“CAROL I” NATIONAL DEFENCE UNIVERSITY
CENTRE FOR DEFENCE AND SECURITY STRATEGIC STUDIES

STRATEGIC IMPACT

No. 1 [94]/2025

Open-access academic quarterly, nationally acknowledged by CNATDCU, indexed in various international databases and catalogues (CEEOL, EBSCO, Index Copernicus, ProQuest, Crossref, NATO Multimedia Library, WorldCat, ROAD, Google Scholar)

“CAROL I” NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, ROMANIA

EDITORS
Editor-in-Chief: Florian CÎRCIUMARU, PhD, Lecturer
Deputy Editor-in-Chief: Iolanda Andreea TUDOR
Editor: Iulia Alexandra COJOCARU, PhD

CONTACT ADDRESS
Șos. Panduri, no. 68-72, Sector 5, 050662,
Bucharest, Romania
Phone: +4021.319.56.49; Fax: +4021.319.57.80
Website: https://cssas.unap.ro/index_en.htm
E-mail: impactstrategic@unap.ro

Opinions expressed within published materials belong strictly to the authors and do not represent the position of CDSSS/ "Carol I" National Defence University/Ministry of National Defence/Romania.

Authors are fully responsible for their articles' content, according to the provisions of Law no. 183/2024 on the status of research, development and innovation personnel.

ISSN 1841-5784; ISSN-L 1841-5784; e-ISSN 1842-9904

CONTENTS

EDITOR’S NOTE

The most recent issue of Strategic Impact (Volume 94) comprises a diverse array of academic articles featuring research on cybersecurity vulnerabilities in logistics due to emerging technologies, the perception of alliances during the Ukraine war shaped by identity and media narratives, and a case study on the humanitarian impacts of the Russia-Ukraine conflict, focusing on data inconsistencies, resilience, and propaganda’s role in public morale. This volume also includes a book review, and it features the outcomes of the Strategies XXI International Scientific Conference “The Complex and Dynamic Nature of the Security Environment” held on February 27st, 2025.

The first section, ***Political-Military Topicality*** rubric, in the article co-authored by Mr. Viorel Ordeanu, PhD, and Mr. Andronic Benoni, PhD, we are provided a case study-based analysis of the humanitarian dimensions of the Russia-Ukraine conflict, highlighting inconsistencies in health and social data, the impact of combatant and civilian losses on resilience and combat effectiveness, and the strategic us of propaganda in shaping public perception and sustaining morale.

The second rubric of this issue, ***Security and Military Strategy***, comprises an article authored by Mrs. Mirela Atanasiu, PhD, who examines the impact of Russia’s military aggression against Ukraine on international security and the rule of law, highlighting how the conflict challenges legal norms and undermines liberal principles in global governance. Through legal analysis and assessment of affected security structures, the research aims to identify emerging legal challenges and anticipate implications for the evolving international legal and security order.

The ***Emerging Technologies*** rubric presents an article written by Mrs. Daniela-Elena Hrab, PhD Candidate, who investigates in her study the cybersecurity vulnerabilities arising from the increasing integration of emerging technologies in logistics, while offering significant economic, social, and environmental benefits, also expose supply chains to heightened cyber risks, particularly amid low awareness levels. The research addresses a critical gap by exploring opportunities for civil-military cooperation in mitigating these threats. Also, the study stresses the need for a paradigm shift in military logistics support, and identifies ten key domains where enhanced civil-military collaboration is essential.

In this edition, the ***Book Review*** rubric we find the work of Radu Umbreș, titled Living with Distrust, reviewed by our colleague, Mr. Vladimir-Mihai Zodian, PhD. The book explores morality, cooperation, and social norms function in a Romanian village, revealing how deep-rooted distrust shapes relationships, community life, and informal institutions in post-communist rural Romania.

The ***Scientific Event*** rubric brings to the reader’s attention the 24th edition of the CDSSS “STRATEGIES XXI” International Scientific Conference, held in hybrid format on February 27th, 2025, which explores current and emerging security challenges. Key topics included security and defence policies, hybrid threats, climate change, the Russia-Ukraine war, great power rivalries in the Indo-Pacific, Middle East tensions, security dynamics in Africa and Central Asia, and future-oriented strategic scenarios.

Also, this edition includes the ***Guide for authors***, a mandatory reading for those who wish to disseminate their research results in our journal.

For those discovering *Strategic Impact* for the first time, the publication is an open-access peer reviewed journal, edited by the Centre for Defence and Security Strategic Studies and published with the support of "Carol I" National Defence University Publishing House, and, also, a prestigious scientific journal in the field of military sciences, information and public order, according to the National Council for the Accreditation of University Titles, Diplomas and Certificates (CNATDCU).

Strategic Impact is an academic publication in the field of strategic defence and security studies. The journal has been published since 2000 in Romanian, and since 2005 in English, print and online. The journal is currently published exclusively in English. The articles are checked for plagiarism and scientifically evaluated (double blind peer review method). The thematic areas include political science, international relations, geopolitics, the political-military sphere, international organizations – with a focus on NATO and the EU information society, cyber security, intelligence studies, military history, and emerging technologies. Readers will find in the pages of the publication strategic-level analyses, syntheses and evaluations, views that explore the impact of national, regional and global dynamics.

In terms of international visibility the primary objective of the publication the recognition of the scientific quality of the journal is confirmed by its indexing in the international databases CEEOL (Central and Eastern European Online Library, Germany), EBSCO (USA), Index Copernicus (Poland), ProQuest (USA), and WorldCat and ROAD ISSN, as well as its presence in the virtual catalogues of the libraries of prestigious institutions abroad, such as NATO and military universities in Bulgaria, Poland, Czech Republic, Hungary, Estonia, etc.

The journal is distributed free of charge in main institutions in the field of security and defence, in the academia and abroad in Europe, Asia and America.

In the end, we encourage those interested in publishing in our journal to rigorously survey and assess the dynamics of the security environment and, at the same time, we invite students, master students and doctoral candidates to submit articles for publication in the monthly supplement of the journal, *Strategic Colloquium*, available at URL: http://cssas.unap.ro/ro/cs.htm, indexed in the international database CEEOL, Crossref, ROAD ISSN, and Google scholar, ResearchBib and Open Journal Systems.

Editor-in-Chief, Colonel Florian CÎRCIUMARU, PhD
Director of the Centre for Defence and Security Strategic Studies

DOI: 10.53477/1842-9904-25-22

HUMANITARIAN LESSONS IDENTIFIED IN THE CONDUCT OF THE ACTUAL CONFLICT IN UKRAINE

Viorel ORDEANU, PhD[*]
Andronic BENONI, PhD[**]

The authors of this study, conducted a comprehensive analysis of information from various domestic and international sources concerning the humanitarian dimensions of the ongoing conflict initiated by Russia in Ukraine. Their study revealed numerous inconsistencies and inaccuracies regarding the health and social aspects of the parties involved, and conclude on several lessons that should be considered in the context of future conflicts.

Employing a case study methodology, the research focused on assessing the casualties among combatants during major military engagements, as well as the losses sustained by the civilian population, regardless of their national, ethnic, or social affiliations. The analysis examined how these losses impacted the physical and psychological resilience of the affected groups, thereby influencing the overall combat effectiveness of the belligerents in this protracted war.

Furthermore, the study scrutinized the role of wartime propaganda disseminated by both Russian and Ukrainian sources. It analysed how information regarding enemy and own casualties was presented to morale among troops and the general population, highlighting the strategic use of information in shaping public perception and sustaining support during prolonged armed conflict.

***Keywords**: War; Ukraine; Russia; medical intelligence; human casualties; collateral damage; lessons identified.*

[*] ***Colonel (Ret.) Viorel ORDEANU, PhD is a Professor at the "Titu Maiorescu" University, Bucharest, Romania. E-mail: ordeanu_viorel@yahoo.com***

[**] ***Colonel (Ret.) Andronic BENONI, PhD is a Professor and a corresponding member of the Romanian Academy of Scientists, Bucharest, Romania.
E-mail: benoneandronic@tahoo.com***

Introduction

The humanitarian aspects of warfare are intrinsically linked to its sanitary and societal dimensions, with war being characterized as an “epidemic (or pandemic) of political traumas.” These considerations pertain to both combatant and non-combatant forces, as well as to the civilians of both belligerents and neutrals, irrespective of affiliation, nationality, or social status.

In the context of military forces operating under the laws and customs of warfare, it is essential to assess human losses by distinguishing between recoverable (injured) losses and non-recoverable (fatalities) losses. Namely, the actual number and proportion of the wounded, deceased, shipwrecked, prisoners and missing individuals, as well as the reduction of both physical and psychological resilience, thereby influencing the overall combat effectiveness of the belligerents engaged in the warfare.

In assessing the impact of armed conflict on civilians, it is important to consider not only the number of fatalities and injured (i.e., collateral casualties), but also the broader categories of individuals affected by the disaster, including the refugees who have fled beyond national borders. Additionally, the conflict’s biomedical and social impacts on these populations must be considered.

Through indirect analyses, *open source intelligence (OSINT)* and *medical intelligence*, we strive to present a depiction of the situation that closely approximates reality. For military planners, it is imperative to have a comprehensive understanding of the actual situation, both for the conception and conduct of operations, as well as for the organization and provisioning of logistical support and medical services that are integral to sustaining combat activities.

The main international organization addressing humanitarian concerns is the International Red Cross and Red Crescent Movement (IFRC), along with its affiliated branches, in conjunction with the United Nations through the United Nations High Commissioner for Refugees (UNHCR).

The impact of armed conflict on living forces is predominantly addressed through medical interventions, with human casualties (both military and civilian) managed through human medicine, and animal casualties (both domestic and wild) addressed through veterinary medicine. In its broader conceptualization, military medicine encompasses both disciplines. For instance, the original emblem of the Romanian Sanitary Service, created by General Professor Dr. Carol Davila, prominently featured the ancient symbol of medicine and pharmacy (the Rod of the god Asclepius) flanked by laurel branches on the right to represent human medicine, and oak branches on the left symbolizing veterinary medicine. Military medicine, therefore, plays a comprehensive role in addressing the full spectrum of victims affected by armed conflicts – whether encountered in combat or in non-combat settings – dealing with the treatment of injuries and illnesses caused by physical, chemical, or biological agents, with a varying degree of severity and prognosis. This includes the care of shipwrecked individuals, prisoners of war, and other vulnerable groups, as well as the assessment of individuals' fitness for combat, labour, or civilian life, and the certification of deaths.

Drawing upon the current experience and recent military history, it is possible to quantitatively and qualitatively estimate the requirements for sanitary and humanitarian support, as well as the necessary forces, resources, and procedures to optimize medical aid and assistance. However, detailing these aspects extends beyond the scope of this discussion (Ordeanu, Andronic 2022, 240). Moreover, we refer to the concept of "sanitary lessons", which semantically encompasses a broader spectrum than strictly medical considerations.

1. Human Losses in Modern Warfare – A Case Study: Ukrainian Forces in the Contemporary Russo-Ukrainian War

Although the human losses inflicted by belligerents in this conflict differ both quantitatively and qualitatively, they are generally comparable, and their analysis is imperative for understanding the military tactics and strategies employed, as well as for evaluating each side's capacity to sustain prolonged combat operations. The human costs of warfare exert a significant influence on the eventual attainment of victory. However, an exhaustive estimate of Ukrainian military losses remains challenging due to the classification of such data by Ukrainian authorities, with little being published regarding their own casualties.

By gathering and comparing the fragmented and occasionally contradictory data available from the written press and audio-visual media, an approximate estimation can be obtained which, in conjunction with the reported of Russian forces losses, may indicate the magnitude of human casualties in a modern, large-scale conventional war fought between European armies. Unfortunately, we are confronted with the case of the current fratricidal war between Russia and Ukraine, widely considered as the largest European conflict since World War II. As an aside, the very existence and prolongation of this war underscores the limitations of existing international mechanisms in conflict resolution. The United Nations has struggled to effectively manage global peace and address this crisis situation. Similarly, the European Union still lacks the requisite strength to impose peace and enforce a cessation of hostilities and facilitate a durable peace agreement. Furthermore, the United States has signalled a shift in its role, indicating a reduced willingness to serve as the *world's arbiter* in violent disputes.

1.1. Losses of the Ukrainian Army

The official number of Ukrainian military fatalities remains undisclosed, as official data is classified – likely due to concerns that if the Western public were to become aware of the high number of deaths and injuries caused by this war, it might oppose the war support provided by the respective governments. Moreover, not all Ukrainians support the conflict, and some are seeking refuge in neighboring countries. Field observations and testimonies from volunteers in Western countries returning from conflict zones tend to confirm the view that Ukrainian forces suffered considerably higher human losses than Russian forces, while the press never publishes estimates of Ukrainian casualties - presumably to sustain both the illusion of victory over the Russians and to justify ongoing weapons deliveries. (Baud, 2023, 278). However, in science, as in justice, to ensure a balanced understanding of the conflict, the Latin principle of *"Audiatur et altera pars"* ("Let the other side be heard") must be applied.

The Ukrainian strategy of defending every square meter of its territory by holding positions until the end ("centimeter," as U.S. President Joe Biden publicly stated) has led to the significant attrition within its own forces. This approach mirrors historical precedents, such as the protracted trench warfare of World War I and Germany's defensive stance in 1945. However, in the current conflict, the Russians have maintained operational mobility, as evidenced in their defensive actions in 1914 and offensive operations in 1943. Consequently, the Ukrainian military capabilities was destroyed as early as the summer of 2022, rendering the subsequent summer counteroffensive ineffective.

In response to the ongoing conflict, Western allies have compensated by supplying the Ukrainian forces with equipment, weaponry, and ammunition. This assistance extends beyond material aid, encompassing the presence of foreign volunteers with military experience who fought alongside the Ukrainian Reserve Forces, as the Ukrainian International Legion.

Following British Prime Minister Boris Johnson's visit to Kyiv, the Russians feared that the West would not allow the Ukrainians to negotiate peace, given statements such as "we will support Ukraine for as long as necessary" and consequently, the conflict would be prolonged to exhaust Russian resources. Thus, Russian military tactics shifted focus from attempting to destroy the combat equipment supplied from the West - since they were unable to halt the flow of weaponry - to concentrating on eliminating the military personnel operating this equipment.

The war has entered a phase characterized by attritional warfare, where the objective remains the reduction of military potential, not through the destruction of armaments per se but by targeting those who utilize them. Thus, in June 2022, Ukrainian President Volodymyr Zelensky -who de facto commands the Ukrainian Armed Forces as per the Ukrainian Constitution, despite having no military training

– reported that the country was experiencing daily losses ranging from 60 to 100 soldiers, while the presidential advisor reported to the BBC daily losses of 100-200 soldiers killed (Lawler 20232, 6). General St. Twitty of the United States estimated the losses of the Ukrainian army at 200,000 soldiers (Kyrylenco, Roshchina 2023,7). A group working for the BBC (United Kingdom) and *MediaZona* (Russian opposition), analyzing obituaries and funerals, estimated Ukrainian losses at 402,000 dead.

During this "secretive" conflict, military analysis based on *open sources intelligence* (OSINT) – intelligence gathering from public, non-classified sources, primarily conveyed by written and audiovisual media – has developed. While these sources are available to the general public, interpreting them poses challenges due to biases and partial representations of reality, often favouring one side over the other. However, the methodology and professionalism of these analysts are lacking, leading to estimates that may underrepresent actual figures (Google 2022). In October 2022, General Surovikin of Russia (then commander of the invasion forces) stated that the Russian army was not attempting major operations but was simply „sweeping" the adversary without exposing Russian soldiers, which led Western observers to believe in the perceived weakness of the Russian army and to continue the war in the same manner. Nevertheless, it appears that after occupying over 20% of the Ukrainian territory in the East and South, the Russians reached their invasion objective and shifted to a defensive stance. In November 2022, European Commission President Ursula von der Leyen stated that over 20,000 civilians and more than 100,000 Ukrainian soldiers have died since the onset of the conflict, triggering the fury of the Kiev government, which requested that she correct her statement, which was promptly (McGarvey 2022) done with the Ukrainians declaring 157,000 and the Turkish press supporting this estimate (Bouzouina 2023, 3), despite by being bias for supporting Ukraine.

According to Colonel Jaques Baud, a Swiss expert who has served with NATO and the EU, Ukrainian propaganda attributes its own losses to Russians actions and vice versa, creating a mirrored effect. Another approach to addressing the issue involves comparing the artillery ammunition consumption to estimate casualties on both sides of the frontline. Ukrainian and Western military officials have calculated that Ukrainians fire between 2,000 and 4,000 heavy artillery shells daily, whereas Russian forces fire between 40,000 to 50,000 shells, which is 10 to 25 times more. On average, this equates to approximately 45,000/3,000, or about 15 times more, suggesting that the human losses could also be 15 times higher on average. While difficult to confirm, this method provides a calculable metric, unlike casualty figures reported by the media without a basis for comparison.

An alternative approach to addressing the issue involves analyzing the manpower of the belligerent armed forces. In May 2022, President Zelensky stated that Ukraine's armed forces comprised 700,000 personnel (Dumitrache C. 2023, Google 2022), and in July 2022, the Ukrainian Minister of Defense announced: „We have approximately 700,000 soldiers, to which the National Guard, Police, and Border Guards are added, bringing us close to a million". In September 2022, the German newspaper *Frankfurter Allgemeine Zeitung* described the Ukrainian army as the second most powerful in Europe, with 250,000 combatants (Zeleb 2023), likely referring to peacetime strength. For comparison, Russian forces engaged on this front were estimated at between 100,000 and 200,000 soldiers.

The battles in western Donbas play a key role in this analysis. At the beginning of 2023, in the city of Bakhmut, which still housed Ukrainian troops, the fighting became tragic. Although the city did not hold a particular strategic importance, the Russian army and the militia of the Donetsk People's Republic aimed to capture it to consolidate control over Donbas, while the Ukrainian army and volunteers (whom Russian sources labeled as "neo-Nazis") sought to maintain its status within Ukraine due to its symbolic political importance. In the initial stage, the West observed the heroic resistance of the Ukrainians and the accumulation of casualties on the Russian side. Subsequently, the press reported severe losses on both sides, drawing comparison to the battles of Verdun in World War I. However, by the end of winter, reports began to reflect the substantial toll the fighting had taken on Ukrainian forces.

It has been demonstrated that the old myth of "waves of infantry" launching attacks is no longer relevant, nor is the heavy concentration of forces for "breakthroughs", which were employed in specific situations during the world wars. These tactics are counterintuitive in modern warfare because, when using firearms, combatants must be as dispersed as possible and avoid exposure to infantry fire. However, what is valid at the tactical level is not always applicable at the operational level. The fact that the Ukrainian army received modern weaponry in staggered, small quantities facilitated the destruction of this equipment on the front lines, preventing the achievement of a "critical mass" necessary for the „principle of saturation". This assistance, which was inefficient and sometimes delayed, seems to suggest that the allies were not seeking a Ukrainian victory, but rather the prolongation of the war to exhaust Russia (Baud J. 2023, 278).

The anticipated ***Ukrainian counteroffensive*** began with the mobilized Ukrainian military receiving armament and ammunition (Soviet-type from former communist countries and NATO-type from other allies), as well as support from foreign volunteers with combat experience, substantial financial aid, and political backing. Ukrainian forces also benefited from up-to-date intelligence and NATO military leadership through American and British strategists and tacticians. It was not until the spring of 2023 that the counteroffensive began tentatively and with repeated delays, eventually evolving into what could no longer be called a counteroffensive but rather a ***Ukrainian offensive***, gaining momentum during the summer and continuing into the autumn with some local successes. Overall, these were small tactical attacks at the subunit level, supported by armoured vehicles and artillery, but lacking air support due to the loss of air superiority. With the onset of autumn rains, the pace of the offensive slowed significantly and came to a near standstill by December 1, 2023, with the promise of a forthcoming winter offensive. However, given the extensive human and material losses (in fact, of both belligerents) and the high consumption of ammunition (especially heavy artillery shells, missiles, drones, etc.), it became clear that launching another offensive would not be feasible and that such promises were overly optimistic. Furthermore, the Ukrainian Air Force had lost control of both the airspace and the battlefield.

Under these unfavourable conditions, the Ukrainian army, technologically supported by Western allies, launched an attack into Russian territory and seized control of the Kursk region. This action proved to be nearly suicidal, as the Russian military bolstered tactically by the equivalent of a North Korean infantry division, swiftly retook the territory and encircled the equivalent of a Ukrainian division. However, Kyiv refused to acknowledge the situation and rejected the military surrender, resulting in increased human losses (*unnecessary excess mortality*) (Ghubotin 2025).

It seems that the tactics, operations, and strategies outlined in NATO regulations, which advocate for expeditionary actions akin to "Blitzkrieg", proved less effective in a classic positional war with fixed frontlines, as reflected by the situation and the level of readiness of the Ukrainian military. This discrepancy in approach likely gave rise to tensions among Ukrainian commanders, as well as between these commanders and their allies, and between the military leadership and the country's political leadership. These contradictions were expressed in an interview with General Zalujni, who was then serving as the Chief of the General Staff of the Ukrainian Armed Forces.

As a result, support from the United States and European support has diminished, leading to the cessation of war funding through the U.S. Congress and the transfer of responsibility to the EU, which is also facing challenges in this regard. It appears that the promise of supporting Ukraine "for as long as necessary" has reached its end, and it should be noted that the Ukrainians were not misled, there was no explicit promise of *victory* or *peace*, only a vague notion of *necessity* - a term that implies no concrete commitment. In this increasingly unfavourable context for the alliance, two main scenarios can be envisioned.

Another ***predominantly military*** scenario involves a final major effort to support Ukraine, both materially and financially, including the deployment of ultra-modern weaponry (which has so far been absent from the battlefield). This could involve F-16 and F-18 aircraft (which also possess nuclear capabilities), *stealth* bombers, next-generation missiles, and advanced tanks (such as the promised *Abrams*, which have not yet been delivered to the front lines). While Ukrainian soldiers may lack the training or time effectively operate this equipment, a strategy similar to those used in various 20th-century wars could be employed – discreetly sending these weapons along with specialized combat and maintenance teams, disguised as *volunteers*. The risk is that even these might not influence the situation on the front, and some could fall into enemy hands, enabling them to upgrade their combat techniques through reverse engineering. There have also been attempts to form a coalition of volunteer states to deploy troops to Ukraine, alongside existing foreign volunteers and mercenaries, but this has not been finalized due to opposition from the USA, which seek to avoid escalating the conflict into a world war.

An alternative, ***predominantly political*** scenario would involve reaching a peace agreement or at least a humanitarian armistice, potentially with some sacrifices, but aimed at preventing the adversary from capitalizing on their victory. This political resolution would be presented by the media as a triumph for the international community, allowing for extensive criticism of the victor from all perspectives and a carefully crafted narrative of the situation. Such an approach would enable the perpetuation of a ***frozen conflict*** zone, which could be reactivated at any time with appropriate forces and resources to achieve a real victory. The key advantage of this approach would be its reduced cost, thus increasing its likelihood of success. The attempt by U.S. President D. Trump to mediate peace following this model failed because the belligerents do not negotiate directly with each other, as Ukrainian legislation prohibits negotiations with Russia, making any negotiator liable to charges of high treason.

1.2. Ukrainian Population Losses

Given that the conflict is unfolding on Ukrainian territory, there is clearly a significant incidence of both human and material losses among civilians. If we consider civilians as non-combatants, it is already evident that substantial civilian casualties – termed “collateral casualties” – occur, even during so-called “surgical” military operations, with figures amounting to tens of thousands. As per the Laws of Armed Conflict is right they are called “collateral casualties.” But for Kremlin, the civil infrastructure and population were considered strategic objectives and targets, especially from 2023 onward, being directly targeted by the Russian Air Force. This approach is reminiscent of Romania’s experience under Anglo-American aerial bombing during War World 2 (1944) (Ordeanu, Andronic 2025). However, the current situation differs, as the the scale and nature of civilian losses have resulted in a marked shortfall of the country’s available human resources.

Military leaders had planned to mobilize hundreds of thousands of men and women, as stated by President Zelensky during the year-end press conference on December 19, 2023. Nonetheless, the Ukrainian armed forces face significant challenges in enlisting additional combatants. This difficulty is attributed to a shrinking demographic base and issues of corruption associated with the conscription process in 2023, as highlighted by *The Daily Digest* in its report "Conscription and corruption issues in 2023 revealed a lot." (The Daily Digest, 2025). Furthermore, large-scale emigration of citizens to other countries, including Romania, has further complicated recruitment efforts.

It is evident that the media sometimes contradicts even official Ukrainian statements, occasionally disseminating hate messages in violation of the Munich Charter. Notably, the same *media* outlets largely ignored the civilian casualties in Donbass from 2014 to 2022, as well as similar incidents. Had these events received greater attention, this criminal military intervention, which U.S. President D. Trump described as „the war that should never have existed," might not have occurred. Trump also noted that Russia and Ukraine were very close to reaching an agreement and emphasized the need for high-level negotiations.

Meanwhile, the population has been severely impacted by the deteriorating living conditions, intensified by Russian attacks, and the inherent risks of war, leading a significant portion to seek refuge either within the country or in neighbouring states. According to the United Nations High Commissioner for Refugees, as of January 2023, over 5 million Ukrainians had sought refuge in neighbouring countries, with more than half in Russia and the rest dispersed across the European Union, Moldova, Belarus, and other regions (Baud 2023, 278). This has drastically reduced the recruitment base for the military and the economic capacity of Ukraine.

Propaganda has attempted to convey to the public that Ukraine is prevailing in the conflict, with the support of its allies being effective, and on the other hand, that Ukraine is much less affected by the war than Russia. The strategic goal of weakening Russia militarily, economically, and financially was evidently to neutralize the main ally of the People's Republic of China, which economically rivals the United States. Furthermore, the two allies are jointly working toward establishing a new multipolar world order to replace the current unipolar system (often reffered to as the American Century), which followed the bipolar order of the post-World War II era. Thus, from a political perspective, this vision places them in fundamental opposition to the values and interests of Western civilization, to which we belong.

The political and economic struggle to maintain a unipolar global order has proven to be both challenging and, sometimes, unpredictable. For the European Union and NATO to continue functioning, sustained and creative efforts must be made, and the provisions of *International Law* must be applied and respected. Most importantly, fostering mutual understanding between the world's nations is necessary to advancing peace and international cooperation. Without such efforts, as recent events have shown, a world war with or without nuclear weapons remains an ever-present possibility.

As the war in Ukraine draws to a close, a preliminary tally of human losses can be made. More than half a million military personnel, both Russian and Ukrainian, have been lost. When civilian casualties on both sides are included, the total surpasses one million lives. Additionally, millions are internally displaced or have sought refuge in neighboring countries such as Poland, Slovakia, Hungary, Moldova, and Romania, with many emigrating further to the West. These human losses represent a significant depletion of military and economic resources for Ukraine, which are likely to have have long-term consequences for a country already facing instability, inadvertently playing into Russia's strategic interests.

Le Monde (France) wrote, "Behind the secrecy of military losses in Ukraine, a large-scale massacre," noting that: "Kyiv and Moscow are minimizing or keeping silent about the number of soldiers killed and wounded. The losses on both sides are comparable to those of the First World War" (Pop, 2023) and, certainly, they are the highest losses of these two armies since the Second World War. The figures presented by *Le Monde* align with previously reported data, lending credibility to the information.

Human casualties are inherent to any conflict - whether through death, injury, shipwrecks, disappearance, prisoners, etc., or displacement. These factors can impact the combat capabilities of the military and the resilience of the civilian population. For this reason, efforts are made to conceal the actual data from public view. However, for military planners, access to accurate data is essential as it forms the basis for "lessons learned" which can transform military strategy at the tactical, operational, and strategic levels.

For guidance in this domain, the available OSINT documents offer a realistic and informative overview. It is evident that human losses in modern warfare are substantial, comparable to those seen during the World Wars. However, contrary to expectations, they have not exceeded those levels, despite the use of modern weaponry, which is more precise, has greater range, and explosive force. Thus, theoretically more effective, they are not always efficient in practice. Additionally, the ratio of critically and moderately injured remains consistent (minor injuries are not included in statistics), but the proportion of fatalities relative to injuries has decreased, in accordance with the "severity pyramid" model. This can be attributed to the increased efficiency of medical services, which have the appropriate logistical capabilities and resources for the care of the injured, significantly reducing mortality.

2. Human Losses in Modern Warfare – Case Study: Russian Forces in the Current Russian Ukrainian War

Human losses refer to the removal of combatants from battlefield and are typically classified into two categories: irrecoverable losses - those killed in action (KIA) or outside of it (accidents, illness, etc.), or recoverable or partially recoverable losses – those wounded in action (WIA) or outside of it, illnesses (common or epidemic, infected, poisoned, burned, radiation exposure, etc.), shipwrecked, prisoners, arrested, deserters, missing in action (MIA).

The summary of human and material losses will lead to the exhaustion of the belligerents, ultimately necessitating an armistice or the conclusion of peace. Throughout history, all wars, regardless of their nature or era, have caused significant human and material damage with the aim of defeating the adversary. A potential nuclear war could result in billions of human casualties and material losses, or even the collapse of modern civilization.

In 2022, the Russians believed they would be welcomed by their Ukrainian brethren with open arms, akin to the Germans in Austria, in 1939, or in East Germany in 1989. However, the intelligence services, either incompetent or treacherous, failed to accurately assess that, since 2014, Ukraine has been gradually distancing itself from Russia and the Commonwealth of Independent States (CIS), aligning itself increasingly with NATO and the West. This process is part of a broader historical trajectory that began after World War I, continued through World War II, and has resumed in the present era (Carrere d'Encausse, 1993).

Therefore, the Russian military found itself ensnared in a meticulously prepared deadly trap. The assault on Kyiv resulted in a tactical failure, and the Chechen Strike Group was annihilated en route to its objective. The Russian strategy of conducting a "special military operation" was inadequate from the outset and had to be improvised along the way, leading to significant losses. By refusing to officially classify the conflict in Ukraine as a war, the Kremlin was unable to declare total or partial mobilization and permanently replace its forces in the Joint Operation Area (JOA).

Contemporary military doctrines theoretically advocate for intelligent combat actions that minimize human casualties, including the number of wounded and ill, thereby avoiding unnecessary "excess mortality" when feasible. In practice, however, the role of commanders at all levels is crucial in conducting operations at tactical, operational, and/or strategic levels in such a manner that physically minimizes (or at least minimizes in media portrayal) human losses, both recoverable and irrecoverable, as well as material losses and damage to prestige.

This entails the preparation of appropriate logistical and medical resources, both quantitatively and qualitatively, to treat the wounded and ill within the fighting forces and to maintain combat readiness. As for understanding the realities of ongoing wars, *being balanced means knowing all perspectives*, in line with the motto of TV NCN Romania. The British press reports that Russian human losses in this war are approaching a new record, being around one million (Google 2025, The

Daily Digest).

2.1. Russian conventional operation in Ukraine

This subchapter explores Russian conventional military operation in Ukraine alongside its use of war propaganda. While it is expected that warring parties will engage in propaganda, yet it tends to exaggerate enemy losses and downplay their own to maintain the morale of both troops and civilians, as well as that of their financial backers. This action is supported by censorship (both military and media-related), although its effects may have unintended consequences. Analyzing how news is presented in mainstream *media* (audiovisual and print), it is noticeable that certain errors in approach persist. Moreover, a new phenomenon has emerged: the use of words with altered meanings (with recent examples reported in war, economic, and medical developments).

We believe that for "actors" actively involved in the decision-making (both military and political) it is crucial to accurately assess the situation to act accordingly and derive meaningful lessons for the future. This underlines the importance of Psychological Operations (PSYOPS), which are tailored to target friendly forces, adversary forces, and international public opinion differently. Additionally, Open Source Intelligence (OSINT) is valuable not just for sensational press articles for the public, but for the actual documentation of those involved or potentially involved in ongoing or future developments. As the folklore saying goes, "intelligent people learn from the mistakes of others, whereas fools fail to learn even from their own".

The ongoing Russian-Ukrainian War, which commenced as a "special military operation" with specific objectives, became stagnant after almost 20% of Ukrainian territory (areas predominantly inhabited by ethnic Russians, often inaccurately labelled as merely Russophones) was occupied through dynamic actions involving armoured and air forces, reminiscent of the tactics used during the Second World War. Subsequently, the conflict has transitioned into a phase of positional warfare, akin to the First World War. In this situation, the Russians constructed a triple defensive line behind the temporary front line. The first line comprises trenches, light weaponry, anti-tank obstacles, and barbed wire, fronted by extensive minefields. The second line - the main one -, includes fortifications, bunkers, anti-tank weaponry, and collective shelters. The third line is designated for artillery, reserves, command posts, logistic support, medical support, supply lines, and lateral movement routes. Combat has primarily involved intense artillery duels, aerial strikes - particularly with drones and missiles - and tactical operations at the subunit level, including feigned attacks. The primary targets have included military objectives, energy infrastructure, strategic nodes, and critical elements of national infrastructure. The intent is to reduce the capacity of the Ukrainian army while eroding civilian morale, similar to NATO's approach in Yugoslavia in 1999.

The Russian aerial superiority has hindered the Ukrainian air force from providing support to ground troops, and thus, the anticipated "Battlefield Air Interdiction 2000" scenario did not materialize as expected. Conversely, at sea, the deployment of aerial drones (provided by Turkey) and naval drones (supplied by the United Kingdom) resulted in the sinking of multiple vessels and forced the Russian Black Sea Fleet to virtually abandon its naval base in Crimea and retreat to Novorossiysk. Strategically, the Ukrainians, with NATO support, targeted the Kerch Strait bridges, the port of Sevastopol, Russia-Germany undersea gas pipelines, certain military airfields in Russia, and both military and civilian vessels in the Black Sea, etc.

The recent Russian winter offensives have achieved partial success, but have also resulted in increased human losses due to the harsh conditions imposed by *General Winter*. To date, the situation seems relatively balanced, with both armies experiencing significant losses in personnel and combat equipment, as well as widespread economic damage. This situation may lead to ceasefire or peace negotiations, even if the initial strategic objectives remain unfulfilled. This could lead to the emergence of a new frozen conflict, stabilized by the recent Agreement on Minerals signed by Ukraine and the USA.

2.2. Losses of Russian Forces

Since the inception of the Russian invasion, the Ukrainian and Western narratives (primarily NATO and the EU) have predicted the defeat of the Russian forces, praised the unexpected resilience of the Ukrainians, and highlighted the inability of the Russian president to rationally assess the risks of the war. Some publications have speculated about his health, labelling him as ill, mentally unstable, or even close to death. The emphasis has been on the notion that Russian losses, both in personnel and equipment, are significantly higher than those of the Ukrainians, thereby triggering a "numbers war" in the media and official statements. This conflict is underpinned by secrecy, maintained through excessive censorship designed to obscure the actual figures from public view.

Examining the number of Russian casualties reveals that pro-Ukrainian media systematically employs the "mirror" technique in strategic communication, hence reversing the data might be closer to reality, as assessed by Colonel Jacques Baud, a specialist in military intelligence from Switzerland, and an expert at the UN and NATO (Baud, 2023, 278; Mazurenko 20227). The objective of this approach is to demonstrate to the public that Russia must and will be defeated.

The terminology used in media reporting support the manipulation of data, such that the term "human casualties" (encompassing deaths, injuries, disappearances, etc.) is often used synonymously with "fatalities", creating confusion regarding the timing, source, and nature of the figures. While the number of deaths is in the thousands, not tens of thousands, the human toll remains tragic. Nearly one thousand Russian military personnel die each month in operations involving over

100,000 ground forces. Additionally, there are losses suffered by other armed forces, separatist militias, Wagner mercenaries, pro-Russian Chechen forces, Russian and foreign volunteers, who have their own human losses. Moreover, military and civilian personnel in Russian territory or neighboring countries, bombed mistakenly or intentionally by Ukrainian forces, as reported in the Romanian press, add to the numbers. There are also victims resulting from invasions into regions such as Kursk and Belgorod.

The available data suggests that Russian combatant losses are approximately 1% per month, equating to over 10% annually. This attrition reduces overall combat capacity and necessitates not only for personnel replacements but also the rotation and withdrawal of units for recovery. Consequently, partial mobilization has been declared in Russia to reinforce the fighting forces.

Throughout the conflict, Ukraine has consistently reported Russian losses. Nine months after the start of the Russian invasion, the Ukrainian General Staff announced that Russian losses totalled over 86,000 personnel (Baud, 2023, 280), a figure which Yahoo News raised to 88,800. President Zelensky predicted that there would be 100,000 deaths, and on December 22, 2022, the threshold of 100,000 Russian deaths was commemorated in Kyiv by projecting the number “100 K” onto the National Library (Olearchyk, Rathbone. 2023). However, on the same date, the Russian opposition reported through MediaZona 10,229 deaths, while official Russian sources continued to withhold casualty figures.

There is a noticeable and often intentional misuse of terminology, where terms like “deaths” and “human losses” are used interchangeably, where indeed the differences are of an order of magnitude, yet the public may fail to perceive the significance.

A journalistic investigation (MediaZona and Meduza) utilizing open-source information provides an overview of the losses suffered by the Russian army in the war in Ukraine, one of the Kremlin’s most closely guarded secrets. Through statistical modelling, it was estimated that approximately 47,000 Russian men under the age of 50 have died in this war, with about 25,000 in the first year and 22,000 in the second. It can be concluded that although firepower has significantly increased, the impact on the human force remains roughly the same, and the proportion of deceased is lower due to the increased efficiency of logistic and medical support to the forces.

In January 2023, Chief of the Norwegian Armed Forces, General Kristoffersen, stated to the press that “Russian losses are approaching approximately 180,000 soldiers killed or wounded”, without specifying the source of these figures, according to Agerpres. In August 2023, The New York Times, citing American officials, indicated that Russian military losses were nearing 300,000, including 120,000 deaths and 170,000-180,000 wounded, significantly more than Ukrainian losses. The British press recently published an article stating that Russian human losses are approaching a new record, with the Russian armed forces alone having suffered nearly one million casualties since the onset of the invasion of Ukraine on February 22, 2022 (Euronews 2022, The Daily Digest 2025).

It is peculiar that although the Russians possess the capability to conduct not only *joint operations* but also *multi-domain operations* (including land, air, naval, space, electromagnetic, cyber, information, etc.), and Ukrainians, supported by NATO and the EU, could do the same, the war appears to be waged in a conventional manner, reminiscent of world wars, or at least that is the impression given. While modern and outdated weaponry is being used, neither side has deployed advanced, state-of-the-art weapons on a large scale. The belligerents have used prohibited weapons, such as landmines and cluster munitions, but since neither Russia nor Ukraine had ratified the relevant international treaties banning them, their use is legal, albeit unethical.

It is possible that advanced technical means are being reserved for a later, decisive phase of the war. Alternatively, they may not be as effective as propaganda suggests, similar to the "wonder weapons" of the Nazis. Another possibility is that these systems are being preserved for a potential *future conflict* between major powers.

As a political demonstration that this war does not pose an existential threat to either of the belligerents and that the actual risk of regional or global escalation is minimal, the President of France refused to prioritize the discussion regarding Ukraine at the 2023 G20 Summit. Moreover, the final joint declaration of the G20 refrain from condemning Russia over the conflict in Ukraine, reflecting "a consensus that does not upset anyone, neither Russia, nor China, nor the Western states" (Fuhr, 2025).

A comparative analysis of the losses by both belligerents could offer valuable insights and *lessons* for the future, as the current conflict involves two modern military powers and foreshadows what might occur in a future war. However, it is entirely different from the mutual destruction war between Palestinians and Israelis, which does not adhere to the laws and customs of war.

Although the laws, customs, and conduct of warfare evolve in accordance with technological advancements and political morality, suggesting that tactics, operations, and strategy will be optimized, and that there will be a new paradigm of warfare in the future, there remains a conceptual inertia. It appears that the failures of the current modern Russian-Ukrainian war have not yet led to meaningful implementation of any "lessons learned" from this unnecessary disaster[1], (Lawrence 2025) which should not have occurred, as recently stated by the President of the United States, Donald Trump.

[1] Patrick Lawrence "La defaite, et surtout ne tirer aucun ensaignement de ce desastre inutile" Mondialisation.ca, 30 Avril 2025 (https://www.mondialisation.ca/la-defaite-et-surtout-ne-tirer-aucun-enseignement-de-ce-desastre-inutile/5698236?doing_wp_cron).

2.3. Russian population losses

The Russian population has incurred substantial losses throughout this conflict, including fatalities, injuries, prisoners of war, and displaced individuals. In the period preceding the "Special Military Operation", approximately 15,000 casualties were reported during the clashes involving separatists in the Donbas region, including both voluntary armed forces and Russian civilians (most of whom held Ukrainian citizenship) residing in the combat zones. Following the initiation of the invasion, collateral damage occurred as a result of combat operations in border regions and areas subjected to bombardment, including Moscow.

Russian civilian casualties have been relatively substantial; though exact figures remain unreported. These casualties primarily resulted from Ukrainian incursions into Russian regions such as Kursk and Belgorod, as indicated by media sources. However, given the quantity and explosive power of modern munitions used in the conflict, the relatively low number of fatalities and injuries on both sides suggests that the belligerents did not specifically target civilians, unlike the tactics commonly employed during World War II. Instead, these casualties are more accurately classified as collateral damage. Comprehensive and definitive data regarding these incidents is likely to emerge only upon the cessation of hostilities.

3. The humanitarian lessons identified

The ongoing Russian-Ukrainian War represents a traditional conventional conflict, conducted between the world's largest nuclear power and a former nuclear power, amid propaganda-fueled threats of tactical nuclear strikes. Although both belligerents possess the capability to conduct multi-domain operations, these remain merely independent single service or joint operations.

Casualties and material losses fall within the known limits from 20th-century wars, without causing particularly severe disruptions. Nevertheless, wartime propaganda is intense and creates an exaggerated perception of the situation.

Both belligerents conceal their human losses, with only one remaining silent and the other disseminating misinformation, making it challenging for an external observer to form an accurate picture of the war casualties. Reliable information is vital for drawing lessons from ongoing conflicts, especially as they occur closer to our own regions.

The collective West possesses the capability to obliterate Russia (or any other country) at any given moment but refrains from doing so for several reasons. Firstly, the destruction of a state generates numerous international issues, resulting in chaos that is difficult and expensive to manage. Secondly, the Russians claim to have acted within the boundaries of International Law, in 2014, citing the right of self-determination of nationalities, which led to a predominantly verbal response from public opinion. In 2022, they argued that their actions were in accordance with the UN Charter's obligation to protect (the Russian nationality). This is also why they referred to their actions as a special operation rather than a war. Consequently, Western nations could legally assist Ukraine but refrained from deploying troops.

The Ukrainians have consistently conducted acts of war on Russian territory, including in Moscow, with the aim of provoking Russia into officially declaring war, which would grant them the right to form combat alliances. Western leaders, including President Macron, along with other state leaders, have clearly understood this strategy and have publicly articulated the Western approach of participation without direct involvement to avoid escalation.

Upon the official conclusion of this war, the "lessons identified" will be systematically documented and likely applied, including humanitarian considerations, to future conflicts, the timing of which remains uncertain. We currently observe an illustrative example of these principles in the ongoing war in the Near East, which shows a tendency to extend into the Middle East and represents a model for future conflicts. These future wars are expected to feature theaters of operations rather than well-defined fronts.

At present, two distinct models of warfare with potential for globalization are unfolding. It is probable that future realities will integrate these models into a unified concept for maximum efficiency.

The Latin expression "Vae victis!" (woe to the vanquished) encapsulates the fate awaiting the defeated. However, neither is a "Pyrrhic victory" desirable, as King Pyrrhus himself remarked: "One more such victory, and I am lost".

Conclusions

We are witnessing and indirectly participating in the first modern conflict between the military forces of a nation subjected to the aggression of a major global power.

The strategies and tactics employed in this conflict have undergone significant evolution. Initially intended as a "lightning war" designed to minimize human and material losses akin to those seen in World War II, the confrontation transformed into a positional warfare reminiscent of the same era. This shift involved substantial quantities of modern weaponry and an immense consumption of ammunition, resulting in notable human casualties. However, these losses have remained within the threshold observed during major battles of the world wars. Over time, the conflict has progressively transitioned into a war of attrition.

Medical casualties are approximately equivalent between the two sides, in number and severity, with both belligerents possessing modern and effective medical support systems.

The medical services have successfully mitigated the enhanced destructive capacity of modern weaponry, resulting in a lower ratio of fatalities to injuries, thereby demonstrating improved operational efficiency.

Civilian casualties remain minimal relative to military losses, indicating that the laws and customs of war are generally adhered to, notwithstanding official statements and the propagandistic accounts presented in the media.

The provisional lessons identified will eventually be consolidated into established "lessons learned" to guide future conventional warfare preparations (*Si vis pacem, parabellum*). However, it remains uncertain whether these lessons will hold relevance in the event of the outbreak of a potential World War III (advocated by certain factions), which would likely involve nuclear weapons in nature and poses a significant risk of destroying human civilization as we know it.

BIBLIOGRAPHY:

Baud J. „*Ukraine entre guerre et paix,* Edition Max Milo, Paris, 2023.

Bouzouina M. "Bachmut se poursuit, deux ponts ont ete detruits par les Russes" Le Parisien, 5 Mars 2023 (https://www.leparisien.fr/international/guerre -en-ukraine-la-bataille-de-bachmut-se-poursuit-deux-ponts-ont-ete-detruits-par-les-russes-suivez-notre-direct-05-03-2023-3.php)

D'encausse H. C., *Imperiul spulberat. Revolta națiunilor în URSS*, Editura Remember, Bucharest, 1993.

Dumitrache C. "Aproape jumatate de milion de militari, pierderi in razboiul din Ucraina" Facebook, 19 August 2023.

Fuhr L. "Die zweinstarkste Armee Europas" Frankfurter Allgemeine Zeitung, 16 Sep 2022 (http://www.faz.net/aktuell/politik/ausland/armee-der-ukraine-ist-die-zweits-taerkste-in -europa-1.html); Declarația comună adoptată în cadrul Summitului G20 nu condamnă agresiunea Rusiei împotriva Ucrainei, stârnind revolta Ministerului de Externe de la Kiev (mea.search.yahoo.com/search?ei-UTF8&p-Declarația+comună+finală+G20).

Ghubotin K., Globai Look Press, "Kiev rejects Putin's offer of mercy for troops in Kursk", 16 Mar 2025 (https://www.sott.net/article/498472-Kiev-rejects-Putins-offer-of-mercy-for-troops-in-Kursk).

Google 2023 http://facebook.com/sharer/sharer.php?u=https://www.euractiv.ro/extern/in-spatele-secretizarii-pierderilor-militare-din-ucraina-un-masacru-pe-scara-larga-6)

Google 2022 700.000 soldiers defending Ukraine now, Zelensky says, as battles rage in the Donbas" Euronews/AP/AFP, 21 mai 2022 (http://www.euronews.com/2022/05/21/live-sieverodinietsk-shelling-brutal-and-pointless-zelensky-says-as-russia-continues-offe)

Google 2024 Russian casualties are approaching a terrible new milestone, The Daily Digest (https://www.msn.com/en-us/news/world/russian-casualties-are-approaching-a-terrible-new-milestone/ss-AA1EasBO).

Google 2024 Ukrainehasserioustroopconscriptionproblems, TheDailyDigest,_ https://thedailydigest.com/singapore/archivo/ukraine-has-serious-troop-conscription-problems

Kyrylenco o, Roshchina O. "Batallion cammander of 46th Brigade demoted after Washington Post interview and resigns" Ukrainska Pravda, 20 Mars 2023 (https://www.pravda.com.ua/eng/news/2023/03/16/7larga_3042053.html

Lawler D. "Ukraine suffering up to 1.000 casualties per day in Dnbas, oficial say" Axios, 15 June 2022 (https://www.axios.com/2022/06/15/ukraine-1000-casualties-day-donbas-arakhamia); Anthony Katie "Ukraine has lost more troops during the Russian invasion than more are infantry in the British army, defense expert says" Business Insider, 28 June 2022 (https://www.businessinsider.co./ukraine-has-lost-more-troops-than-there-are-in-the-british-army-expert-2022-6)

Lawrence P. "La defaite, et surtout ne tirer aucun ensaignement de ce desastre inutile" Mondialisation.ca, 30 April 2025 (https://www.mondialisation.ca/la-defaite-et-surtout-ne-tirer-aucun-enseignement-de-ce-desastre-inutile/5698236?doing_wp_cron).

Mazurenko A., Ukrainska Pravda (https://www.pravda.com.ua/news/2022/06/9/7/)

Mcgarvey E. "Ukraine aims to amass million strong army to fight Russia, says defence minister" BBC News 11 Jul 2022, (https://www.bbc.com/news/world-europe-6); Fuhr L. „Die zweinstarkste Armee Europas" Frankfurter Allgemeine Zeitung, 16 Sep 2022 (http://www.faz.net/aktuell/politik/ausland/armee-der-ukraine-ist-die-zweits-taerkste-in -europa-1.html)

Mcgarvey E. "Ukraine aims to amass million strong army to fight Russia, says defence minister" BBC News 11 Jul 2022, (https://www.bbc.com/news/world-europe-6)

Olearchyk R, Hall B, Rathbone P. "Bachmut: Ukrainian losses may limit capacity for counter-attack" The Irish Times, 9 March 2023.

Ordeanu V, Andronic B. *Retrospective analysis of human and material losses in Romania, under aerial bombardments, during the World Wars* Annals series on Military sciences, vol 17 iss 1, 2025.

Ordeanu V, Andronic B. *of the military sanitary service and by default, of the national health service system, in multi-domain operations,* Bulletin of Carol I National Defence University, 3, 2022.

Pop R., “În spatele secretizării pierderilor militare din Ucraina, un masacru pe scară largă”, https://www.stiripesurse.ro/in-spatele-secretizarii-pierderilor-militare-din-ucraina-un-masacru-pe-scara larga

Von Der Leyen statement about death of 100,000 Ukrainian soldiers cut from speech” The New Voice of Ukraine, 30 nov 2022 (https://english.nv.ua/nation/von-der-leyen-statement-abaut-death-of-100-000 ukrainian-soldiers-cut-from-speech-5.html)

Zeleb E. “Ukraine’s military wants more soldiers but is isn’t that easy” The Daily Digest, Discover, Microsoft, 22 Dec 2023.

DOI: 10.53477/1842-9904-25-23

THE IMPACT ON INTERNATIONAL SECURITY AND THE RULE OF LAW. THE RUSSIAN MILITARY AGGRESSION IN UKRAINE[*]

Mirela ATANASIU, PhD[*]

Russia's military aggression against Ukraine has significantly impacted both the international security system, by shifting paradigm regarding the conduct of conflicts in the 21st century, and also the rule of law, by undermining liberal principles that form the foundation of the current international relations system. Moreover, the ongoing war between Russia and Ukraine, carried out through violation of general legal norms and the principles of international humanitarian law, has generated, and continues to do so, a range of consequences in the system of international law.

The purpose of this research is to underpin key concepts concerning the impact on international security and the rule of law resulting from the proliferation of the Russian Federation's military aggression in Ukraine and the continuation of the war that began in 2022. The main objective of the analysis is to foresee future legal challenges in the context of the transformation of the international security system and the ongoing reform of its legal framework. To this end, the study follows several stages of research: a legal analysis of the criteria for categorizing Russia's actions as military aggression; an examination of how certain elements of the international security system have been affected; and an assessment of the effects of this conflict on the system of international law.

Keywords: *aggression; abusive war; paradigm shift; security challenges.*

[*] *This paper was presented at the National Spring Scientific Conference "Science and Cultural Diplomacy – Drivers of International Cooperation", organized by the Military Sciences Section of the Academy of Romanian Scientists, held at the "Carol I" National Defence University in Bucharest, on May 23, 2025.*

[**] ***Mirela ATANASIU, PhD, is Senior Researcher within the Center for Defence and Security Strategic Studies/"Carol I" National Defence University, Associate member of the Academy of Romanian Scientists, Bucharest, Romania, and Associate Researcher at the Doctoral School of Safety and Security Sciences, Obuda University, Budapest, Hungary. Email: atanasiu.mirela@yahoo.com***

Introduction

War was until the beginning of civilization a decisive factor in the configuration of international relations and global balance of power. Along the time, the armed conflicts shaped frontiers, generated alliances and give birth to theoretical paradigms to explain the international actors' behaviour.

In the 21st century, although the international order seemed to be increasingly guided by solid juridical norms, international cooperation and economic interdependency, the reality check regarding conflicts have proven the resilience of power logic and the use of force in global politics.

The military aggression of Russia, triggered in 2008 in Georgia, continued in 2014 in Crimea and amplified in 2022 by the involvement in full-scale war against Ukraine, marked a inflection point in the international relations among actors and in the manner liberal norms are perceived by them.

The reason for this paradigmatic shift stands not only in the major geopolitical crisis generated in Europe but as well in the direct undermining of basic principles of international law as the respect for states sovereignty, territorial integrity and non-aggression.

This article shows how the international security and the rules-based system are transformed under the pressure of Russian aggression and Russian-Ukrainian ongoing war and by the delivered analysis the study will emphasize the tension among international legal order and power dynamics in times when the law and force coexist in an increasingly fragile balance.

1. The Escalation of Russian Military Actions in Europe and Their Legal Qualification

The progressive intensification of the Russian military aggression in Europe in the late 10 years illustrates a gradual strategy to expand its sphere of influence and to undermine the current international order.

This trajectory of military assertiveness began with the 2008 intervention in Georgia, during which Russian forces deployed tanks into South Ossetia and expelled Georgian troops from Tskhinvali claiming the protection of Russian citizens as justification. Moreover, in February 2014, under the same pretext of safeguarding the Russian-speaking minority, Russia occupied and annexed the Crimean Peninsula. Simultaneously, it launched a hybrid war in the eastern Ukrainian regions of Donetsk and Luhansk by supporting and arming separatist militias.

On February 24, 2022, Russia launched a full-scale military invasion of Ukraine, marking the most serious act of military aggression in Europe since the World War II. Despite the absence of a formal declaration of war by either side, the conflict qualifies, under international law, as an international armed conflict (GC-I 1949, Article 2). This classification obliges both parties to comply with the provisions of international humanitarian law.

The legal foundation for qualifying the Russian Federation's military actions as acts of aggression is grounded in public international law, particularly the following legal instruments:

a) The Charter of the United Nations (1945), which mandates that "All members shall refrain in their international relations from the threat of use of force against the territorial integrity or political independence of any state" (ONU 1945, art. 2(4)) Additionally, Article 51 affirms the right to individual or collective self-defence in the event of an armed attack. Therefore, the use of armed forces by UN Member State against another state, regardless of whether the latter is a UN member, constitutes a direct violation of Article 2(4), and Ukraine is entitled to exercise its right of self-defence under Article 51.

b) UN General Assembly Resolution 3314 (1974) defines aggression as "the use of armed forces by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations" (UNGA 1974, art. 1). Moreover, the resolution affirms that "the first use of armed force by a State in contravention of the Charter shall constitute prima facie[1] evidence of an act of aggression" (UNGA 1974, art. 2). The resolution further enumerates specific acts that may be classified as aggression, many of which have been committed by the Russian Federation in Ukraine, including: the invasion or attack by armed forces of one state on the territory of another; the bombardment of another state's territory; the blockade of ports or coastlines; the provision of support to armed groups operating against another state; and the dispatch, by or on behalf of a state, of armed bands, irregular forces, or mercenaries engaging in armed force and substantially participating in armed conflict (UNGA 1974, art. 3(a),(b),(c),(g)). Accordingly, under public international law, not only the armed aggression that resulted in the direct Russo-Ukrainian war qualifies as an act of aggression, but so do earlier actions by the Russian Federation – namely, the invasion of Crimea, the support provided to separatist forces in Donbas, and the deployment of foreign mercenaries against Ukraine armed forces. Each of these actions falls within the definition of aggression as set out in the resolution.

In addition to these considerations, the *Rome Statute of the International Criminal Court* also provides a legal framework for the classification of aggression. It defines the crime of aggression as "the planning, preparation, initiation or execution of an act of aggression" (CPI 1998, art. 8 bis (1))[2].

[1] "Prima facie" is a legal term used to describe a case that presents sufficient evidence to warrant proceeding to trial or judgement.

[2] Neither Russia nor Ukraine is a party to the Rome Statute; however, in 2023, the International Criminal Court issued an arrest warrant for Vladimir Putin for the unlawful deportation of Ukrainian children - an act classified as a war crime.

In response to the classification of the Russia's military actions as military aggression against Ukraine, several international efforts have been initiated to ensure its accountability.

The United Nations General Assembly has adopted several resolutions condemning the Russian invasion – for instance, Resolution ES-11/1 of March 2022, which called for the immediate and unconditional withdrawal of Russian troops from Ukraine (United Nations Digital Library 2022), and although such resolutions are not legally binding, they are nonetheless reflect the will of the international community.

In March 2023, the International Criminal Court issued an arrest warrant for Russian President Vladimir Putin, accusing him of the unlawful deportation of Ukrainian children from occupied territories to the Russian Federation (International Criminal Court 2023a). At the same time, the Court also opened a broader investigation into President Putin for alleged war crimes against humanity, and potential acts of genocide committed during the conflict in Ukraine. Additionally, the International Court of Justice took up proceedings following Ukraine's application in February 2022, in which it accused Russia of misusing the Genocide Convention as a justification for its invasion. In response, the Court issued a provisional order requiring Russia to immediately suspend its military operations in Ukraine. Moreover, as early as 2022, under the coordination of EUROJUST, a Joint Investigation Team was established, comprising Ukraine and several European countries with the purpose to collect evidence and document international crimes committed in the context of the ongoing war (European Union Agency for Criminal Justice Cooperation 2024) and in 2023, the International Centre for the Prosecution of the Crime of Aggression against Ukraine was inaugurated (European Union Agency for Criminal Justice Cooperation 2023). Also, such initiatives aimed to reclaim Russia's accountability for its aggression and abuses are also reflected in the agreement to establish a Special Tribunal for the Crime of Aggression against Ukraine, in Strasbourg, signed by the President of Ukraine, and the Secretary General of the Council of Europe in June 2025.

2. The Impact of Russian Military Aggression in Ukraine on the International Security System

The war initiated by the Russian Federation against Ukraine in February 2022, added to its prior acts of military aggression, marked the end of a period of relative stability in post-Cold War Europe and has left a significant less wanted imprint on the international security system.

However, it is obvious that many of the effects currently observed cannot be attributed solely to the actions undertaken by the Russian Federation since 2022, or even to the 2008 incursion into Georgia – the first military aggression against another sovereign state in post-Soviet era. Rather, these outcomes are largely the result of a broader set of complex, dynamic and often unpredictable developments that have shaped the international environment over the least past two decades. Some of these developments refer to the rapid advancement of emerging technologies whose applications may prove disruptive to global security, or the widespread globalization, which fosters both integration and polarization, or the intensification of geopolitical competition among major powers. Also, the strengthening of multipolar tendencies in the global order, the growing diversification of actors on the international stage and the worsening of transnational crises, increasing economic instability, the hybridisation of conflict, and the exacerbation of social tensions and crises are among these outcomes.

In the following section, based on informed analysis and personal perspective, we will distinguish the effects of the Russian aggression against Ukraine on the international security system, as identified in international law and/or the specialised literature, into the two aforementioned categories: *direct effects* and *catalysed effects*.

The main *direct effects* on the international security system include:

a) Redefining threats against regional and international security, in the following respects:

- Russian-Ukrainian war has brought conventional military threats back to the borders of European states;

- Risk of nuclear escalation has increased, particularly in light of Russia's repeated threats to employ nuclear weapons;

- International sanctions against Russia and the associated economic war became more assertive;

- Hybrid warfare, especially through disinformation campaigns, cyberattacks, and the instrumentalization of migration, has gained heightened strategic significance.

b) The strengthening of the North Atlantic Alliance, driven by the heightened perception of regional threats posed by the Russian Federation's conventional military actions, as reflected in:

- The membership of Finland (2023) and Sweden (2024), both of which had previously maintained a status of military neutrality;

- The increased military presence of the Euro-Atlantic alliance in Eastern Europe;

- The exponential growth of military investments in military equipment;

c) The EU's mobilisation to provide financial and political support to Ukraine, along with the initiation of strategic autonomy plans aimed at bolstering the defence of its Member States, represents another significant direct consequence.

The prior *effects* of Russian aggression but that have been *catalysed* by the actual international context may be identified as follows:

a) *The substantial increase in global military spending*, which reached $2.718 trillion in 2024, marking a 37% rise between 2015 and 2024. The countries with the most significant increases in military expenditures in 2024 were the United States, China, Russia, Germany, and India, collectively accounting for approximately 60% of global spending. At the same time, total military expenditures in Europe rose by 17%, reaching $693 billion[3] (SIPRI 2025, 1);

b) *The acceleration of global order fragmentation*, whereby the Russian-Ukrainian conflict has further deteriorated East-West relations and intensified the global polarisation between the Global North and the Global South, thereby complicating the architecture of international security;

c) *The weakening of the United Nations*, resulting from its inability to adopt firm positions in condemning the military aggression against Ukraine, most resolutions addressing this issue have been obstructed by Russia's[4] exercise of its veto power. For example, in September 2022, Russia blocked a UN Security Council resolution condemning the illegal annexation of the Ukrainian regions of Luhansk, Donetsk, Kherson, and Zaporizhzhia. But not only Russia was in this case, as in February 2025, the United States voted against a UN General Assembly resolution that condemned Russian aggression and called for the withdrawal of Russian troops from Ukraine. Likewise, China has maintained ambiguous positions, often abstaining from votes explicitly condemning the Russian Federation, while supporting resolutions that promote peaceful solutions without attributing blame to either party.

3. The Effects of the Russian-Ukrainian War on the International Legal Order

The Russian-Ukrainian war, which began in 2022, has had a tremendous impact on the norms and practices of international law, prompting discussions and potential changes across several areas. The following are some of the key aspects that have been affected or have sparked debate:

a) *International legitimacy of territorial annexations* in light of the Russian annexation of Ukrainian territories. Although the international community has overwhelmingly rejected these actions, it has emphasized the importance of respecting the right to self-determination, according to which any territorial changes

[3] Malta is the only country that did not increase its military spending.

[4] In September 2022, Russia vetoed a UN Security Council resolution condemning the illegal annexation of the Ukrainian regions of Luhansk, Donetsk, Kherson, and Zaporizhzhia. In February 2025, for example, the United States voted against a UN General Assembly resolution that condemned Russian aggression and called for the withdrawal of Russian troops from Ukraine. Likewise, China has maintained ambiguous positions, often abstaining from votes explicitly condemning the Russian Federation, while supporting resolutions that promote peaceful solutions without attributing blame to either party.

must consider the will of the population within the territory and must refrain from the use of force against territorial integrity. Thus, UN Resolution 68/267 of March 2014, which declared the Crimean referendum illegal and reaffirmed Ukraine's international borders, clearly states that the annexation of Crimea is unlawful. Similarly, during 2022-2023, the UN adopted resolutions condemning Russia's annexation of four other Ukrainian regions – Donetsk, Luhansk, Kherson, and Zaporizhzhia. Furthermore, these UN resolutions are consistent with the 1978 Vienna Convention on Succession of States, which does not recognize territorial transfers executed by force or under the threat of force.

b) Legitimacy of the use of armed force and the right to self-defence of states. Ukraine invoked the right to self-defence as stipulated in Article 51 of the UN Charter, and the international community supported this right by providing military assistance. This underscored the importance of backing states facing military aggression. Moreover, the Russian-Ukrainian war reignited debates concerning the legitimacy of humanitarian intervention and military support in the context of aggression, as well as the limits of such actions.

c) Triggering collective responses by the international community to penalize the Russian military aggression has materialized primarily through economic sanctions[5], especially pronounced from the European Union and the United States. Russia was also excluded or suspended from various international organizations[6]. Nevertheless, these collective responses have raised questions regarding the effectiveness and legality of unilateral or collective sanctions under international law.

d) Re-evaluation of international legal mechanisms for the protection of civilians and the implementation of human rights during conflict, as well as states' responsibilities regarding migration, has occurred due to the refugee crisis generated in Europe and the abuses committed during the conflict. This has highlighted the need for stricter adherence to and enforcement of international humanitarian law norms, including those concerning the protection of refugees, civilians, and civilian infrastructure.

[5] The economic sanctions imposed on the Russian federation include financial measures (disconnection from the SWIFT international payment system, freezing of foreign assets, transaction restrictions); trade sanctions (embargoes and export bans, import bans); individual sanctions targeting oligarchs, government officials, and associates of Russian leaders, involving asset freezes and travel bans; technological and industrial restrictions, including export controls on components and equipment, as well as prohibitions on cooperation in sectors such as aerospace and nuclear energy. Additionally, thousands of Western companies have withdrawn from Russia (for example, McDonald's, BP, Shell, Ikea, and Apple).

[6] Russia was excluded from political-economic bodies (Council of Europe, UN Human Rights Council, Organization for Economic Cooperation and Development, G8, World Tourism Organization, European Bank for Reconstruction and Development) and sports organizations such as FIFA, UEFA, and the International Paralympic Committee (International Paralympic Committee 2024).

e) *Use of drones and other advanced technologies in military actions between the Russian and Ukrainian Armed Forces* has underscored the necessity of regulating such technologies in accordance with the principles of international humanitarian law.

f) Necessity for organizational reform of the UN, particularly the Security Council, has become apparent due the limitations exposed by Russia's exercise of its veto power concerning issues related to the conflict in Ukraine. Such reform is seen as necessary to ensure more effective enforcement of international law.

By engaging in military actions against Ukraine, as well as previously against Georgia, Russia *has violated several key principles of international law*, examples of which include:

a) The principle of the inviolability of borders and non-interference in the internal affairs of other states, as established in the Helsinki Final Act (OSCE 1975, sections IIII, VI);

b) *The principles of sovereignty, territorial integrity, and the non-use of force,* reaffirmed in the Paris Charter for a New Europe (C.S.C.E. 1990). Russia's invasion of Ukraine constitutes a direct breach of the principles of sovereignty and territorial integrity, which are fundamental pillars of international law also established by the UN Charter. This has reopened discussions on the importance of respecting these principles and has prompted a re-evaluation of the mechanisms for enforcing international law in cases of similar aggression;

c) *The principles of international humanitarian law*:

- *Humanity*[7] (UN-HC 1899, Preamble) which governs the treatment of civilians, particularly vulnerable groups (including children, women, the elderly, and the sick), prisoners of war, medical personnel, religious workers, and humanitarian aid staff is further codified in Common Article 3 of the 1949 Geneva Conventions and reiterated in the Preamble of Additional Protocol I;

- *Proportionality*, a principle which holds that "… an attack is prohibited if it may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" (ONU-GC-PA-I 1977, art. 51(5)(b));

- *Distinction* between combatants and civilians, and between military and civilian objects, as regulated by Additional Protocol I to the Geneva Conventions of 1977, which mandates that "To ensure respect and protection for the civilian population and civilian objects, parties to the conflict must at all times distinguish between the civilian population and combatants…." (ONU-GC-PA-I 1977, art. 48, 51, 52);

[7] The Preamble of the 1899 Hague Convention II reflects the Martens Clause, a cornerstone of the laws of armed conflict.

- *Military necessity,* although not explicitly defined as a principle in international law, can be inferred from Article 52 of Additional Protocol I to the Geneva Conventions, which limits "military objectives to those objects that by their nature, location, purpose, or use effectively contribute to military action" (ONU-GC-PA-I 1977, art. 52(2)). This principle is also recognized in the San Remo Manual on International Law Applicable to Armed Conflicts at Sea published on June 12, 1994.

Russia's breaches of these principles, manifested in various ways, constitute war crimes. Indeed, the Russian-Ukrainian conflict has been marked by numerous allegations of war crimes, including indiscriminate attacks against civilians, use of prohibited weapons, and the destruction of civilian infrastructure. Such violations have been examined in prior studies (Atanasiu 2022), (Atanasiu 2022) (Atanasiu 2023) and have intensified efforts to legally document and investigate these acts, including by the International Criminal Court.

4. Future Legal Challenges in the Context of the Transformation of the International Security System and the Reform of its Legal Framework

Russia's use of its veto power, along with the ambiguous positions adopted by China and, more recently, the United States, has obstructed the adoption of decisive resolutions by the United Nations Security Council regarding the war in Ukraine. These developments reflect not only the prevailing geopolitical tensions but also the persistent difficulties in reaching international consensus on condemning the Russian military aggression and affirming Ukraine's sovereignty and territorial integrity. However, such ambiguous stances may also be interpreted as calculated diplomatic strategies through which the United States may seek to broker peace from a mediator's standpoint[8], while China may be signaling its preference for economic pre-eminence over political dominance within the global order.

In November 2007, President Vladimir Putin withdrew Russia from the Treaty on Conventional Armed Forces in Europe (CFE), signed in 1990, which imposed limits on the deployment of heavy military equipment across Europe (NATO Association of Canada 2025). Although currently inactive, the treaty's framework, including its definitions, provisions, procedures, and categories for arms limitation, could serve as a model for designing a comprehensive ceasefire agreement in Ukraine. This could include robust mechanisms for post-conflict monitoring and verification (Simonet 2025).

With regard to the international prosecution of Russian leadership for alleged crimes of aggression or war crimes, the situation is complicated by Russia's failure to ratify the Rome Statute and its non-recognition of the jurisdiction of the International

[8] "Path to Peace" resolution put forward by the U.S. and adopted by the Security Council in February 2025.

Criminal Court. In response, a coalition of 44 states, primarily European nations such as the Netherlands, Poland, the Baltic states, France, Germany, and Ukraine, that have not aligned with the Russian military actions have taken the initiative to establish a Special Tribunal for the Crime of Aggression as an ad hoc body intended to hold Russian leaders accountable for acts of aggression (Council of Europe 2025).

The initiation of military aggression by the Russian Federation in February 2022, and its continuation in the form of an intensified conventional armed conflict on Ukrainian territory, combined with aggressive non-conventional actions not only against Ukraine, triggered a corresponding response by Ukraine in 2024-2025, in the form of a "large-scale ground counteroffensive into Russian territory along its northern border" (Biggerstaff 2024). This counteroffensive has raised an unprecedented issues regarding Ukraine's compliance with international law, namely, whether Ukraine, as the indisputable victim of an ongoing armed attack by Russia, may lawfully launch an incursion into the aggressor's territory in self-defence, without violating the principle of proportionality.

Further juridical problems can also be triggered if certain NATO countries do not comply with the fact that Ukraine is not a Member State, hence article 5 of Washington Treaty is not applicable. Therefore, in order to respect the international law the military support must be voluntary-based for NATO's Member States and limited to material and know-how support in terms of money, munition, training and information, but not active participation with troops in combat actions. Also, the supporters must assure themselves that the equipment and munition is not used to commit war crimes.

Of course, the most acute challenge is the legality of the chosen path to peace and inhere we speak about means to conjure Russia to end the war without the prejudice of international law principles and norms and the Ukraine rights inherited in its status of recognized country by the international community.

Conclusions

The Russian aggression against Ukraine particularly as manifested in the Russian-Ukrainian war, triggered and intensified a series of developments within the global security environment, amid a backdrop of dynamic, complex, and uncertain transformations. Among the most notable consequence are the global increase in military expenditures, the acceleration of the fragmentation of the international order though increased polarisation, and a profound reassessment of the international security architecture established under the auspices of the United Nations.

In the context of the Russian-Ukrainian war, the international security system has come under heightened pressure not only from revisionist states but also from status quo-oriented states dissatisfied with the weakening of the UN Security Council, whose mechanisms of cooperation and conflict prevention have proven only partially effective in the face of Russia's decisive use of its veto power. Thus, Russia's aggression represents a critical inflection point that calls into question multiple aspects of the current international security system and underscores the urgent need for a more coherent and effective implementation of existing international norms. Likewise, it has sparked broader debates concerning the necessity of structural and procedural reforms in global security institutions to better address such crises in the future.

The initiation and conduct of this war have profoundly influenced established norms, practices, and jurisprudence within the international legal system, particularly with respect to the protection of human rights, the application of international humanitarian law, and the emerging need to develop new legal frameworks that address the hybrid nature of contemporary conflicts. Among areas generating significant legal debate and highlighting the need for regulatory adaptation are: breaches of sovereignty and territorial integrity, war crimes and the issue of international criminal accountability, the use of force and the right to self-defence, the imposition of economic sanctions and collective responses in support of parties to the conflict, the protection of civilians and the safeguarding of human rights, the regulation of emerging weapons systems and technologies, and the evolving role of international organisations in managing modern armed conflicts.

In the future, beyond the ongoing peace negotiations facilitated by the United States, a key challenge remains the pursuit of legal accountability for Russia's crime of aggression against Ukraine, as well as for acts already classified as war crimes, such as the forced deportation of Ukrainian children. Equally important is the development of investigative tools for addressing future allegations of similar violations of public international law, whether committed by the Russian Federation or by Ukraine.

BIBLIOGRAPHY:

Atanasiu, Mirela. 2022. "Coordonate juridice ale războiului din Ucraina." *Colocviu Strategic*, Martie, ed. 1: 5-7. doi:10.53477/1842-8096-22-1.

—. 2022. "Efectele conflictului armat asupra copiilor şi femeilor din Ucraina." *Colocviu Strategic*, Octombrie, ed. 10: 1-6. doi:10.53477/1842-8096-22-10.

—. 2023. "International Law Dimension." *Colocviu Strategic*, 3-4.

—. 2022. "Războiul ruso-ucrainean între abuzuri mediatizate la adresa dreptului internațional, sancțiuni și negocieri de pace." *Colocviu Strategic*, ed. 7: 5-7. doi:10.53477/1842-8096-22-7.

—. 2022. “Războiul ruso-ucrainean. Consecințe în planul dreptului internațional.” *Colocviu Strategic*, ed. 9: 5-9. doi:DOI: 10.53477/1842-8096-22-9.

—. 2022. “Reglementări și încălcări ale dreptului internațional în intervenția militară din Ucraina.” *Colocviu Strategic*, ed. 3: 7-10. doi:10.53477/1842-8096-22-3.

Biggerstaff, William Casey. 2024. “UKRAINE SYMPOSIUM – UKRAINE’S “INDEFINITE” INCURSION INTO RUSSIA AND THE JUS AD BELLUM.” *Liweber Institute. West Point.* 22 October. Accesed at 25 05, 2025. https://lieber.westpoint.edu/ukraines-indefinite-incursion-russia-jus-ad-bellum/

Blinken, J. Antony. 2023. “Crimes Against Humanity in Ukraine.” *U.S Department of State.* 18 February. Accesed at 02 05, 2024. https://www.state.gov/crimes-against-humanity-in-ukraine/

C.S.C.E. 1990. “Carta de la Paris pentru o nouă Europă.” 21 noiembrie. Accesat 05 06, 2025. https://legislatie.just.ro/Public/DetaliiDocument/35915.

CPI. 1998. “Statutul de la Roma al Curţii Penale Internaţionale .” *lege5.ro.* 17 07. Accesed at 01 12, 2024. https://lege5.ro/Gratuit/ge3tqmbu/crime-de-razboi-statut?dp=giytsojvgizdm

EuroNews. 2025. “EU hails ‘major’ progress on plan to set up special tribunal to judge Vladimir Putin.” 04 02. Accesed at 05 06, 2025. https://www.euronews.com/my-europe/2025/02/04/eu-hails-major-progress-on-plan-to-set-up-special-tribunal-to-judge-vladimir-putin

European Union Agency for Criminal Justice Cooperation. 2024. „Joint investigation team into alleged crimes committed in Ukraine.” Accesed at 05 06, 2025. https://www.eurojust.europa.eu/joint-investigation-team-alleged-crimes-committed-ukraine

GC-I. 1949. “Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva.” *International Humanitarian Law Databases* . 12 August. Accesed at 03 04, 2024. https://casebook.icrc.org/a_to_z/glossary/international-armed-conflict

ICRC. 2024. “States Party to the Following International Humanitarian Law and Other Related Treaties as of 19-January-2024.” *IHL databases.* Accesed at 03 05, 2024. https://ihl-databases.icrc.org/public/refdocs/IHL_and_other_related_Treaties.pdf

International Court of Justice. 2024. “ALLEGATIONS OF GENOCIDE UNDER THE CONVENTION ON THE PREVENTION AND PUNISHMENT OF THE CRIME OF GENOCIDE (UKRAINE v. RUSSIAN FEDERATION.” 2 February. Accesed at 03 05, 2024. https://www.icj-cij.org/sites/default/files/case-related/182/182-20240202-ord-01-00-en.pdf

International Criminal Court. 2023. “Situation in Ukraine: ICC judges issue arrest warrants against Vladimir Vladimirovich Putin and Maria Alekseyevna

Lvova-Belova." 17 March. Accesed at 01 10, 2024. https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and

—. 2023a. "Vladimir Vladimirovich Putin." Accesed at 05 06, 2025. https://www.icc-cpi.int/defendant/vladimir-vladimirovich-putin

International Paralympic Committee. 2024. Accesed at 05 06, 2025. https://www.paralympic.org/news/ipc-general-assembly-partially-suspends-npc-russia.

Murray, Shona, și Mared Gwyn Jones. 2024. „Putin will be tried and prosecuted for war crimes, Ukraine's prosecutor general vows." *Euronews.* 05 03. Accesed at 03 06, 2024. https://www.euronews.com/my-europe/2024/03/05/putin-will-be-tried-and-prosecuted-for-war-crimes-ukraines-prosecutor-general-vows#:~:text=Ukraine%20is%20currently%20probing%20123%2C000,since%20the%20Second%20World%20War

NATO Association of Canada. 2025. "A Timeline Of Russian Aggression." Accesed at 05 05, 2025. https://natoassociation.ca/a-timeline-of-russian-aggression/

ONU. 1945. "Carta Națiunilor Unite." *Legislatie.Just.* 26 iunie. Accesed at 05 06, 2025. https://legislatie.just.ro/Public/DetaliiDocument/19362

ONU-GC-PA-I. 1977. "Protocolul adiţional I la Convenţiile de la Geneva din 12 august 1949 privind protecţia victimelor conflictelor armate internaţionale." *Crucea Roșie.* 10 06. Accesed at 05 06, 2025. https://crucearosie.ro/assets/Uploads/Protocolul-Aditional-I.pdf

OSCE. 1975. "Act internațional al Conferinței pentru Securitate și cooperare în Europa." *Legislație.Just.* 1 august. Accesed at 05 06, 2025. https://legislatie.just.ro/Public/DetaliiDocument/35947

Simonet, Loïc. 2025. "The CFE Treaty Is Dead. Could It Still Inspire a Ceasefire in Ukraine?" *Arms Control Association.* March. Accesed at 05 05, 2025. https://www.armscontrol.org/act/2025-03/features/cfe-treaty-dead-could-it-still-inspire-ceasefire-ukraine

SIPRI. 2025. "SIPRI Fact Sheet." April. Accesed at 05 05, 2025. https://www.sipri.org/sites/default/files/2025-04/2504_fs_milex_2024.pdf

Ucrainina World Congress. 2024. "44 countries endorse establishment of special tribunal on Russian crimes in Ukraine." 3 April. Accesed at 05 06, 2025. https://www.ukrainianworldcongress.org/44-countries-endorse-establishment-of-special-tribunal-on-russian-crimes-in-ukraine/

UNGA. 1974. "Definition of aggression. General Assembly Resolution 3314 (XXIX)." *Institute for International Law and Justice.* 14 December. Accesed at 05 06, 2025. https://iilj.org/wp-content/uploads/2016/08/General-Assembly-Resolution-3314.pdf

UN-HC. 1899. “Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague.” *International Humanitarian Law Databases.* 29 July. Accesed at 05 06, 2025. https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-ii-1899/preamble?activeTab=

United Nations Digital Library. 2022. “Aggression against Ukraine: resolution / adopted by the General Assembly.” 18 March. Accesed at 05 06, 2025. https://digitallibrary.un.org/record/3965290?ln=en&v=pdf

DOI: 10.53477/1842-9904-25-24

CYBERSECURITY SYNERGIES IN LOGISTICS: ADDRESSING THREATS ACROSS CIVILIAN AND MILITARY DOMAINS

Daniela-Elena HRAB[*]

Current and anticipated developments in logistics focus on implementing a range of emerging technologies that promise substantial economic, social, and environmental advantages. However, these technological innovations also give rise to cyber vulnerabilities that pose significant risk of disruption within supply chains, in the context of a low level of awareness. This study addresses this research problem by investigating such vulnerabilities within the specific context of logistics as a domain shared between civilian and military sectors. The article's research niche lies in its examination of cybersecurity risks at the intersection of civil and military logistics, aiming to identify opportunities for cooperation to mitigate these threats. The study employs a literature review methodology to achieve its objectives. By analysing the cybersecurity implications for civilian logistics and supply chain management first, and then examining the most vulnerable functional and related areas of military logistics, the study adopts a complementary perspective that integrates logistics and cybersecurity. The findings highlight ten key areas of civil-military collaboration, underlining the necessity of a paradigm shift in the delivery of logistic support to military forces, especially in military procurement and operational planning processes.

Keywords: *logistics; military; cybersecurity; procurement; operational planning.*

[*] ***Lieutenant Colonel Daniela-Elena HRAB is an Advanced Military Instructor and PhD Candidate within the "Carol I" National Defence University in Bucharest, Romania. E-mail: edaniela.hrab@gmail.com***

Introduction

The logistics sector is progressively adopting digital solutions to enhance operational efficiency. In 2020, the World Economic Forum projected that digitization could contribute up to $1.5 trillion for the sector by 2025. Among the innovations driving this transformation are technologies such as warehouse robotics, electro-mobility, artificial intelligence/AI, Blockchain, predictive maintenance, and drone supervision. While these technologies offer considerable benefits, these also produce vast quantities of data, thereby increasing the sector's exposure to cybersecurity threats – a risk exacerbated by a persistent deficit in cybersecurity awareness (Prabhughate 2020, 3-4). Prior research indicates that the willingness of logistics managers to implement cyber resilience strategies is significantly influenced by their perception of cyber risks (Gaudenzi and Baldi 2024, 99-122), thereby underscoring the imperative for increased awareness and an integrated focus on both physical and cybersecurity dimensions (Chan and Choi 2023, 1-18).

Military logistics faces similar threats, with China investing in targeting US civilian and military logistics. Such actions pose a significant risk to the operational readiness and responsiveness of NATO forces However, the rapid pace of technological advancement also presents opportunities to develop effective countermeasures. (US Army Futures Command n.d., 8-12). Therefore, identifying cyber threats and fostering military-civil cooperation is critical to enhancing cybersecurity resilience across both sectors.

More than 20 emerging and disruptive technologies have been identified as influencing military cybersecurity, including AI, machine learning/ML, advanced materials, and quantum technologies (NATO Science & Technology Organization 2020, 41-111). Additional relevant technologies include data storage systems, 5G networks, and advanced sensor systems, etc. (Bellasio and Silfversten 2020, 88-108). By 2030, NATO member states are expected to implement private and hybrid 5G networks to support logistics operations in areas such as maintenance, transportation, and training (Pernik 2022, 67). Given this technological landscape, it is imperative for military logisticians to remain informed about developments in both logistics and cyber domains, as cyber threats have the potential to disrupt supply chains and undermine the sustainability of military operations. Within this context, the study addresses the following research problem: a low level of awareness regarding cyber threats and their potential to disrupt supply chain, thereby jeopardizing the continuity and effectiveness of military operations.

Logistics functions differ significantly between civilian and military contexts. In the civilian sector, logistics primarily encompasses transportation, warehousing, and distribution, while Supply Chain Management/SCM include activities such as procurement, production planning, and demand management (Mentzer, Stank and

Esper 2008, 32-35). In contrast, military logistics is considerably broader, comprising six functional areas: the supply of various categories of goods, materiel life-cycle support, equipment maintenance, movement and transportation, general support services (including catering, accommodation, warehousing, laundry and sanitation, postal and courier services, equipment recovery, etc.), as well as medical and veterinary support. Additionally, six related areas are being added, namely: budget and finance, military engineering, mortuary affairs, contractor support to operations, civil-military cooperation and military police functions (NATO Standardization Office 2018, 5_1-6_5). This broader scope highlights that military logistics not only incorporates but extends beyond the functions of civilian logistics and SCM. Accordingly, the objective of this study is to identify and pinpoint potential areas for civil-military collaboration aimed at mitigating cyber risks and improve the sustainability of military operations.

1. Literature Review

The existing body of research on cyberattacks within the logistics sector do not differentiate between civilian and military actors. For instance, Microsoft reported a ransomware attack, allegedly orchestrated by the Russian military operatives, targeting Ukrainian and Polish logistics organizations supporting frontline operations (Lyngaas 2022). Despite the significant impact, limited information was made public, resulting in significant awareness gaps. Consequently, cyber threats to logistics have not been prioritized as a key research area by military logistics experts in at least one of the affected countries over the next five-year period (Jałowiec and Grala 2022, 8-12).

Additionally, research combining cybersecurity and logistics is limited, possibly due to insufficient data highlighting its importance, as most studies address cybersecurity within the broader context of Supply Chain Management (SCM), often overlooking the distinct challenges faced by logistics operations (Cheung, Bell and Bhattacharjya 2021, 1-12). At the same time, logistics often falls under SCM, where continuity of supplies is a key focus (Dymyt, Wincewicz-Bosy and Skubisz 2024, 187), attracting more research interest.

Cybersecurity within logistics and SCM encompasses a broad spectrum of domains, including management, engineering, and operations (Cheung, Bell and Bhattacharjya 2021, 2), rarely considering military contributions. Therefore, military logistics studies often lack detailed analyses of cyber vulnerabilities, missing opportunities to address these through civil-military collaboration. Similarly, civilian-focused research overlooks the potential for military contributions. As a result, military managers lack insights into leveraging civilian expertise to enhance cybersecurity, and civilian sectors miss opportunities for military support. This study aims to bridge this gap by exploring joint civil-military initiatives to bolster logistics cybersecurity in both domains.

2. Research methodology

To achieve the stated objective, the research employs a qualitative strategy grounded in a literature review approach, using the military logistics functional and related areas framework to identify key stakeholders and potential cooperation opportunities. This qualitative method is particularly appropriate as it covers an interdisciplinary topic, enabling preliminary exploration within the intersecting fields of cybersecurity and logistics. Through its characteristics, this strategy allows the applicability of "understanding as a discovery principle" and "the construction of reality as a basis" (Kuckartz and Rädiker 2023, 5).

Moreover, the qualitative strategy aligns well with the exploratory focus of the research goal, which does not aim to test hypotheses (Creswell J.W. and Creswell J.D. 2018, 40, 192). The study adopts an interpretive stance (Denzin and Lincoln 1994, 2), exploring cybersecurity in civilian logistics and SCM, and using a deductive approach to pinpoint areas where military expertise can enhance civilian operations. Furthermore, it analyses military logistics through a comparative approach, highlighting best practices and potential contributions to civilian efforts. As a result, the research offers a holistic view on the issue by analysing various components of military logistics (Creswell J. W. 1998, 15).

3. Cybersecurity Implications for Civilian Logistics and Supply Chain Management

Addressing cybersecurity threats in civilian logistics and SCM is increasingly critical, particularly in the context of Industry 4.0 developments. Emerging technologies such as Blockchain play a key role in safeguarding data generated in logistics by other technologies (Boyson 2014, 2) while also fostering innovation (Tang and Veelenturf 2019, 1-11). Cyber-physical systems/CPS, data science applications (Muhuri, Shukla and Abraham 2019), drones and robots further optimize logistics operations (Cheung, Bell and Bhattacharjya 2021, 13). Despite these benefits, such technologies also increase vulnerability to a range of risks: physical disruptions (e.g., accidents or natural disasters) and cyberattacks, leading to both tangible consequences (reduced production, labour disruptions) and intangible damages, including loss of consumer trust or reputational harm (Chen and Chang 2021, 2-13).

Implementing precautionary measures is essential, beginning with the identification of system vulnerabilities and involving the Chief Information Officer (CIO) to mitigate risks in both information technology/IT and supply chain operations (Cheung, Bell and Bhattacharjya 2021, 5-7). High-profile cyberattacks, such as the attacks on Colonial Pipeline and SolarWinds – underscore the CIO's dual role in ensuring cybersecurity across a broad spectrum of logistics activities, ranging from the supply of everyday products to the acquisition of advanced assets like fighter aircrafts (Dury and O'Meara 2021). Effective measures include implementing blockchain technology, multi-factor authentication (Zhang et al. 2020, 1187-91), installation of secure firewalls and gateways (Hutchins et al. 2015), conducting supplier audits, training personnel (Cheung, Bell and Bhattacharjya 2021, 7-8), and implementing safeguards against counterfeit products (Eggers 2020, 880-5).

Experts highlight that civil-military teams can coordinate three key real-time recovery measures: component recovery, system isolation, and continuous monitoring (Cheung, Bell and Bhattacharjya 2021, 8). In the event of a cyberattack, recovery efforts may also require engaging managers responsible for logistics, procurement, and customer service (Chopra 2018, 1-528).

Aftermath measures often involve CIO-led teams and include behavioural analysis and feedback loops (Sepulveda and Khan 2017, 1293-5), data backups, recovery planning, resilient system design (Colicchia, Creazza and Menachof 2019, 215-40), forensic investigations (Tuptuk and Hailes 2018, 93-106), and system restoration activities (Heath, Mitchell and Sharkey 2020, 5-19). Collaborative recovery strategies often require coordination with supply chain partners (Colicchia, Creazza and Menachof 2019, 221) and insurance providers (Boyson 2014, 9). Additionally, if military supply chains are affected or contractual agreements are in place, military experts may be called upon to support recovery efforts.

Integration sustainability specific to sustainable development in logistics requires strong cybersecurity measures to prevent supply chain disruptions. While technologies such as Blockchain, AI, the Internet of Things (IoT), and Big Data Analytics support this integration, they also heighten vulnerability to cyber threats. Mitigation strategies include the use of Machine Learning (ML) and Cyber Threat Intelligence, while effective implementation requires coordinated efforts among decision-makers, governmental bodies, industry stakeholders, academic institutions, and specialized military personnel in logistics, cybersecurity, and intelligence (Layode et al. 2024, 1954-73).

Maritime logistics, in particular, also presents significant risks, with ports targeted for espionage, terrorism, and cyber warfare, threatening both civilian and military operations. Recommended countermeasures include training, IT infrastructure upgrades, and cooperation with government and international entities (Senarak 2021, 20-36).

Emerging technologies such as Cyber-Physical System (CPS) and Complex Event Processing are increasingly bridging logistics and cybersecurity by enabling real-time data analysis and threat detection (Alias et al. 2018, 1-4). Military logistics could benefit from adopting these innovationss through enhanced cooperation with private companies and the development of smart logistics solutions, addressing risks across personnel, operational processes, and technologies. Recommended measures include network segmentation, rigorous device testing, and AI-based threat monitoring, paired with encryption and employee cybersecurity training programs (Prabhughate 2020, 4-6).

This analysis highlights opportunities for military engagement in addressing logistics cybersecurity, setting the stage for tailored strategies to military operational frameworks.

4. Cybersecurity Implications for Military Logistics

Military logistics is a cornerstone of the broader logistics sector, defined by key domains outlined in NATO standards. These include functional areas such as supply, materiel life cycle support, equipment maintenance, transportation, and medical support, alongside logistics related areas such as finance, engineering, contractor support to operations, and civil-military cooperation (NATO Standardization Office 2018, 5_1-A_1). Additionally, some researchers further emphasize the importance of operational processes, stocks, and technical components, particularly within supply, transport, and services (Brzeziński 2024, 144).

Given the susceptibility of military logistics to cyberattacks, this section explores threats across these domains and explore collaborative countermeasures involving both military and civilian actors. This approach is vital as supply chains underpinning military and civilian logistics share a common structure based on four lines of logistical support. The fourth tier -which includes national depots, contractors, and industrial partners - serves as the strategic foundation for the others (NATO Standardization Office 2018, 1_8). Therefore, cyber threats aiming at civilian logistics can have cascading effects on military supply chains, which may themselves become direct targets.

Research highlights specific vulnerabilities within military supply chains, especially concerning weapon systems, which function as intricate systems-of-systems. These systems are prone to cyberattacks, partly due to flaws in their integrated circuits (Koch and Golling 2016, 192). Additionally, the outsourcing of production to Asia for cost-efficiency has introduced additional risks, such as unauthorized access via backdoors and kill switches in externally manufactured chips, compromising highly classified systems (Adee 2008, 34-9).

Furthermore, cyber risks in military logistics remain persistent due to issues like counterfeit components in naval assets (United States Government Accountability Office 2016, 11-12) and challenges maintaining supply sources for aging weapon platforms. Additionally, the use of commercial off-the-shelf products introduces cyber vulnerabilities, while the integration of legacy systems with modern technologies can create weak points capable of compromising entire military operations (Koch and Golling 2016, 193-5).

Researchers stress that effective cybersecurity begins with the assumption that systems may already be compromised. This requires identifying critical components and implementing risk management practices guided by international standards such as ISO 31000 and IEC 31010 (Koch and Golling 2016, 198). To reduce risks, military logisticians must adopt advanced technologies within their supply chains, develop reliable methods to detect counterfeit parts, and create migration strategies for bridging incompatible systems, with input from civilian and military cybersecurity experts. In parallel, strengthening chip production and supporting EU industrial alliances in semiconductor technologies development are also key priorities (European Commission 2021, 14).

Cyberattacks on civilian supply chains, such as those impacting Colonial Pipeline and JBS Foods, highlight vulnerabilities that could also jeopardize military operations, especially when contractors are involved. Medical support systems face similar threats; for instance, cyberattacks on civilian hospitals as seen in Ireland can hinder healthcare services for both civilian and military patients due to the interconnected nature of their medical infrastructures (NATO 2019, 1_19-1_22). To address these risks, military logisticians should diversify contractors for critical supplies, ensure timely software updates, and foster collaboration between military and civilian sectors. Coordinated efforts are essential to strengthen logistical resilience against cyber threats (NATO Cooperative Cyber Defence Centre of Excellence 2022, 2-4). Furthermore, cybersecurity responsibilities must be clearly assigned across the supply chain, especially for manufacturers, distributors, and importers of digitally integrated products, particularly in information and communication technology. These actors must proactively assess cyber risks, mitigate threats, and comply with conformity assessment procedures to reinforce overall supply chain security (European Commission 2022, 1-17).

In the domains of equipment maintenance and materiel life-cycle support, cybersecurity risks are closely linked to Additive Manufacturing technology. Already adopted by the U.S. military, it enables on-site production of parts, thereby reducing logistical strain and advancing sustainability objectives (Hrab and Minculete 2023, 130). Addressing these risks requires coordinated efforts among 3D printer manufacturers, software developers, equipment suppliers, procurement teams, and military maintenance units.

Similarly, the movement and transportation of military assets are also vulnerable to cyber threats. The U.S. Transportation Command depends heavily on commercial transportation providers and civilian infrastructure - including roads, ports, railways, and electrical grids - to deploy approximately 90% of its troops and equipment. However, these systems lack military protection, leaving critical deployment capabilities exposed to cyber risks (The Brookings Institution 2023, 3-7).

Enhanced military involvement is essential to safeguard critical networks from cyberattacks and economic coercion. For example, China's integrated digital platform for military and civilian entities, connecting 70 ports and more than ten airports, enables coordinated cyber operations. This raises significant concerns about national sovereignty, as controlling and monitoring port data, including entries and departures, may lead to the unintended transfer of operational authority in exchange for assured access (The Brookings Institution 2023, 8).

Furthermore, the military's growing interest in using drones to transport essential supplies, such as petroleum, highlights the need for strong cybersecurity. These autonomous systems require robust cybersecurity to prevent malicious interference. One potential threat scenario involves cyberattacks rerouting autonomous commercial vessels, causing maritime congestion that could obstruct naval operations (U.S. Army Futures Command n.d., 8-9). As adoption of autonomous systems in military mobility depends on IT Systems, smart railroads, and harbours, which heavily rely on GPS (Pernik 2022, 74), the cybersecurity dimension becomes essential.

The EU and NATO acknowledge the critical role of cybersecurity in ensuring effective military mobility. A project under the Permanent Structured Cooperation (PESCO) framework highlights mitigating cyber threats through collaboration between public and private sectors during deployment phases. Key logistical factors, include port accessibility, bridge load capacity, and tunnel dimensions for transporting heavy equipment, and are central to these efforts (Beckvard and Zotz 2021, 1).

Essential for logistic support, critical infrastructure also relies on technology systems, ensuring cybersecurity is imperative. Military logistics platforms, including LOGFAS and warehouse management tools, must also be secured. As a proactive measure, mapping the interdependencies between civilian and military systems is a crucial precautionary step (Beckvard and Zotz 2021, 2). Planners should focus on identifying critical infrastructure and information systems for each operation, and evaluating the risk of potential cyberattack disruptions in both departure and host nations. Additionally, building partnerships to enhance cybersecurity and using Information Sharing and Analysis Centres can foster cooperation and trust. Within the Mission Assurance Process, adopting cybersecurity standards such as ISO/IEC 27001 or the U.S. NIST Cybersecurity Framework is key to establishing a secure operational environment (Beckvard and Zotz 2021, 2-4).

Warehousing is another area vulnerable to cyber threats. Cyberattacks, such as denial-of-service/DoS or database manipulation can disrupt storage facilities by altering product data, especially when systems like Radio Frequency Identification or cellular data are used. Man-in-the-middle attacks pose additional risks by potentially exposing sensitive logistical data to unauthorized entities. Mitigation strategies include securing automated systems, maintaining regular backups, performing routine audits, and providing comprehensive staff training (Beckvard and Zotz 2021, 4).

In the domain of movement and transportation, several aspects need to be thoroughly addressed. First, heavy equipment transport often relies on sea routes using private contracted ships, which are susceptible to cyber disruptions via internet-connected systems. Such cyber threats can delay or obstruct essential deliveries. According to researchers, military planners should engage private companies early in the planning process and mandate adherence to the International Maritime Organization's guidelines on maritime cyber risk management (Beckvard and Zotz 2021, 4). They also stress the need for a robust international legal framework to more effectively address these threats (Al Ali, Chebotareva and Chebotarev 2021, 248).

Secondly, inland waterway transport is exposed to cybersecurity risks similar to those facing maritime transport, River Information Systems and IT infrastructure making these networks attractive targets for cyberattacks (Benga, et al. 2019, 248-50). Any disruption to traffic control could cause cascading effects, such as waterway congestion and broader supply chain interruptions (Beckvard and Zotz 2021, 6).

Thirdly, air transport also faces substantial cyber risks. Military aircraft, much like their civilian counterparts, depend on navigation and air traffic control management systems that ae vulnerable to cyberattacks, including potential breaches in Air Traffic Management systems. Mitigation strategies include establishing alternative flight routes, protection via Military Computer Emergency Response Teams, and coordinating closely with civilian aviation authorities (Beckvard and Zotz 2021, 5-7).

Fourthly, rail transportation is at risk due to its increasing reliance on digital systems like Advanced Train Control Systems, which are susceptible to eavesdropping, spoofing, and denial-of-service (DoS) attacks (Xiang et al. 2020, 46). Addressing these vulnerabilities requires thorough risk assessment during operational planning process/OPP (Beckvard and Zotz 2021, 8).

Seaport cybersecurity plays a vital role in military operations, as ports are integral components to the Joint Logistic Support Network/JLSN, alongside airports and rail ports (NATO Standardization Office 2018, 1_6). Vulnerabilities in systems such as Vessel Traffic Services and cargo handling processes require the deployment of rapid response teams of military personnel, port authorities, and contractor representatives, with joint training and awareness efforts such as infographics and pocket guides. Military mobility, reliant on aerial assets, requires civilian and military cooperation to adopt such measures and embed them within the Operational Planning Process (OPP) (Beckvard and Zotz 2021, 5).

Last but not least, road transportation is essential for military exercises and operations, yet it remains susceptible to threats like attacks on traffic light systems, which can cause congestion that disrupts deployments (Zhiyi et al. 2016, 60-68).

Cities, as part of the JLSN, host key facilities such as hospitals, depots, and convoy support centres (NATO Standardization Office 2018, 1_6). However, the advent of smart cities – where technology is embedded into infrastructure, such as traffic management, energy grids, and healthcare systems – introduces new cyber vulnerabilities. Such threats could disrupt military planning and logistics, highlighting the need for strong collaboration between military leaders and city administrations to implement "security by design" principles into public procurement processes (Bellasio and Silfversten 2020, 111-120).

In this complex landscape, national regulations often fall short in addressing cross-border cyber threats. Effective solutions include mapping vulnerabilities, updating policies and legal frameworks, implementing standards, and fostering agreements among stakeholders to ensure a secure cyber environment (Beckvard and Zotz 2021, 8-9).

Another key area of military logistics highly vulnerable to cyberattacks is contractor support for operations. When responsibilities are outsourced, cybersecurity risks shift to private entities; nonetheless, military logisticians must ensure these risks are effectively addressed. For example, in Japan, defence procurement entities require cyber risk assessments and supplier to comply with cybersecurity standards, including audits and secure supply chains (*Apud* Kono and De Tomas Colatin 2023, 15-16).

In the United Kingdom, Ministry of Defence contractors are required to adhere to the Cyber Security Model, including risk assessments, questionnaires, and evaluations applied to both contracts and subcontracts. However, many contractors face challenges with cloud service and software providers due to the lack of certification and audit standards, underscoring the need for government action and a stronger regulatory framework (UK Government 2021, 3).

The USA has taken a stricter approach, banning high-risk equipment and services from companies such as Huawei, Kaspersky, and ZTE in military contracts, along with restrictions on import and export activities (Federal Communications Commission 2024). Experts advocate for proactive international regulatory frameworks to strenghten supply chain cybersecurity before attacks can occur (Kono and De Tomas Colatin 2023).

5. Main Findings

The analysis highlights key logistics activities across military and civilian domains vulnerable to cyber threats, emphasizing the need for strong collaboration. It also outlines practical solutions achievable through joint efforts involving both logisticians and cybersecurity experts. As a result, ten collaboration areas between military and civilian stakeholders have been identified and are illustrated in Figure no. 1.

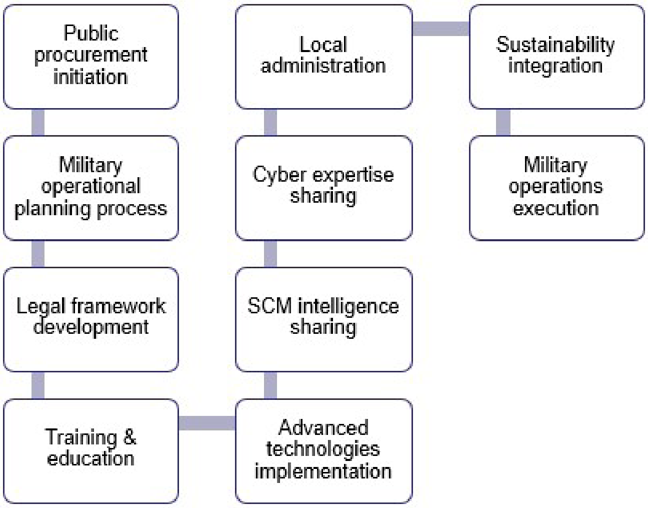
Public procurement initiation
Military operational planning process
Legal framework development
Training & education
Local administration
Cyber expertise sharing
SCM intelligence sharing
Advanced technologies implementation
Sustainability integration
Military operations execution

Figure no. 1: Areas of civilian-military cooperation for cybersecurity in logistics

Conclusions

The current landscape in both military and civilian logistics is increasingly complex and exposed to significant cyber vulnerabilities. Although these sectors are interconnected, the military sector demonstrates a higher level of dependency on secure and resilient logistics. However, logisticians alone cannot address the challenges posed by technology integration and cyber threats to logistic support. Therefore, in the military sector, the success of operations and missions hinges on the establishment of interdisciplinary teams. These teams should include civilian and military logisticians, IT and cyber experts, representatives from producers, contractors, intelligence agencies personnel, administrative authorities, academic researchers, and other key stakeholders to effectively address cyber vulnerabilities across the ten identified areas of collaboration.

Within these interdisciplinary teams, logisticians play a critical role by deconstructing logistics processes into detailed components, enabling the identification of key actors and potential cyber threats. Nonetheless, the input of other team members is essential to ensure, for instance, that procurement processes and operational planning effectively mitigate a wide range of threats that could compromise the supply chain. This approach applies to all functional and related areas of military logistics, whether addressing the need for daily consumables or essential military equipment on the battlefield. Overlooking these considerations, particularly in procurement and operational planning, could render a military force unable to mobilize or sustain operations effectively.

From a procurement standpoint, military structures must expand their focus beyond standard product specifications, delivery terms, and payment conditions. Additional considerations, such as demand forecasting, the creation of a vetted and certified pool of national suppliers subject to military audits and oversight, securing multiple sources for critical products and service, imposing restrictions on the import and export of certain types or components of essential military equipment, and assigning clear cyber responsibilities to contractors, are already proving a significant impact on military procurement practices. Their effectiveness depends on the establishment of a robust legal framework, which can be developed collaboratively and supported through agreements among all relevant stakeholders. Furthermore, a cultural shift within military institutions may be necessary, such as fostering openness and transparency, as these are essential for successful collaboration with third parties.

Incorporating cybersecurity considerations into the operational planning process requires a fundamental shift in perspective, as emphasized in this study. To facilitate this change, several key actions should be prioritized during peacetime and validated through military exercises. These include: integrating cybersecurity into the design, monitoring, protection, and management of public infrastructure; active involvement from private and public sectors; focus on identifying interdependencies across systems; and establishing rapid-response teams to address cyberattacks effectively.

In addition to involving external parties into logistics-related military activities, military actors can also enhance engagement with the civilian sector through initiatives such as: cooperating with local authorities, identifying critical information infrastructure, protecting critical logistic infrastructure, promoting cybersecurity awareness, and providing education and training for both civilian and military logisticians. Additionally, offering cyber expertise to key stakeholders. In fact, education and training in cybersecurity for logistic processes to key stakeholders remains a valuable option. Notably, joint education and training in cybersecurity for logistics represents a strategic priority that can be significantly advanced through military-civilian collaboration.

While the ten areas of civil-military cooperation identified in this study encompass various distinct yet interconnected activities, the effectiveness of cybersecurity in logistics can be achieved through a coordinated and integrated implementation of these actions. Since they are interlinked, failure in one area could have a cascading negative impact on others, underscoring the need for a strategic approach.

Drawing on the insights presented, this study also identifies practical ways to implement cybersecurity measures into logistic practices. One of the most achievable steps is to *raise awareness among logisticians*, encouraging them to look beyond the traditional characteristics of military products and conventional logistics processes. To this end, logisticians should have access to updated training programs that not only address logistics but also highlight the cyber risks associated with its proper functioning. Furthermore, they should be equipped to understand how emerging technologies support logistics operations while simultaneously introducing cyber threats that could compromise military missions and operations.

Another approach to implementing cybersecurity measures in logistics is to establish an organizational habit of consulting cybersecurity experts prior to the procurement of military equipment. These experts can better assess the cybersecurity implications and contribute to refining operational requirements so that technical specifications explicitly address cybersecurity vulnerabilities. It is increasingly clear that merely acquiring equipment is not sufficient to safeguard against supply chain disruptions caused by cyberattacks. While this approach could be formalized through military directives and regulations, its success depends on decision-makers recognizing the negative consequences of maintaining the current modus operandi.

As the defence industry continues to evolve, a third approach to integrate cybersecurity into logistics practices involves engaging interdisciplinary teams – bringing together civilians and military personnel, logisticians and cyber experts, as well as producers and end-users – during the early stages of product design. To support this collaborative effort, a dedicated legal framework should be developed to clearly outline the scope and limits of cooperation between military procurement authorities and industry partners, aligned with the nation’s economic capabilities and strategic priorities.

Lastly, military exercises designed to evaluate the resilience of both civilian and military logistics support lines against cyberattacks should be routinely conducted. These exercises can help assess the scale of the problem and identify practical entry points for mitigation, especially given the diversity of equipment and systems used by various armed forces. For nations engaged in military alliances and partnerships, interoperability presents an additional layer of complexity. Therefore, procurement decisions made by one country should be carefully considered by partner nations, and multinational, interdisciplinary teams should be involved to develop the most effective and coordinated responses.

In addition to identifying important areas of civil-military cooperation to address cybersecurity threats to logistic operations and exploring practical ways to implement cybersecurity measures into practice, this article highlights another critical aspect: the need for a comprehensive, in-depth approach when identifying such cooperation opportunities. As such, future studies should focus on identifying common ground in civil-military relations and further exploring potential avenues for joint actions to counter cyber threats.

Acknowledgement: *This study was carried out within the framework of the Strengthening Synergies in Defence and Civilian Cybersecurity - ECYBRIDGE project, funded by the European Union, under Grant Agreement No. 101158784 - DIGITAL-ECCC-2023-DEPLOY-CYBER-04-CIVIL-DEFENCE.*

BIBLIOGRAPHY:

Adee, Sally. 2008. *The hunt for the kill switch. Are chip makers building electronic trapdoors in key military hardware? The Pentagon is making its biggest effort yet to find out.* https://spectrum.ieee.org/the-hunt-for-the-kill-switch (accessed November 5, 2024).

Al Ali, Naser Abdel Raheem, Anna A. Chebotareva, and Vladimir E. Chebotarev. 2021. "Cyber security in marine transport: opportunities and legal challenges." *Scientific Journal of Maritime Research* 35: 248-255. https://hrcak.srce.hr/file/387886

Alias, Cyril, Frank Eduardo Alarcón Olalla, Hauke Iwersen, Julius Ollesch, and Bernd Noche. 2018. "Identifying Promising Application Areas for Cyber-Physical and Complex Event Processing in Logistics Practice." *Logistics* (MDPI) 2, no. 4: 1-24. https://www.mdpi.com/2305-6290/2/4/23

Beckvard, Henrik, and Philippe Zotz. 2021. *Cyber Considerations for Military Mobility.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 1-11. https://ccdcoe.org/uploads/2021/05/Releasable_Cyber-Considerations-for-Military-Mobility_Beckvard_Zotz.pdf

Bellasio, Jacopo, and Erik Silfversten. 2020. "The Impact of New and Emerging Technologies and the Cyber Threat Landscape and Their Implications for NATO'." In *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, by Amy Ertan et al. (eds)., 88–108. CCDCOE.https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis/

Benga, Gabriel Constantin, Ionel Dănuț Savu, Sorin Vasile Savu, Bebe Adrian Olei, and Răzvan Ionuț Iacobici. 2019. "Assesment of Trends in Inland Waterway Transport within European Union.", Advanced Engineering Forum, 34.": 247–254. https://www.researchgate.net/publication/336256544_Assesment_of_Trends_in_Inland_Waterway_Transport_within_European_Union

Boyson, S. 2014. "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems." *Technovation* (Elsevier) 34, no. 7: 342–353. https://www.sciencedirect.com/science/article/abs/pii/S0166497214000194

Brzeziński, Marian Henryk. 2024. "Holistic foundations of military logistics theory development." *Military Logistics Systems* 60: 135-147. https://slw.wat.edu.pl/pdf-193854-114911?filename=114911.pdf

Chan, Hau Ling, and Tsan-Ming Choi. 2023. "Logistics management for the future: the IJLRA framework." *International Journal of Logistics Research and Applications* (Taylor & Francis) 27, no. 12: 1-19. https://www.tandfonline.com/doi/full/10.1080/13675567.2023.2286352

Chen, Li-Ming, and Wei-Lun Chang. 2021. "Supply- and cyber-related disruptions in cloud supply chain firms: Determining the best recovery speeds." *Transportation Research Part E* (Elsevier) 151: 1-18. https://www.sciencedirect.com/science/article/abs/pii/S1366554521001186

Cheung, Kam-Fung, Michael G.H. Bell, and Jyotirmoyee Bhattacharjya. 2021. "Cybersecurity in logistics and supply chain management: An overview and future research directions." *Transportation Research Part E* (Elsevier) 146: 1-18. https://www.sciencedirect.com/science/article/abs/pii/S1366554520308590

Chopra, Sunil. 2018. *Supply Chain Management: Strategy, Planning, and Operation.* Seventh Edition. Pearson Education Limited.

Colicchia, Claudia, Alessandro Creazza, and David Menachof. 2019. "Managing cyber and information risks in supply chains: insights from an exploratory analysis." *Supply Chain Management* (Emerald) 24, no. 2: 215-240. https://doi.org/10.1108/SCM-09-2017-0289

Creswell, J. W., Creswell, J. D. 2018. *Research design: qualitative, quantitative, and mixed methods approaches*. Fifth edition. SAGE Publications Inc.

Creswell, J. W. 1998. *Qualitative Inquiry and Research Design. Choosing among Five Traditions*. Thousand Oaks. SAGE Publications Inc.

Denzin, Norman K., Lincoln, Yvonna S. (*eds*.) 1994. *Handbook of Qualitative Research*. Thousand Oaks, SAGE Publications Inc.

Dury, Jason, and Jack O'Meara. 2021. *The CIO's role in maintaining a strong supply chain. Supply chains are no longer focused wholly on just-in-time delivery and logistics any more than CIOs are focused entirely on help desks and printers.* https://www.ciodive.com/news/cio-supply-chain-tips/605795/.

Dymyt, Małgorzata, Marta Bianka Wincewicz-Bosy, and Oskar Skubisz. 2024. "Global or local - glocalization as a challenge for the modern supply chains management." *Military Logistics Systems* 60: 181-197. https://slw.wat.edu.pl/pdf-193857-114914?filename=114914.pdf

Eggers, Shannon. 2020. "A novel approach for analyzing the nuclear supply chain cyber-attack surface." *Nuclear Engineering and Technology* 53: 879-887. https://www.sciencedirect.com/science/article/pii/S1738573320308573

European Commission. 2022. "Cyber Resilience Act." Brussels, 1-17. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Commission. 2021. "Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery." Brussels,1-23. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1884

Federal Communications Commission. 2024. *List of Equipment and Services Covered by Section 2 of The Secure Networks Act*. https://www.fcc.gov/supplychain/coveredlist.

Gaudenzi, Barbara, and Benedetta Baldi. 2024. "Cyber resilience in organisations and supply chains: from perceptions to actions." *The International Journal of Logistics Management* 35, no. 7: 99-122. https://www.emerald.com/insight/content/doi/10.1108/ijlm-09-2023-0372/full/html

Heath, E.A., J.E. Mitchell, and T.C. Sharkey. 2020. "Models for restoration decision making for a supply chain network after a cyber attack." *The Journal of Defense Modeling and Simulation* (Sage Journals) 17, no. 1: 5–19. https://journals.sagepub.com/doi/full/10.1177/1548512918808410

Hrab, Daniela-Elena, and Gheorghe Minculete. 2023. "Building tomorrow: additive manufacturing unleashing sustainable progress in the US military." *Insights into Regional Development* (Entrepreneurship and Sustainability Center) 5, no. 4: 115-134. https://www.researchgate.net/publication/376797913_Building_tomorrow_additive_manufacturing_unleashing_sustainable_progress_in_the_US_military

Hutchins, M.J., R. Bhinge, M.K. Micali, S.L. Robinson, J.W. Sutherland, and D. Dornfeld. 2015. "Framework for identifying cybersecurity risks in manufacturing." *Procedia Manufacturing 1*: 47–63. https://www.sciencedirect.com/science/article/pii/S2351978915010604

Jałowiec, Tomasz, and Dariusz Grala. 2022 "Research dilemma of military logistics." *Military Logistics Systems* 56: 5-14. https://www.researchgate.net/publication/364080355_Research_dilemma_of_military_logistics

Koch, Robert, and Mario Golling. 2016. "Weapons Systems and Cyber Security – A Challenging Union", in N.Pissanidis, H.Rőigas, M.Veenendaal (Eds.). *8th International Conference on Cyber Conflict: Cyber Power.* Tallinn, Estonia: NATO CCD COE Publications. 191-203. ". https://www.ccdcoe.org/uploads/2018/10/Art-12-Weapons-Systems-and-Cyber-Security-A-Challenging-Union.pdf

Kono, Keiko, and Samuele De Tomas Colatin. 2023. *National Approaches to the Supply Chain Cybersecurity: Taking a More Restrictive Stance Against High-Risk Vendors.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Kuckarts, Udo, and Rädiker, Stefan. 2023. *Qualitative Content Analysis. Methods, Practice and Software.* Second Edition, SAGE Publications Inc., London.

Layode, Oluwabunmi, Henry Nwapali Ndidi Naiho, Talabi Temitope Labake, Gbenga Sheriff Adelek, Ezekiel Onyekachukwu Udeh, and Ebunoluwa Johnson. 2024. "Addressing Cybersecurity Challenges in Sustainable Supply Chain Management: A Review of Current Practices and Future Directions." *International Journal of Management & Entrepreneurship Research* 6, no. 6: 1954-1981. https://www.researchgate.net/publication/383398010_Addressing_Cybersecurity_Challenges_in_Sustainable_Supply_Chain_Management_A_Review_of_Current_Practices_and_Future_Directions

Lyngaas, Sean. 2022. *Microsoft blames Russian military-linked hackers for ransomware attacks in Poland and Ukraine.* Prod. CNN.

Mentzer, John T., Theodore P. Stank, and Terry L. Esper. 2008. "Supply Chain Management and Its Relationship to Logistics." *Journal of Business Logistics* (Wiley) 29, no. 1: 31-46. https://onlinelibrary.wiley.com/doi/abs/10.1002/j.2158-1592.2008.tb00067.x

Muhuri, Pranab K., Amit K. Shukla, and Ajith Abraham. 2019. "Industry 4.0: A bibliometric analysis and detailed overview." *Engineering Applications of Artificial Intelligence* (Elsevier) 78: 218-235. https://www.sciencedirect.com/science/article/abs/pii/S0952197618302458

NATO Cooperative Cyber Defence Centre of Excellence. 2022. "Recent Cyber Events: Considerations for Military and National Security Decision Makers. Reflections on 2021: the ransomware threat, supply chain security, spyware export controls.". https://ccdcoe.org/uploads/2022/02/Report_Reflections_on_2021_A4.pdf

NATO Science & Technology Organization. 2020. "Science & Technology Trends 2020–2040. Exploring the S&T Edge.", 1-160. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

NATO Standardization Office. 2019. "NATO Standard AJP-4.10, Allied Joint Doctrine for Medical Support", Edition C, Version 1. https://www.coemed.org/files/stanags/01_AJP/AJP-4.10_EDC_V1_E_2228.pdf

NATO Standardization Office. 2018. "NATO Standard AJP-4 Allied Joint Doctrine for Logistics". https://assets.publishing.service.gov.uk/media/5f2d4db5d3bf7f1b1b53e80e/doctrine_nato_logistics_ajp_4.pdf

Pernik, Piret. 2022. "Drivers of Change Impacting Cyberspace in 2030." Chap. 5 in *Cyberspace Strategic Outlook 2030. Horizon Scanning and Analysis*, edited by Piret Pernik, 104. Tallinn: NATO CCD COE Publications. https://ccdcoe.org/library/publications/cyberspace-strategic-outlook-2030-horizon-scanning-and-analysis/

Prabhughate, Arati. 2020. *Cybersecurity for Transport and Logistics Industry. View Point.* Infosys Limited, 1-8. https://www.infosys.com/services/cyber-security/documents/transport-logistics-industry.pdf

Senarak, Chalermpong. 2021. “Port cybersecurity and threat: A structural model for prevention and policy development.” *The Asian Journal of Shipping and Logistics* (Elsevier) 37, no. 1: 20-36. https://www.sciencedirect.com/science/article/pii/S2092521220300389

Sepulveda, D. A., and O. Q. Khan. 2017. “A system dynamics case study of resilient response to IP theft from a cyber-attack.” *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM).* Singapore: IEEE,1291-1295.https://backend.orbit.dtu.dk/ws/portalfiles/portal/149425868/PID4982587.pdf

Tang, Christopher S., and Lucas P. Veelenturf. 2019. “The strategic role of logistics in the industry 4.0 era.” *Transportation Research Part E: Logistics and Transportation Review* (Elsevier) 129: 1-11. https://www.sciencedirect.com/science/article/abs/pii/S1366554519306349

The Brookings Institution. 2023. *Securing Global Mobility: A Conversation with General Jacqueline Van Ovost, 14th Commander of the US Transportation Command, Webinar*.

The UK Government. 2018. “DCPP Cyber Security Model: Industry Buyer and Supplier Guide.”, 1-30. https://www.gov.uk/government/publications/dcpp-cyber-security-model-industry-buyer-and-supplier-guide

The UK Government. 2021. “Policy Paper: Government Response to the Call for Views on Supply Chain Cyber Security.” *UK Government website.*. https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security/government-response-to-the-call-for-views-on-supply-chain-cyber-security (accessed November 5, 2024).

Tuptuk, Nilufer, and Stephen Hailes. 2018. “Security of smart manufacturing systems.” *Journal of Manufacturing Systems* 47: 93-106. https://www.sciencedirect.com/science/article/pii/S0278612518300463

United States Government Accountability Office. 2016. “Report to Congressional Committees, Counterfeit Parts. DoD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk.”, 1-49. https://www.gao.gov/products/gao-16-236

US Army Futures Command. n.d. “Future Operational Environment: Forging the future in an uncertain world 2035-2050.”, 1-25. https://community.apan.org/cfs-file/__key/telligent-evolution-components-attachments/01-9016-00-00-00-16-09-66/AFC-Pam-525_2D00_2-The-Future-Operational-Environment-2035_2D00_2050.pdf

Xiang, Liu, et al. 2020. *Cyber Security Risk Management for Connected Railroads.* Washington, DC: US Department of Transportation. https://railroads.dot.gov/elibrary/cyber-security-risk-management-connected-railroads

Zhang et al. 2020. "Industrial Blockchain of Things: A Solution for Trustless Industrial Data Sharing and Beyond." *16th International Conference on Automation Science and Engineering (CASE)*. IEEE, 1187-1192. https://ieeexplore.ieee.org/document/9216817

Zhiyi, Li, Dong Jin, Christopher Hannon, Mohammad Shahidehpour, and Jianhui Wang. 2016. "Assessing and mitigating cybersecurity risks of traffic light systems in smart cities." *Cyber-Physical Systems: Theory & Applications 1* (IET) 1, no. 1: 60-69. https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-cps.2016.0017

THE ANTHROPOLOGY OF DISTRUST AND CHANGE IN ROMANIA: A REVIEW

RADU UMBREȘ
ANTROPOLOGIE
NEÎNCREDEREA
Cum funcționează
România profundă
O cercetare antropologică
Miza cărții este nu un mic sat din nordul țării, ci marele sat pe nume România. O poveste pasionantă și esențială despre noi.
—IULIAN COMĂNESCU
HUMANITAS

Radu Umbreș, Living with Distrust: Morality and Cooperation in a Romanian Village, Oxford University Press 2022 – original edition, (Neîncrederea. Cum funcționează România profundă – o cercetare antropologică, 2024, Humanitas).

Distrust represents a significant issue in Romania. According to the latest instalment of *World Values Survey*, 87.3% of respondents expressed a general state of lack of trust, with 75% reporting skepticism towards the government and 84% towards the parliament (Haerpfer 2022). Meanwhile, trust remains high within familial relationships, with 96% of individuals expressing confidence in their families, and approximately 54% maintain caution toward their neighbors (Haerpfer 2022). Distrust can be interpreted as a form of security vulnerability, the implications of which may have become evident over the past year and a half.

How does this phenomenon manifest in everyday life and is there a path forward? *Living with Distrust by* Radu Umbreș aims to address exactly these issues. The book presents the findings of an anthropological research, endeavored for Oxford University, and the present review refers to the Romanian translation (Umbreș 2024). The research focuses on a small village in Eastern Moldova in recent years and offers valuable insights for those interested in subjects such as local social interactions, development, politics, but also in national security concerns.

Living with Distrust is narratively structured, unfolding as a story. It begins with an exploration of political life, then delves into deeper social structures and cultural practices of housing, family life and funeral rites, culminating in a discussion of potential resolutions to the challenges presented. The beginning and the ending are antithetical: the former shows the consequences of this lack of trust, while the latter emphasizes pathways toward cooperation. The overall context also plays a crucial role in shaping the analysis.

The village under study is situated in one of the economically disadvantaged regions of Romania. Public services and the effects of state's policies are faulty at best, often harmful and the local population is frequently marginalized. Radu Umbreș points out that there is a notable absence of local solidarity or a shared sense, of community among inhabitants, which challenges conventional sociological explanations that attribute trust and cooperation to localist bonds. From the beginning, the book's title – *Living with Distrust* – carries an air of enigma, inviting the reader to explore the roots and manifestations of pervasive mistrust.

The opening sequence shows a fight in a tavern. This way, the reader is introduced to the major factions of *Săteni*, the fictionalized name used for the village. Local leaders have monopolized public positions and strategically deploy resources to reward their followers and to marginalize opponents. *Living with Distrust* shows the tavern functioning as a symbolic and literal stage for the performance of power and prestige. However, the story is not simply about theatricals.

Beyond the broader context of distrust, *Living with Distrust* turns its focus to the family, portrayed as a fundamental social unit. This sphere is characterized by a pragmatic maxim: one should trust one's relatives, but only to a limited extent. The domestic domain was once self-sufficient and although the ideal of familial autonomy persists, the pressure of historical change have significantly eroded many of its foundational conditions. In Umbres' ethnography, the family is understood less in terms of lineage, and more in terms of behavioral expectations and reciprocal obligations.

Social alliances are often made between familial units. They became kin (*neamuri*) by the once complicated ceremonies of marriage, which were once the product of agreements between families, often centered around the transfer of property. As it happened in many places, these rites have undergone processes of modernization and the tendency of individualization grew in strength, a trend clearly documented in *Living with Distrust*. Even with all these changes, the family remains the main form of trust-creating institution and it still creates rights and obligations, described with humor by Radu Umbreș.

Funerary practices occupy a central place in the social life of *Săteni*. The author shows to the reader the way these rites and practices function like reflections of deep held beliefs and social institutions. The funeral is a moment when private sphere of the family becomes temporarily open to the broader community, and the rules must be followed with utmost precision, or otherwise, the community takes notice. According to *Living with Distrust*, funerals are also influenced by the relationship of cooperation and conflict developed between the families.

The distribution of trust explains the economy and the politics of the village. This relational pattern aligns with what social scientists have long recognized as "amoral familism", a concept famously articulated by Edward Bancroft in a famous research dedicated to the South of Italy (Banfield 1958). In this framework, the distrust between the units and the relative trust inside them leads to a pattern of relationships somehow similar to the one from world politics. The author describes in *Living with Distrust* how alliances are made and unmade, the local spirit of community is weak, and the public services and integrity are faulty.

The village appears caught in a self-reinforcing cycle, reminiscent of a *Catch 22:* the pervasive lack of trust hinders cooperation, and limited cooperation further deepens distrust. But there are ways of this vicious circle. The setting can partially be explained by a complex historical legacy of ineffective public policy and social detachment exibited by Romanian elites, and the trend may change its direction, argues Radu Umbreș. *Living with Distrust* offers the example of a local entrepreneur, Mihai, who manages to transcend prevailing social constraints by useful and predictive work and private initiative.

The analysis presented in *Living with Distrust* is not without ambiguities. It is difficult to write about a group of distrustful people from outside and the Romanian reception of the book reflects this complexity, resembling a system of mirrors and reflections. Radu Umbreș used Thomas Hobbes and Émile Durkheim - figures whose views on authoraty, order, and social cohesion serve both points of inspiration and critique, and intellectual references (and opposites), but John Locke is closer to his vision and he plays a relatively minor role in the book. The translator of *Living with Distrust*, Iulian Comănescu argues that the book`s ideas can be generalized, but Romania's social landscape is marked by considerable regional and cultural variation. Nevertheless, the phenomenon of widespread mistrust appears to be a common thread, cutting across these diverse contexts and reinforcing the book's relevance to broader national debates.

Overall, the research represents a very useful contribution to the study of contemporary Romanian society. The topic is both highly relevant and frequently overlooked in scholarly discourse. Notably, some suggestions can lead to further studies, especially the connection between local social interactions and patterns of emigration. The study is based on a rigourous research activity, corresponding to the best practices available worldwide in the discipline of social anthropology. The arguments presented by the author, who employs a writing style and language both accesible and engaging.

BIBLIOGRAPHY:

Banfield, Edward C. 1958. *The Moral Basis of a Backward Society.* Chicago : Free Press.

Haerpfer, C., Inglehart, R., Moreno, A., Welzel, C., Kizilova, K., Diez-Medrano J., M. Lagos, P. Norris, E. Ponarin & B. Puranen (coord.). 2022. "World Values Survey: Round Seven – Country-Pooled Datafile Version 6.0." *JD Systems Institute & WVSA Secretariat.* doi:10.14281/18241.24.

Umbreș, Radu. 2024. *Neîncrederea: cum funcționează România profundă.* București: Humanitas.

Mihai ZODIAN, PhD[*]

[*] ***Mihai ZODIAN, PhD, is Researcher at the Centre for Defence and Security Strategic Studies within "Carol I" National Defence University, Bucharest, Romania.***
E-mail: zodian.vladimir@unap.ro

STRATEGIES XXI

INTERNATIONAL SCIENTIFIC CONFERENCE

THE COMPLEX AND DYNAMIC NATURE OF THE SECURITY ENVIRONMENT

February 27, 2025

The 24th edition of the *CDSSS "STRATEGIES XXI" International Scientific Conference* took place as a hybrid event on February 27, 2025. This esteemed academic forum serves as a platform for exchanging ideas, sharing perspectives, and presenting advanced research in the fields of security, strategy, and the contemporary military studies. It also aims to foster a culture of strategic and security awareness, encourage engagement with experts from the National Defence, Public Order, and National Security System (SNAOPSN), and strengthen scientific collaboration both nationally and internationally.

This year's edition brought together prominent experts, researchers, and practitioners to address current security challenges and emerging threats, focusing on a range of topics including:

- *Security and defence policies in the new strategic environment;*
- *Concepts and theories in security and defence;*
- *Hybrid threats in today's security environment - state and non-state actors amid great power rivalries;*
- *Impact of climate change on national security;*
- *The Russia - Ukraine war: shaping future security and defence policy – The Indo-Pacific region and U.S;*
- *China rivalry – tensions and crises in the Middle East – security trends in the Caucasus and Central Asia;*
- *Security environment developments in Africa;*
- *Strategic scenarios – prospective studies on security and defence.*

The conference had the honour of hosting distinguished keynote speakers who offered strategic insights from the evolving security dynamics.

Panel 1, titled ***Contemporary Crises and International Security***, featured discussions on a range of critical topics, such as *military manpower - a new challenge for the European states - possible solutions for Romania; Romania's role in NATO's evolving strategic posture; analysis of Eurasian geopolitical shifts and their impact on European security; emerging security threats in the Black Sea region*, among others. These subjects were addressed by:

• Dan-Florin GRECU, PhD, Major General (Ret.), President of the Association of Reserve Officers from Romania;

• Emilian CHIREA, PhD, Brigadier General, Deputy Military Representative of Romania to NATO and the EU;

• Antonia COLIBĂȘANU, PhD, Assoc. Prof., from Geopolitical Futures and the Foreign Policy Research Institute, Romania;

• Răzvan BUZATU, PhD, expert in strategic affairs.

Panel 2, titled ***Emergent Technologies as a Game Changer in Contemporary Global Competition,*** fostered a dynamic and engaging scientific dialogue. The panel featured insightful contributions from:

• Stelian CRISTEA, Deputy Director of the Romanian National Cyber Security Directorate;

• Ștefan CANTARAGIU, PhD, Brigadier General (Ret.), Vice-President of the Association of Reserve Officers from Romania and Corresponding Member of the Romanian Academy of Scientists;

• Andrei PĂUN, PhD, Professor, Director of the "Mihai Drăgănescu" Institute for Artificial Intelligence Research (ICIA), Romania;

• Cristian SFICHI, Regional Director for Ukraine, Romania, and the Caucasus at Thales Group – Conference Sponsor.

• Mario MARINOV, PhD, Researcher at the University of Library Studies and Information Technologies, Bulgaria.

The discussions centered on the evolving role of cyber operations on the security environment – the integration of Human-Technology interaction to enhance multi-domain operations; the strategic role of cyberspace in regional conflicts; the transformative impact of disruptive technologies (such as Artificial Intelligence and Quantum technology, etc.) in reconfiguring spheres of influence in a geopolitical context; the potential of emerging and disruptive technologies as enablers for advanced military capabilities; the threats and risks associated with integrating disruptive technologies into defence systems and their implications on national security; convergent and divergent trends in military technology developments – military cooperation; and the concept of human augmentation, exploring the boundary between myth and reality.

A special session was also dedicated to the Conference Sponsor, Thales Group, showcasting the company's contributions to cutting-edge defence technologies, cybersecurity, and AI-powered military solutions;

Centre for Defence and Security Strategic Studies
THALES
THALES
THE IMPACT OF CLIMATE CHANGES ON NATIONAL SECURITY

The scientific event included a presentation of the *Integrated Educational Infrastructures for Intelligent Learning - 4EDU* project, funded through the National Recovery and Resilience Plan (PNNR), Component C15 – Education[1]. The project is coordinated by Colonel Assoc. Prof. Florin Popescu, PhD, who delivered a lecture on *Digital Architectural Frameworks Designed for Civil and Military Applications*. In addition, two books were presented during the event:

- *The Impact of Climate Change on Romania's National Security (Impactul Schimbărilor Climatice asupra Securității Naționale a României)*. The book presents a series of analyses conducted by the authors across key areas and dimensions of national security, utilising a structured analytical model. The findings and conclusions provide insight into the current state and projected developments regarding the influence of climate change on Romania's national security.
- *Operational Design: Applying Operational Art in the Operations Planning Process (Designul Operațional: Aplicarea Artei Operative în Procesul de Planificare a Operațiilor)* offers an in-depth and dynamic exploration of the role of art in the military field. The book explores how the essential components of operational design

[1] The implementation of Component 15 is overseen by the Ministry of Education, the Ministry of Development, Public Works and Administration and the Ministry of European Investments and Projects.

are developed and applied to support the commander's decision-making process, while also functioning as a practical tool to support the operational planning cycle.

Finanțat de Uniunea Europeană NextGenerationEU

Planul Național de Redresare și Reziliență

„PNRR: INFRASTRUCTURI EDUCAȚIONALE INTEGRATE PENTRU ÎNVĂȚAREA INTELIGENTĂ"

GRANT NR. 1511212569

WORKSHOP:

DIGITAL ARCHITECTURAL FRAMEWORKS DESIGNED FOR CIVIL AND MILITARY APPLICATIONS

-27.02.2025-

https://mfe.gov.ro/pnrr/
https://www.facebook.com/PNRROficial/
https://www.facebook.com/unapcarol1/

IMPACTUL SCHIMBĂRILOR CLIMATICE ASUPRA SECURITĂȚII NAȚIONALE A ROMÂNIEI

Coordonatori: Florian Circiumaru
Dan-Lucian Petrescu

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
BUCUREȘTI, 2024

DESIGNUL OPERAȚIONAL

APLICAREA ARTEI OPERATIVE ÎN PROCESUL DE PLANIFICARE A OPERAȚIILOR

Crăișor-Constantin IONIȚĂ
Daniel ROMAN

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
BUCUREȘTI, 2024

Event photo: *4EDU Project: - Digital Architectural Frameworks Designed for Civil and Military Applications*
Books: • The Impact of Climate Change on Romania's National Security;
• Operational Design: Applying Operational Art in the Operations Planning Process

The conference showcased significant contributions from distinguished academics and professionals from Bulgaria, Hungary, Moldova, and the Czech Republic. The presentations spanned a broad array of contemporary topics, addressing key issues such as geopolitical rivalries, radicalization, cybersecurity, military strategies, and hybrid threats:

• ***Motives, Mechanisms and Map of Far-Right Radicalisation in Europe. Myths and Sociological Confirmations*** – Iulian CHIFU, PhD, Prof.; Cosmin GRIGORE, PhD Candidate, Center for Conflict Prevention and Early Warning (CPCEW), Romania

• ***Trump's Second Term and Us-China Rivalry: Geopolitical Implications*** – Mădălin ENESCU, PhD; Ana Maria FLOREA, PhD Candidate, National University of Political Studies and Public Administration, Romania

• ***Holding the Line: American Military Diplomatic Actions in the Sinosphere in the Context of the Second Cold War*** – Mihai VLAICU, University of Craiova, Romania

• ***Russia: A Terrorist State and Sponsor of Terrorism*** – Iulian-Constantin MĂNĂILESCU, PhD Candidate, "Alexandru Ioan Cuza" Police Academy, Romania

- ***The Russian-Ukrainian War and its Geopolitical Implications*** – Eugen SITEANU, PhD, Colonel (Ret.), Prof. Eng., Academy of Romanian Scientists, Romania; Eng. Iulian TOADER, PhD Candidate, "Carol I" National Defence University, Romania
- ***National Security Imperatives and The Challenge of Civilian-Defence Cybersecurity Integration in the European Union*** – Niculae IANCU, PhD, Maritime Cybersecurity Centre of Excellence, Constanța Maritime University, Romania
- ***The Third and the Fourth Departments of the People's Liberation Army and Cyber Threats -*** Alida Monica Doriana BARBU, PhD, PhD Candidate, "Babes-Bolyai" University, Romania
- ***Challenges at National Level Regarding Enhanced Military Mobility Capacity in the Framework of Implementing the Multi-Domain Operations Concept*** – Ionela Cătălina MANOLACHE, PhD Candidate, "Carol I" National Defence University, Romania
- ***Evolution of the Strategic Rocket Forces of the Russian Federation in the Post-Cold War Era; Precision Glide Munitions. Methods for Effective Counteraction Based on the Conflict in Ukraine*** – Mario MARINOV, PhD, Researcher, University of Library Studies and Information Technologies, Bulgaria
- ***Pager Explosions in Lebanon – Impact on Regional and International Security*** – Lyubosvet STOEV, PhD, Assoc. Prof.; Zhivo PETROV, Colonel, PhD, Assoc. Prof., "Georgi Stoykov Rakovski" National Defense College, Bulgaria
- ***Drones – A Threat to Security?*** – Ana-Raluca STAN, PhD, CDSSS, "Carol I" National Defence University, Romania
- ***National Ideal and National Interests Linked by the National Strategy*** – Grudi Ivanov ANGELOV, PhD, Major General (Ret.), Assoc. Prof., University of Library Studies and Information Technologies, Bulgaria
- ***Strategic Coordination, Institutional Fragmentation and Policy Challenges in Governing Romania's National Security*** – Niculae IANCU, PhD, Maritime Cybersecurity Centre of Excellence, Constanta Maritime University, Romania
- ***Hungary's Transformation from Security Consumer to Provider within NATO*** – Faragó BENCE, PhD Candidate, National University of Public Service (NUPS), Hungary
- ***Narratives in the Czech Society Regarding the War in Ukraine*** – Libor FRANK, PhD, Assistant Professor, Centre for Security and Military Strategic Studies, University of Defence, Czech Republic
- ***The New NATO Policy on Reserves. A Romanian Project to Implement It*** – Crăișor-Constantin IONIȚĂ, PhD, Brigadier General (Ret.), Researcher, CDSSS, "Carol I" National Defence University, Romania; Elena-Adriana BRUMARU, PhD Candidate, "Alexandru cel Bun" Military Academy, Republic of Moldova

• ***Challenges of Illegal Migration in the Context of Romania's Accession to the Schengen Area*** – Emanuel Sebastian GEORGESCU, PhD Candidate, "Carol I" National Defence University, Romania

• ***Weaponization of Religion as one of the Main Hybrid Instruments Directed Against Romanians in the Republic of Moldova, Ukraine and Romania*** – Matei BLĂNARU, PhD Candidate, University of Bucharest, Romania

• ***Disinformation and Its Threats to Economic Security: The Impact of False Rumors on Financial Markets and Global Economic Stability*** – George Gabriel NISTORESCU PhD, Deputy Police Commissioner National Anticorruption Directorate, Romania; Vasile Cătălin GOLOP, PhD, Police Commissioner, "Alexandru Ioan Cuza" Police Academy, Romania

• ***Recent International Security Crises – Conceptual Framework and Empirical Insights*** – Mirela ATANASIU, PhD, Senior Researcher, CDSSS, "Carol I" National Defence University, Romania

• ***Methodological Debates and Great Power Identity*** – Mihai ZODIAN, PhD, Researcher, CDSSS, "Carol I" National Defence University, Romania

• ***A Theoretical Approach to Understanding Security Culture and Its Impact on National Security*** – Alexandra SARCINSCHI, PhD, Senior Researcher, CDSSS, "Carol I" National Defence University, Romania

• ***Considerations on the Causes of Climate Change and the Scientific Consensus Regarding Anthropogenic Factors*** – Daniela LICĂ, PhD, Researcher, CDSSS, "Carol I" National Defence University, Romania

• ***Building Urban Security in Climate Change Context*** – Sorina-Georgiana RUSU, PhD, Lect. Habil. Urb. Mil. Sc., "Ion Mincu" University of Architecture and Urban Planning, Romania.

The conference papers will be published in the Conference Proceedings, which are indexed in international databases including EBSCO, PROQUEST, and CEEOL. They will also be publicly accessible on the CDSSS website at https://cssas.unap.ro/en/books.htm and on the International Scientific Conference STRATEGIES XXI website at https://strategii21.ro/index.php/en/conference-proceedings

Event photo: *STRATEGIES XXI International Scientific Conference*
The complex and dynamic nature of the security environment

This year's conference highlighted the complex and ever-changing nature of security challenges, emphasizing the critical need for interdisciplinary collaboration and strategic foresight in tackling global threats. It marked a significant milestone in the scientific calendar of "Carol I" National Defence University and Centre for Defence and Security Strategic Studies, offering an academic forum for in-depth strategic discussion.

Raluca STAN, PhD*

[*] ***Raluca STAN, PhD, carries out her professional activities in the Scientific Events Department of the Centre for Defence and Security Strategic Studies (CDSSS).***
E-mail: stan.raluca@unap.ro

GUIDE FOR AUTHORS

We welcome those interested in publishing articles in the academic journal *Strategic Impact*, while subjecting their attention towards aspects to consider upon drafting their articles. **Starting with issue no. 1/2023, the journal shall be published in the English language only!**

MAIN SELECTION CRITERIA are the following:

- ✓ **Compliance with the thematic area of the journal – security and strategic studies** and the following topics: political-military topical aspects, trends and perspectives in security, defence, geopolitics and geostrategies, international relations, intelligence, information society, peace and war, conflict management, military strategy, cyber-security;
- ✓ **Originality** of the paper – own argumentation; novelty character – not priorly published;
- ✓ **Quality of the scientific content** – neutral, objective style, argumentation of statements and mentioning of all references used;
- ✓ **A relevant bibliography**, comprising recent and prestigious specialized works, including books, presented according to herein model;
- ✓ **English** language shall meet academic standards (British or American usage is accepted, but not a mixture of these).
- ✓ **Adequacy to the editorial standards adopted by the journal.**

EDITING NORMS

- ✓ **Article length** may vary between **6 and 12 pages** (25.000 - 50.000 characters), including bibliography, tables and figures, if any.
- ✓ **Page settings**: margins – 2 cm, A 4 format.
- ✓ The article shall be written in **Times New Roman font, size 12, one-line spacing.**
- ✓ The document shall be saved as Word (.doc/.docx). The name of the document shall contain the author's name.

ARTICLE STRUCTURE

- ✓ **Title** (centred, capital, bold characters, font 24).
- ✓ **A short presentation of the author**, comprising the following elements: given name, last name (the latter shall be written in capital letters, to avoid

confusion), main institutional affiliation and position held, military rank, academic title, scientific title (PhD title or PhD Candidate – domain and university), city and country of residence, e-mail address.

- ✓ A relevant **abstract**, not to exceed 150 words (italic characters)
- ✓ 6-8 relevant **keywords** (italic characters)
- ✓ **Introduction / preliminary considerations**
- ✓ **2 - 4 chapters** (numbered, starting with 1) (subchapters if applicable)
- ✓ **Conclusions**.
- ✓ **Tables / graphics / figures**, if they are useful for the argumentation, with reference made in the text. They shall be also sent in .jpeg /.png/.tiff format as well.

In the case of tables, please mention above "**Table no. X**: Title", while in the case of figures there shall be mentioned below (e.g. maps, etc.), "**Figure no. X:** Title" and the source, if applicable, shall be mentioned in a footnote.

REFERENCES

It is academic common knowledge that in the Abstract and Conclusions there shall not be inserted any references.

The article shall have references and bibliography, in the form seen below. Titles of works shall be mentioned in the language in which they were consulted, with transliteration in Latin alphabet if there is the case (e.g. in the case of Cyrillic, Arabic characters, etc.). Please provide English translation for all sources in other languages.

The article will comprise in-text citation and bibliography (in alphabetical order), according to The Chicago Manual of Style[1], as in examples below:

BOOK

Reference list entries (in alphabetical order)

Grazer, Brian, and Charles Fishman. 2015. A Curious Mind: The Secret to a Bigger Life. New York: Simon & Schuster.

Smith, Zadie. 2016. Swing Time. New York: Penguin Press.

In-text citation

(Grazer and Fishman 2015, 12)

(Smith 2016, 315–16)

[1] URL: https://www.chicagomanualofstyle.org/tools_citationguide/citation-guide-2.html

CHAPTER OF AN EDITED BOOK

In the reference list, include the page range for the chapter. In the text, cite specific pages.

Reference list entry

Thoreau, Henry David. 2016. "Walking." *In The Making of the American Essay*, edited by John D'Agata, 167–95. Minneapolis: Graywolf Press.

In-text citation

(Thoreau 2016, 177–78)

ARTICLE

In the reference list, include page range for the whole article. In the text, cite specific page numbers. For article consulted online, include a URL or the name of the database in the reference list entry. Many journal articles list a DOI (Digital Object Identifier). A DOI forms a permanent URL that begins https://doi.org/. This URL is preferable to the URL that appears in your browser's address bar.

Reference list entries (in alphabetical order)

Keng, Shao-Hsun, Chun-Hung Lin, and Peter F. Orazem. 2017. "Expanding College Access in Taiwan, 1978–2014: Effects on Graduate Quality and Income Inequality." *Journal of Human Capital* 11, no. 1 (Spring): 1–34. https://doi.org/10.1086/690235.

LaSalle, Peter. 2017. "Conundrum: A Story about Reading." *New England Review* 38 (1): 95–109. Project MUSE.

In-text citation

(Keng, Lin, and Orazem 2017, 9–10)

(LaSalle 2017, 95)

WEBSITE CONTENT

Reference list entries (in alphabetical order)

Bouman, Katie. 2016. "How to Take a Picture of a Black Hole." Filmed November 2016 at TEDxBeaconStreet, Brookline, MA. Video, 12:51. https://www.ted.com/talks/katie_bouman_what_does_a_black_hole_look_like

Google. 2017. "Privacy Policy." Privacy & Terms. Last modified April 17, 2017. https://www.google.com/policies/privacy/

Yale University. n.d. "About Yale: Yale Facts." Accessed May 1, 2017. https://www.yale.edu/about-yale/yale-facts

Citare în text

(Bouman 2016)

(Google 2017)

(Yale University, n.d.)

NEWS OR MAGAZINE ARTICLES

Articles from newspapers or news sites, magazines, blogs, and like are cited similarly. In the reference list, it can be helpful to repeat the year with sources that are cited also by month and day. If you consulted the article online, include a URL or the name of the databases.

Reference list entries (in alphabetical order)

Manjoo, Farhad. 2017. “Snap Makes a Bet on the Cultural Supremacy of the Camera.” *New York Times*, March 8, 2017. https://www.nytimes.com/2017/03/08/technology/snap-makes-a-bet-on-the-cultural-supremacy-of-the-camera.html

Mead, Rebecca. 2017. “The Prophet of Dystopia.” *New Yorker*, April 17, 2017.

Pai, Tanya. 2017. “The Squishy, Sugary History of Peeps.” *Vox*, April 11, 2017. http://www.vox.com/culture/2017/4/11/15209084/peeps-easter

In-text citation

(Manjoo 2017)

(Mead 2017, 43)

(Pai 2017)

For more examples, please consult The Chicago Manual of Style.

SCIENTIFIC EVALUATION PROCESS is developed according to the principle *double blind peer review*, by university teaching staff and scientific researchers with expertise in the field of the article. The author’s identity is not known by evaluators and the name of the evaluators is not made known to authors.

Authors are informed of the conclusions of the evaluation report, which represent the argument for accepting/rejecting an article.

Consequently to the evaluation, there are three possibilities:

a) the article is accepted for publication as such or with minor changes;

b) the article may be published if the author makes recommended improvements (of content or of linguistic nature);

c) the article is rejected.

Previous to scientific evaluation, articles are subject to an *antiplagiarism analysis*.

DEADLINES:

All authors will send their articles in English to the editor’s e-mail address, **impactstrategic@unap.ro**.

We welcome articles all year round.

NOTA BENE:

Authors are not required any fees for publication and are not retributed.

By submitting their materials for evaluation and publication, the authors acknowledge that they have not published their works so far and that they possess full copyrights for them.

Parts derived from other publications should have proper references.

Authors bear full responsibility for the content of their works and for ***non-disclosure of classified information*** – according to respective law regulations.

Editors reserve the right to request authors or to make any changes considered necessary. Authors give their consent to possible changes of their articles, resulting from review processes, language corrections and other actions regarding editing of materials. The authors also give their consent to possible shortening of articles in case they exceed permitted volume.

Authors are fully responsible for their articles' content, according to the provisions of *Law no. 206/2004 regarding good conduct in scientific research, technological development and innovation*.

Published articles are subject to the Copyright Law. All rights are reserved to "Carol I" National Defence University, irrespective if the whole material is taken into consideration or just a part of it, especially the rights regarding translation, re-printing, re-use of illustrations, quotes, dissemination by mass-media, reproduction on microfilms or in any other way and stocking in international data bases. Any reproduction is authorized without any afferent fee, provided that the source is mentioned.

Failing to comply with these rules shall trigger article's rejection. Sending an article to the editor implies the author's agreement on all aspects mentioned above.

For more details on our publication, you can access our site, http://cssas.unap.ro/en/periodicals.htm or contact the editors at impactstrategic@unap.ro

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE

Layout editor: Gabriela CHIRCORIAN

The publication consists of 76 pages.

"Carol I" National Defence University Printing House
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
E-mail: editura@unap.ro
Tel: 021/319.40.80/215

No. 566/10.09.2025 C. 187/2025