanov, that Romania could order the expulsion of important Bulgarians from the country, which was finally put into practice, or take whatever measure he saw fit in them, unless he gets involved in finding the culprits that committed the assassination on the evening of July 22, 1900. Finally, under pressure from foreign ministers and protest notes from the Romanian foreign minister, the Bulgarian government specified that as soon as they were in possession of solid evidence regarding the criminals of Stefan Mihaileanu present on the national territory, they would take the necessary measures (Archives of the Ministry of Foreign Affairs, 47). To support this claim, the investigation started in the case of the anarchist Ciolakov, who shot Theodor M. Krajda. Regarding the financial blackmail of the members of the committee, Ivanciov said that the Bulgarian justice did not take any action because no complaints were filed by the Romanian traders. Obviously, they were not submitted because, under the threat of the Macedonian Central Supreme Committee, they declared that they willingly gave the respective amounts of money, after which they left Bulgaria leaving in particular the abandoned shops at the discretion of the anarchist organization (Archives of the Ministry of Foreign Affairs 1966, 47).

On 10 August 1900, Alexandru Marghiloman was informed by the Romanian minister in Belgrade, C. Diamandy, that two agents of the Committee left Sofia with the mission to commit new attacks against King Carol and the politicians in Romania. Against the backdrop of this information, Romanian-Bulgarian relations deteriorated from hour to hour, which is why, when the Romanian diplomatic

representative in Sofia asked for a response from the Bulgarian government regarding the existence of rumours about the possible mobilization of the Bulgarian army, prime minister Ivanciov replied that Bulgaria could mobilize if Romania took such a military measure (Archives of the Ministry of Foreign Affairs 1966, 48).

The concern of the foreign minister Alexandru Marghiloman was well founded because besides the fact that there were signalled movements of troops on the southern border, on the Danube line the spirits were very agitated amid the rumours of the mobilization of three divisions from Northern Bulgaria to Vidin, Rusciuc and Sumla and the observation of an intense circulation of military ships and boats on the Danube. The presence of the Russian ship Bolgaria was reported in the port of Nicopolis where it was unloading weapons brought from Odessa. There were reports of border incidents. On August 24, 1900, troop movements attracted the attention of foreign observers, the concentration of reservists in the Silistra region was announced for military exercises and applications for a period of 3 weeks, while the Bulgarian War Minister inspected troops stationed at the border with Romania (Archives of Ministry of Foreign Affairs 1966, 48).

In April 1900, the Ministry of War, Fifth Division, Marina, notified the Ministry of Foreign Affairs about the finding of the commander of the Regiment no.5 Vlasca on taking possession by Bulgarians of the Covanlac. According to the minutes drawn up by him on the spot, *today March 27, 1900 according to the confidential order of the Ministry of War no.1440 of March 22, 1900, the undersigned in charge of investigating the possession of the Covanlac and Cama hostages proceeded as follows:1) On March 25, 1900 the undersigned, accompanied by elderly people who knew these localities closely, were transported with the Siret canon and I descended into both Islets, giving myself all the information necessary to solve this investigation; 2) On March 26, 1900, we were transported by land to the village of Malu which is located in front of these areas, from where, besides the observations made on their situation, we also took categorical information on the possession of these bodies from old people who had done the forest service before 1877; 3) With regard to the current Danube course and the current configuration of these islands, the Austrian map of 1853, as well as all the statements of the people who served us, give us clarification in this finding that fully assured us that the current course of the Danube and the configuration of the islands in matter are in everything as shown in the annexed documents;4) With regard to the list of the islands of the Ministry of Domain showing, namely, the fields and the trusses belonging to the Romanian state and all the information collected, we have the following results: a) the tail of the islet Cama shown on both sketches named by Bulgarians Perigos who has it in possession is attached to an islet in the possession of Romania. The two islands were separated by a Danube waterway just after 1877. At the time of the checks, they were joined as demonstrated when the waters were low* (Archives of Ministry of Foreign Affairs 1966, 48).

A confidential report on the occupation of the Covanlac islet located on the left bank and at the back of the Cama islet by Bulgarian citizens submitted by the Boerescu

Cesar lieutenant to the Ministry of War signalled the presence on the islet of some Turkish fishermen who received a fishing permit from the Bulgarian authorities in Ruciuc. At the same time, the back of the Cama or Dinul, named by Bulgarians Pergos, was occupied by sheep. The shepherds and the four people who had started to build a hut were also allowed by the Bulgarian authorities. From the study of the tables with the names of the estates received from the Ministry of Foreign Affairs and the Ministry of Domains, the two officers did not find mention of the Islet Covanlac, however, they noted that this island was present on the Danube map in 1898 where the figure close to the territory of Romania, being listed in 1898 as belonging to the Romanian state. The inconsistency started from the minutes of the Ports Inspectorate and the Forest Inspectorate that mentioned that Pergos belonged to Bulgaria although the two officers noted that it had united with the island of Cama. The proposal of Officer Boerescu Cesar was that in order to eliminate any possible divergences, a superior representative of the Ministry of Domains would be appointed to make a new recognition of these islands. After completing this process, it was planned to mark the territorial limits by terminals, so that the regiment responsible for border guard and forestry workers had the necessary landmarks to respect the Romanian-Bulgarian border line. A rigorous delimitation, adapted to geological and geographical changes, was beneficial for both the Romanian and Bulgarian fleets.

To clarify the issue, on July 27, 1900, the Ministry of Foreign Affairs was notified by the Ministry of War, Fifth Directorate for the establishment of a joint commission consisting of a marine officer and a delegate of the Ministry of Domains to resolve issues related to the possession of Danube estates, establishing at the same time their area and production. Interesting was the proposal of the Ministry of War on the reasonable compensation of the losing state by changing the regime of the possession of the respective islands. In the case of united islets respect the dividing channel or if the channel disappears through alluvium deposits there is the possibility of delimitation through terminals. However, Romania had the oldest, largest, and richest islands formed on the right side of the Danube Thalweg, the Thalweg limit could not be invoked according to the nominal list established in 1830 under the Treaty of Adrianople. In order not to be suspicious, the participation of some Bulgarian delegates in the discussions was generated by the possible appeals to be analysed and resolved by the Romanian and Bulgarian governments in accordance with the provisions of international laws. In this regard, the appointment of Bulgarian delegates required the intervention of the Minister of Foreign Affairs (Archives of the Ministry of Foreign Affairs 1966, 48).

Against the backdrop of these incidents, Nicolae Misu sent to the Bulgarian government a note of protest brought to the attention of the foreign ministers present in Sofia. The diplomatic note mentioned the limitation of the rights stipulated by the international legislation. The measure ordered by the Bulgarian authorities regarding the refusal of entry in Bulgaria of Romanians even if they had passports with the visa of the Bulgarian

Legation in Bucharest and the impossibility of the personnel of the Romanian vessels sailing on the Danube to go down to ports for various manoeuvres necessary for a good river circulation (Archives of the Ministry of Foreign Affairs 1966, 49).
The situation at the end of August was very tense. The Romanian minister in Berlin was interested in the possibility of representing Romania's interests in Bulgaria by the German diplomatic agent in Sofia. Meanwhile, Romanian troops were discreetly concentrated at the southern border (Archives of the Ministry of Foreign Affairs 1966, 50).

On August 10, 1900, the Ministry of War, Fifth Division, The Navy delegated them to study the Danube islands on the Lieutenant Commander Boerescu Cesar of the Military Navy who knew and was aware of the topographical and hydrological works carried out until this date and lieutenant Stoyanovich Constantin whose mission was to help the members of the commission. The two were to report to the Ministry of Foreign Affairs on August 14, 1900. At the same time, the Ministry of Domains was notified to appoint its representatives. The two officers were remunerated from the Navy budget and the necessary materials were paid by the Ministry of Domains. The representative of this ministry, the forestry inspector Ghehaia, together with the officer Boerescu Cesar completed the map of the Danube in December 1900. On January 31, 1901, this map accompanied by two memoirs were sent to the Ministry of Foreign Affairs of Romania to start the necessary arrangements with the neighbouring states bordering the Danube to establish by mutual agreement river borderline (Archives of the Ministry of Foreign Affairs 1966, 50).

In the mediation of the Romanian-Bulgarian crisis in the summer of 1900 by Bahmetiev, the Russian minister in Sofia, the Bulgarian government ordered coercive measures against members of the Macedonian Central Supreme Committee and punished Boris Sarafov if he was to be found guilty of Romanian justice. In this context, on 6 September 1900, Bulgarian justice pronounced Ciolakov's one-year prison sentence and the possibility of his release on bail. On September 16, 1900, on the occasion of the opening of the works of Sobrania, during his official speech, Bulgarian King Ferdinand said that the disagreements between Romania and Bulgaria were to be resolved (Archives of the Ministry of Foreign Affairs, 50).
Although a diplomatic resolution of the frequent incidents at the river border was attempted, on December 23, 1900, three Bulgarian soldiers from picket no.24 opened fire on a Romanian sentry of picket no. 5 who wanted to stop a Bulgarian smuggler who was clandestinely passing in Romania (Archives of the Ministry of Foreign Affairs 1966, 50).

In April 1901, the Romanian subjects Beitullah Bechir and Iusuf Ibrahim were killed on Romanian territory by Bulgarians Petcu Dinu and Iordan Ivanov, who, although found guilty following the investigation carried out by a joint commission, received a 5-day prison sentence based on their statements that the two victims were smugglers who did not respond to their summons (Archives of the Ministry of Foreign Affairs 1966, 50).

In the spring of 1901, the 2nd Army Corps Command reported to the Ministry of War forays of the Bulgarian inhabitants on the Gasca Mare, Gasca Mica, Cinghina and Bersina from where they were stealing wood. For the intercession of these facts, there was sent on patrol between Giurgiu and Turnu Magurele the „Arges" military boat that was stationed in Zimnicea. On this occasion, port captains in the region were ordered to request Navy ships whenever they found irregularities from Bulgarian and Serbian neighbours. In their support, the light boat type was sent, under the command of sub-lieutenant Coanda Gheorghe who was stationed in Gruia to perform the patrol service between Calafat and Turnu-Severin (Archives of the Ministry of Foreign Affairs 1966, 50).
On February 13, 1901, Alexandru Marghiloman ceased his prerogatives at the Foreign Ministry, shortly before the arrest and trial by the Bulgarian justice of those who planned the assassinations in Bucharest and the plot against King Carol I.

In early April 1901, the sentence handed down in absentia in Bucharest produced legal effects in Bulgaria, meaning that the chairman of the Macedonian Committee in Sofia, Boris Sarafov was arrested along with the other missing convicts. The process started by the Bulgarian judiciary ended with their acquittal on 1 August 1901, but Boris Sarafov's influence and prestige on the committee declined. Bulgarian Prime Minister Petko Karavelov declared to Nicolae Misu immediately after receiving the sentence that he was not satisfied with the final result of the trial, but it was almost impossible to fight against a general political trend above the will of the magistrates. The new leadership of the Macedonian Central Supreme Committee had a moderate trend regarding the Romanian-Bulgarian conflict, encouraging the re-establishment of good neighbourly relations, as a result of the way in which the foreign minister Alexandru Marghiloman managed the Romanian-Bulgarian crisis from 1900-1901 river (Archives of the Ministry of Foreign Affairs 1966, 56).

However, all these events foreshadowed the involvement sooner or later of the two countries in an armed conflict. The provocative attitude supported by the expansionist policy of the government in Sofia determined the involvement of Romania during the Balkan wars (1912-1913) and the asymmetric positioning of the two parties during them.

Conclusion

The terrorist activity/the premeditated anarchy of the Central Macedonian Supreme Committee at the beginning of the 20th century changed and influenced Romanian-Bulgarian relations and the way in which Romania and Bulgaria related to what we call today the international security environment. While Romania was fighting for the preservation of the regional status quo established by the treaties concluded and assumed with legal consequences under international public law, Bulgaria in the 1900s was assimilated to a terrorist state/ an anarchist who provided instability in the Balkan

Peninsula and in the region. Obviously, the terrorist/anarchist actions of the Bulgarian revolutionary secret committees represented a threat to Romania's national security.
Today, more than 100 years after the events mentioned in this article, we identify some common features of the actions of the Bulgarian revolutionary secret committees such as surprise, the diversity of terrorist/anarchist actions, the use of the human being as a weapon with the extreme valences of suicide attacks with explosive devices, the impetuousness, sometimes the lack of tactical and strategic coordination, elements that we quantify today in the phrase confrontation, war or asymmetric threat.

This article is a tribute to the Romanian border guards, Romanian justice, police bodies, Romanian diplomacy and Romanian society since the beginning of the 20th century who protested vehemently against terrorist activity/ anarchists of Bulgarian revolutionary committees aware of the effects of such actions.

References

Adevărul Newspaper. 1990. No.3966/no. 3949.

Arhives of the Ministry of Foreign Affairs. 1966. *Fund Office of studies and documents f.n.*

Atanasiu, Mirela, and Lucian Stăncilă. 2014. *Terrorism — The shadow evil of the beginning of the century.* Bucharest: "Carol I" National Defence University Publishing House.

Bulettin of linguistic and intercultural studies. 2022. No.2.

Dreptul Magazine. 1900. No. 63. Bucharest: Gutenberg, Joseph Gobl Publishing House.

Gazeta Transilvaniei Newspaper. 1900. No.165.

Sinadinoski, Victor. 2017. *The Macedonian Resurrection. The Story of the Internal Macedonian Revolutionary Organization*. U.S.

Telegraful român Newspaper. 1900. No.127. Sibiu.

Tribuna Newspaper. 1907. No. 267.


AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2021-2026
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2021-2026

BIROUL EXECUTIV AL CONSILIULUI ARACIS

EDITOR
„Carol I" National Defence University Publishing House
(Publishing house with recognized prestige validated
by the National Council for Attestation of University
Degrees, Diplomas and Certificates)
Adress: Panduri Street, no. 68-72, Bucharest, 5th District
e-mail: buletinul@unap.ro
Phone: +4021.319.48.80 / 0365; 0453

Signature for the press: 05.07.2024
The publication consists of 166 pages.

510/05.07.2024

C.157/2024